AutoUni – Schriftenreihe

Matthias Trojahn

Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens

AutoUni – Schriftenreihe

Band 85

Herausgegeben von / Edited by
Volkswagen Aktiengesellschaft
AutoUni

Die Volkswagen AutoUni bietet den Promovierenden des Volkswagen Konzerns die Möglichkeit, ihre Dissertationen im Rahmen der „AutoUni Schriftenreihe“ kostenfrei zu veröffentlichen. Die AutoUni ist eine international tätige wissenschaftliche Einrichtung des Konzerns, die durch Forschung und Lehre aktuelles mobilitätsbezogenes Wissen auf Hochschulniveau erzeugt und vermittelt.
Die neun Institute der AutoUni decken das Fachwissen der unterschiedlichen Geschäftsbereiche ab, welches für den Erfolg des Volkswagen Konzerns unabdingbar ist. Im Fokus steht dabei die Schaffung und Verankerung von neuem Wissen und die Förderung des Wissensaustausches.
Zusätzlich zu der fachlichen Weiterbildung und Vertiefung von Kompetenzen der Konzernangehörigen, fördert und unterstützt die AutoUni als Partner die Doktorandinnen und Doktoranden von Volkswagen auf ihrem Weg zu einer erfolgreichen Promotion durch vielfältige Angebote – die Veröffentlichung der Dissertationen ist eines davon. Über die Veröffentlichung in der AutoUni Schriftenreihe werden die Resultate nicht nur für alle Konzernangehörigen, sondern auch für die Öffentlichkeit zugänglich.

The Volkswagen AutoUni offers PhD students of the Volkswagen Group the opportunity to publish their doctor’s theses within the “AutoUni Schriftenreihe” free of cost. The AutoUni is an international scientific educational institution of the Volkswagen Group Academy, which produces and disseminates current mobility-related knowledge through its research and tailor-made further education courses. The AutoUni's nine institutes cover the expertise of the different business units, which is indispensable for the success of the Volkswagen Group. The focus lies on the creation, anchorage and transfer of knew knowledge.
In addition to the professional expert training and the development of specialized skills and knowledge of the Volkswagen Group members, the AutoUni supports and accompanies the PhD students on their way to successful graduation through a variety of offerings. The publication of the doctor’s theses is one of such offers.
The publication within the AutoUni Schriftenreihe makes the results accessible to all Volkswagen Group members as well as to the public.

Herausgegeben von / Edited by
Volkswagen Aktiengesellschaft
AutoUni
Brieffach 1231
D-38436 Wolfsburg
http://www.autouni.de

Matthias Trojahn

Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens

Springer

Matthias Trojahn
Wolfsburg, Deutschland

Zugl.: Dissertation, Otto-von-Guericke Universität Magdeburg, 2016

Die Ergebnisse, Meinungen und Schlüsse der im Rahmen der AutoUni Schriftenreihe veröffentlichten Doktorarbeiten sind allein die der Doktorandinnen und Doktoranden.

AutoUni – Schriftenreihe
ISBN 978-3-658-14048-9 ISBN 978-3-658-14049-6 (eBook)
DOI 10.1007/978-3-658-14049-6

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH

Danksagung

Die vorliegende Dissertation entstand während der Tätigkeit als Doktorand bei der Volkswagen Aktiengesellschaft im Bereich der mobilen Endgeräte am Standort Wolfsburg in Zusammenarbeit mit dem Institut für Verteilte Systeme (IVS) an der Fakultät für Informatik der Otto-von-Guericke-Universität in Magdeburg.

Zunächst möchte ich Herrn Prof. Dr. Frank Ortmeier für die hervorragende wissenschaftliche Betreuung und zahlreichen Diskussionen danken. Des Weiteren gilt Herrn Prof. Dr. Thomas Leich und Herrn Prof. Dr. Heinrich Hußmann mein Dank für die zahlreichen Gespräche und die Übernahme des Zweit- bzw. Drittgutachtens.

Die vorliegende Arbeit wäre ohne die Unterstützung der vielen Probanden, die sich dazu bereit erklärt haben, an den Studien teilzunehmen, nicht möglich gewesen. Insbesondere möchte ich den zahlreichen Studenten für die Durchführung der Studien und die vielen Anregungen danken.

An dieser Stelle bedanke ich mich bei allen Kollegen der Abteilung „Client & Communication Technologies“ der Volkswagen AG für die vielen Ratschläge, Hinweise und Inspirationen.

Den wissenschaftlichen Mitarbeitern des Fachgebiets „Software Engineering“ der Otto-von-Guericke-Universität möchte ich für die freundschaftliche Aufnahme und die vielen fachlichen Diskussionen danken.

Nicht zuletzt geht ein großer Dank an meine Familie und meine Freunde, insbesondere an meine Frau Kristina, die mich in der Zeit meines Studiums und meiner Dissertation unterstützt und motiviert haben.

Matthias Trojahn

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

API	Application Programming Interface (dt. Schnittstelle bei der Programmierung)
App	Applikation
BSI	Bundesamt für Sicherheit in der Informationstechnik
DPI	Dots Per Inch (dt. Auflösung u. a. beim Drucken)
DTW	Dynamic Time Warping (dt. Klassifikator für unterschiedlich lange Sequenzen)
EER	Equal Error Rate (dt. Punkt bei dem FAR und FRR gleich sind)
FAR	False Acceptance Rate (dt. prozentualer Anteil an falsch akzeptierten Personen)
FFT	Fast Fourier-Transformation (dt. schnelle Fourier-Transformation)
FRR	False Rejection Rate (dt. prozentualer Anteil an falsch zurückgewiesenen Personen)
GAR	Genuine Accept Rate (dt. prozentualer Anteil an korrekt zurückgewiesenen Personen)
GPS	Global Positioning System (dt. Globales Positionsbestimmungssystem)
HD	High Definition (hochauflösendes Display)

IBAN International Bank Account Number

IBk Instance-Based learner for k (dt. Instanz-basierter Klassifikator)

IEC International Electrotechnical Commission (dt. Normungsgremium für Elektrotechnik)

ISO International Organization for Standardization (dt. Internationale Organisation für Normung)

IT Information Technology (dt. Informationstechnologie)

kNN k-Nearest-Neighbor (dt. k nächsten Nachbarn - Algorithmus)

LED Light Emitting Diode (dt. Leuchtdiode)

NLP Natural Language Processing (dt. Computerlinguistik)

NIST National Institute of Standards and Technology (dt. Nationales Institut für Standards und Technologie)

OHA Open Handset Alliance (Konsortium zur Entwicklung offener Standards für mobile Endgeräte)

OLED Organic Light Emitting Diode (dt. organische Leuchtdiode)

OTP One Time Password (dt. Einmalpasswort)

PC Personal Computer (dt. persönlicher Computer)

PIN Personal Identification Number (dt. (persönliche) Geheimnummer)

PKI Public Key Infrastructure (dt. Public-Key-Infrastruktur)

PSPP Open-Source Version von SPSS (Statistical Package for the Social Sciences)

RBFN	Radial Basis Function Network (dt. radiale Basisfunktionsnetzwerk – Klassifikator)
QWERT	Standard Tastaturenlayout
ROC	Receiver Operator Characteristic (dt. Kurve zur Grenzwertoptimierung)
SPSS	Statistical Package for Social Scientists (Statistik- und Analyse-Software)
SVM	Support Vector Machines (dt. Klassifikation basierend auf Stützvektoren)
TAN	Transaction Number (dt. Transaktionsnummer)
Weka	Waikato Environment for Knowledge Analysis (dt. Klassifikationsumgebung)

1 Einleitung

Der Fokus dieser Arbeit liegt auf der biometrischen Authentifizierung anhand des Tippverhaltens mithilfe der in Smartphones verbauten Sensoren. In der Motivation wird dargestellt, weshalb dieses Themenfeld von entscheidender Bedeutung ist. Im Anschluss daran wird das Thema von bisherigen Untersuchungsbereichen abgegrenzt und aufgezeigt, in welches Gebiet diese Forschungsarbeit einzugliedern ist. Die Zielstellung dieser Arbeit und der daraus resultierende Aufbau werden im letzten Abschnitt vorgestellt.

1.1 Motivation

Die Authentifizierung gegenüber digitalen Systemen ist heutzutage ein alltäglicher Prozess. Für eine elektronische Banküberweisung werden Kontonummer (ab 2014: International Bank Account Number (IBAN)), ein geheimes Passwort und eine einmalig verwendbare Transaction Number (TAN) benötigt; Spieler des Online-Rollenspiels „World of WarCraft“ nutzen One Time Password (OTP)-Generatoren, um ihre virtuelle Identität vor Hackern zu schützen; Anmeldungen am E-Mail-Postfach oder an einem Computer benötigen Benutzernamen und Passwort, in einigen Firmen ist darüber hinaus ein Mitarbeiterausweis notwendig. Diese Passwörter sollten einer Richtlinie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) [Bun11a] folgen, die besagt, dass ein Passwort folgende Merkmale aufweisen sollte: eine ausreichende Länge (mindestens acht Zeichen), alpha-numerisch mit Sonderzeichen und nicht im Wörterbuch stehend. Insbesondere bei der Eingabe von Passwörtern in Smartphones sollte diese Richtlinie befolgt werden, da Eingaben selten unbeobachtet durchgeführt werden können [Bun11b, S. 9]. Wenn Wörter als Passwort verwendet werden,

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_1

können sich diese schneller gemerkt werden als eine kryptische Zeichenabfolge mit Sonderzeichen. Somit muss ein Angreifer die Eingabe des Passworts mehrfach beobachten, falls ein komplexes Passwort verwendet wird.

Diese Richtlinien für Passwörter werden jedoch aufgrund von zu kurzer Personal Identification Number (PIN)/Passwort oder Standardpasswörtern (wie z. B. die Zeichenfolge 1 bis 6 oder das Wort „Passwort“) oft nicht eingehalten. Besonders durch Techniken, wie der Brute-Force-Methode, bei der alle möglichen Passwörter getestet werden, kann so in kurzer Zeit das richtige Passwort ermittelt werden. Gleichzeitig existieren Verfahren, wie z. B. Shoulder Surfing (über die Schulter schauen bei der Eingabe) oder Social Engineering (Passwort von der Person durch eine geschickte Fragetechnik erfahren [HKNT09]), mit welchen das Passwort herausgefunden werden kann.

Passwörter allein stellen somit keinen ausreichenden Sicherheitsschutz dar. Daher werden diese in vielen Firmen mit einem Mitarbeiterausweis mit integriertem Public Key Infrastructure (PKI)-Chip oder einem OTP-Generator kombiniert. Hiermit wird die Sicherheit zwar erhöht, aber das zusätzliche Gerät muss immer mitgeführt werden, wenn die Authentifizierung erfolgen soll. Wird das Gerät vergessen, ist entweder keine Authentifizierung möglich oder nur mit eingeschränktem Zugriff. Jedes zusätzliche Gerät/Karte stellt zugleich ein Platzproblem dar, wodurch die Akzeptanz der Anwender sinken kann.

Für Smartphones werden die dazu genannten Authentifizierungsmethoden nur beschränkt genutzt und meist in Form von: kurzer PIN/Passwort, ein Entsperrmuster oder gar kein Mechanismus. Doch besonders für diese Geräte sollte ein höheres Sicherheitsniveau erreicht werden, das gleichzeitig benutzerfreundlich ist. Dies zeigt z. B., dass 2009 in einem halben Jahr in Londoner Taxis 55.000 Mobiltelefone liegen gelassen wurden [Twe09]. Außerdem hat laut einer Studie des Bundesverbandes Informationswirtschaft, Telekommunikation und Neue Medien (BITKOM) bereits jeder zehnte Deutsche ab 14 Jahren sein Handy schon einmal verloren [BI12]. Zudem können sie sehr schnell und einfach gestohlen werden. Mit der zunehmenden Anzahl an Geräten (bis 2012 wurden insgesamt über eine Milliarde Smartphones

auf der Welt verkauft [Bic12]) wird diese Technologie für Kriminelle immer interessanter und kann, nachdem das Passwort einmal herausgefunden wurde, beliebig oft verwendet werden. Auf Smartphones kann bei Fettrückständen des Fingers auf dem Display durch Betrachtung der spiegelnden Oberfläche auf das Passwort geschlossen werden. Insbesondere durch die gespeicherten Daten (sensible, berufliche Informationen oder intime, private Daten [BI12]) und Zugriffe der Geräte auf entsprechende Systeme, kann ein entsperrtes Gerät in falschen Händen erheblichen Schaden anrichten.

Eine Alternative zu den Authentifizierungsgeräten bietet die Nutzung von Biometrie. Die Biometrie beschreibt das Erkennen einer Person anhand von individuellen physischen, chemischen oder verhaltensbasierten Eigenschaften [JFR08b, S. 1]. Dazu gehören u. a. die Erkennung des Benutzers auf Basis des Fingerabdrucks, aber auch die Schrift und Sprache. Vorteil der Biometrie ist, dass sie sich mit dem Benutzer bewegt und somit nicht vergessen werden oder verloren gehen kann. Nachteil ist die nicht hundertprozentige Erkennungsgenauigkeit, daher sollte zudem ein Passwort/PIN eingegeben werden. Ob PIN oder Passwort, bei beiden Authentifizierungsmethoden erfolgt die Eingabe über die Tastatur. Während der Eingabe kann eine Erkennung der Person anhand ihres Tippmusters erfolgen, was als ein biometrisches Charakteristikum definiert werden kann. Jedoch wurde dieses Verfahren bisher nur auf Computertastaturen oder Tastaturen auf einem Handy mit 12-Hardwaretasten analysiert. Für Smartphones mit kapazitivem Display (Displayart, die auf Kapazitätsänderungen reagiert – genauere Beschreibung vgl. Abschnitt 5.2.1) wurden bisher keine Studien durchgeführt. Gleichzeitig beschränkten sich die Auswertungen auf einen Klassifikator, ein Gerät und ein Szenario. Wie benutzerfreundlich und sicher dieses Verfahren ist, wurde hingegen nicht untersucht. Eine Authentifizierung mittels des Tippverhaltens und eines Passwortes kann als 2-Faktor-Authentifizierung gesehen werden und ist somit sicherer als eine 1-Faktor-Authentifizierung mittels Passwort, da nicht automatisch jeder Authentifizierungsversuch erfolgreich ist, selbst bei bekanntem Passwort.

Doch nicht nur die Authentifizierung zum Entsperren eines Gerätes muss berücksichtigt werden. Wird ein Gerät direkt nach der Authentifizierung gestohlen, dann kann diese Person ohne Authentifizierung auf das Gerät zugreifen. Für diesen Fall muss eine Lösung gefunden werden, wie in diesem Szenario eine Identifizierung der Person erfolgen kann.

1.2 Zielstellung der Arbeit

Für das Tippverhalten ergeben sich, wie für alle biometrischen Systeme, eine Reihe von Anforderungen, die das System erfüllen muss. Diese Anforderungen sind *Allgemeingültigkeit*, *Einzigartigkeit*, *Dauerhaftigkeit*, *Messbarkeit*, *Effizienz*, *Akzeptanz* und *Umgehen des Verfahrens* [PPJ03, JBP02, Cla94, IEE10].

Darüber hinaus existieren im Bereich der Smartphones weitere Anforderungen, z. B. dass die Authentifizierung geräteunabhängig, geräteübergreifend, unabhängig und universell anwendbar sein muss. Diese werden in Abschnitt 2.3.1 beschrieben.

Zusätzlich zu diesen Anforderungen muss eine Verringerung der Fehlerraten erfolgen, damit das Authentifizierungsverfahren in Bezug zur Sicherheit und Benutzerfreundlichkeit verbessert wird.

Das Hauptziel dieser Arbeit ist die Prüfung der Authentifizierung mittels des Tippverhaltens auf Smartphones. Damit diese Erkennung durchgeführt werden kann, müssen durch die vorliegende Arbeit die folgenden vier Ziele, die sich aus den Anforderungen ergeben, erreicht werden:

- Es muss eine hohe Sicherheit durch das Verfahren gewährleistet werden, sodass nicht mehr als 3,9 % der Angriffe bei bekanntem Passwort erfolgreich sind. Gleichzeitig darf einem echten Benutzer nur in weniger als 3,9 % der Versuche der Zugriff verweigert werden. Der Wert 3,9 % basiert auf einer in einer skandinavischen Bank eingesetzten Methode [Beh13a], welche im Vergleich zu anderen durchgeführten Untersuchungen (siehe Abschnitt 3.1.1) eine geringe Fehlerrate aufweist und gleichzeitig in der Praxis eingesetzt wird.

- Verschiedene Geräte besitzen Sensoren, die Daten in unterschiedlicher Qualität aufnehmen. Diese Qualitätsunterschiede dürfen die Fehlerraten nicht negativ beeinflussen, sodass keine Authentifizierung mehr möglich ist. Falls doch eine Authentifizierung auf unterschiedlichen Geräten durchführbar sein soll, stellt sich die Frage (die beantwortet werden muss), ob die Merkmalseigenschaften auf ein anderes Gerät übertragen werden können (geräteübergreifende Authentifizierung), ohne dass ein Einfluss auf die Fehlerraten erkennbar ist.

- Das Authentifizierungsverfahren soll nicht nur in klinischen Szenarien (die keine Praxisrelevanz besitzen), z. B. nur im Sitzen, verwendbar sein, sondern auch in verschiedenen Alltagssituationen (u. a. im Gehen oder Stehen), ohne dass sich die Fehlerraten über den Wert 3,9 % vergrößern.

- Es muss ein System für die kontinuierliche Überprüfung des Benutzers des Smartphones generiert werden, welches implizit und transparent agiert. Es soll gezeigt werden, ob biometrische Authentifizierungsverfahren genutzt werden können, die Personen auch während der Nutzung überprüfen. Dabei soll die Fehlerrate unter 7,0 % liegen, die durch ein textunabhängiges Verfahren bereits an Telefonen mit einer Hardwaretastatur erreicht wurde (siehe Abschnitt 3.1.1). Ohne ein solches Verfahren ist die Sicherheit nach der initialen Authentifizierung nicht mehr gegeben. Zusätzlich muss das Lernverhalten betrachtet werden, welches im Laufe der Zeit das Tippverhalten verändert. Es muss geprüft werden, ob das Modell mit den Merkmalen einer Person dauerhaft angepasst werden muss.

1.3 Rahmenbedingungen und Einschränkungen

Neben den Zielen gibt es für die reale Nutzung weitere zu analysierende Punkte, die jedoch in dieser Arbeit nicht betrachtet werden:

Rechtliche Grundlagen: Die Dissertation soll die wissenschaftliche und technische Durchführbarkeit eines solchen Verfahrens darstellen.

Daher wird auf die rechtlichen Grundlagen, insbesondere das Speichern von personenbezogenen Daten, nicht eingegangen. Dies stellt ein allgemeines Problem aller biometrischer Verfahren dar und muss an anderer Stelle verallgemeinert betrachtet werden.

Akzeptanz des Verfahrens: Die Akzeptanz gegenüber dem Verfahren wird nicht betrachtet. Es wird vom Einverständnis der betreffenden Personen ausgegangen, ihr Tippverhalten aufzunehmen. Zudem kann z. B. die Nutzung von der Leitung eines Unternehmens vorgeschrieben werden (Corporate Environment), eine persönliche Akzeptanz ist dann für die Nutzung nicht Voraussetzung.

Angriffsmodalitäten: Angriffsmodalitäten, die auf Schnittstellen zu anderen Bereichen (z. B. Benutzeroberfläche oder Datenbank) basieren, wurden bereits bei mehreren biometrischen Authentifizierungsverfahren analysiert [JNN08]. Daher werden die Schnittstellen in dieser Arbeit nicht weiter adressiert.

Lauffähiges Design auf dem Smartphone: Die Arbeit stellt ein Konzept mit teil-automatisierten Prozessen dar. Es sollen lediglich Funktionsweisen verglichen und bewertet werden. Die Entwicklung eines lauffähigen Prototyps ist nicht angedacht.

Weitere Sicherheitsmechanismen: Antivirus-Software bzw. gehärtete Betriebssysteme sind neben der Authentifizierung essentiell für die Sicherheit von Smartphones wichtig, stehen aber nicht im Fokus dieser Arbeit.

1.4 Struktur der Arbeit

Die nachfolgende Abbildung 1.1 stellt den strukturellen Aufbau der vorliegenden Arbeit dar.

Die Heranführung an das Thema ist im Rahmen der Motivation und der Abgrenzung des Untersuchungsbereiches sowie der Einordnung der Forschungsarbeit in Kapitel 1 gegeben. Um die dort präsentierten

Zielstellungen zu erreichen, werden im zweiten Kapitel die Grundlagen für die Thematik definiert. Dazu zählen Aspekte aus der Information Technology (IT)-Sicherheit, biometrische Lösungen sowie allgemeine Anforderungen an ein Authentifizierungssystem. Zu diesem Wissen wird in Kapitel 3 der Stand der Forschung bezüglich Authentifizierungssystemen an Smartphones hinzugefügt. Das beinhaltet sowohl das Tippverhalten als auch die Bewegungserkennungen.

Damit die Algorithmen getestet und die vorgestellten Ziele überprüft werden können, wurden neun Studien durchgeführt, deren Vorstellung in Kapitel 4 erfolgt. Zusätzlich werden die deskriptiven Daten der Personen und die in den Studien verwendeten Geräte genannt. Gleichzeitig erfolgt eine Betrachtung des grundlegenden Konzeptes der Applikationen und des generellen Aufbaus der Studie.

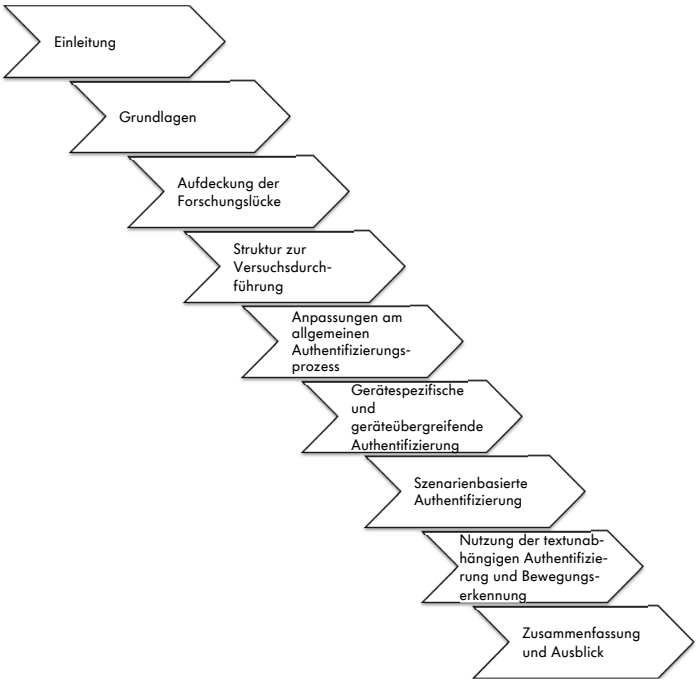


Abbildung 1.1: Strukturelle Vorgehensweise innerhalb der Arbeit

In den folgenden vier Kapiteln werden die einzelnen Ziele genauer betrachtet. Zunächst erfolgt in jedem Kapitel eine genaue Zielstellung, danach werden die Konzepte definiert und im Anschluss durch Studien nachgewiesen. Es werden bestehende Algorithmen verglichen, neu kombiniert und entwickelt. Der abschließende Bereich der Kapitel stellt eine Bewertung der Zielerreichung dar. Kapitel 5 fokussiert die allgemeinen Herausforderungen in der Umgebung eines Smartphones und welche Verbesserungen durchgeführt werden können. In Kapitel 6 erfolgt die Analyse der gerätespezifischen Authentifizierung und in Kapitel 7 die szenarienübergreifende Authentifizierung mit unterschiedlichen Szenarien. Das vierte Ziel wird in Kapitel 8 dargestellt. Dort wird auf ein Konzept für ein Re-Authentifizierungssystem, das kontinuierlich die Identität überprüft, eingegangen. Dazu erfolgen zusätzlich zur textabhängigen Authentifizierung eine textunabhängige Authentifizierung und eine Bewegungserkennung. Gleichzeitig wird das Vertrauensmodell für die Re-Authentifizierung auf ihre Durchführbarkeit analysiert.

Das Kapitel 9 fasst die Ergebnisse zusammen und zeigt einen Ausblick für zukünftige Arbeiten auf. Allgemeine Limitationen und Nutzen für die Algorithmen bzw. die Studien werden zusätzlich gegeben.

2 Grundlagen des Aufgabenfeldes

Die vorliegende Dissertation beschäftigt sich mit der biometrischen Authentifizierung. Deshalb müssen sowohl Grundlagen zur IT-Sicherheit als auch zur Authentifizierung und Biometrie definiert werden. Im Anschluss wird auf multi-biometrische Verfahren und deren Fusion sowie auf die allgemeinen Probleme bei der biometrischen Authentifizierung eingegangen. Das neue Umfeld von Smartphones bietet mit deren weiterentwickelten Sensoren eine Perspektive im Bereich der Sicherheit, welche aufgezeigt wird.

2.1 Sicherheit und Sicherheitsaspekte

Der deutsche Begriff „Sicherheit“ hat zwei verschiedene Bedeutungen. Zum einen handelt es sich dabei um die Sicherheit von Personen (auch bezeichnet als physische Sicherheit). Im Englischen wird dafür das Wort *safety* mit der Bedeutung verwendet, dass zumeist keine böswilligen Angriffe auf den Menschen beinhaltet sind. Beispielsweise ist von *safety* die Rede, wenn in einem Chemielabor eine Gewährleistung gegeben wird, dass keine Chemikalien auslaufen.

Zum anderen kann der englische Begriff *security* gemeint sein, womit der Schutz vor böswilligen Angriffen bezeichnet wird. Dazu zählen Diebstähle, Zerstörung und andere Delikte. Am Beispiel des Chemielabors würde die *security* die Sicherheit in Bezug auf den Diebstahl von Chemikalien bedeuten [Tro11].

In dieser Dissertation ist bei der Verwendung des Begriffs Sicherheit immer die Bedeutung der *security* gemeint.

Es werden drei verschiedene Sicherheitsaspekte betrachtet (laut National Institute of Standards and Technology (NIST) 800-33 [Sto01]):

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_2

die *Verfügbarkeit*, die *Integrität* und die *Vertraulichkeit*. Diese werden im Folgenden genauer beschrieben:

Verfügbarkeit: Verfügbarkeit meint, dass Informationen nutzbar sind, wenn sie benötigt werden. Je nach System können dabei die Anforderungen an ein System variieren. Oft ist entscheidend, wie stark bei Firmen das System in das operative Geschäft eingebunden ist [Rae01].

Integrität: Integrität ist das Schützen der Daten gegen beabsichtigte oder zufällige Manipulationen [Rae01]. Während der Datenübertragung kann es unter anderem zu böswilligen Attacken kommen. Durch Generierung von Hashwerten (Prüfsumme mit einer festen Länge) ist eine Überprüfung möglich, ob die Daten verändert wurden, wobei nicht rückwirkend auf die Nachricht geschlossen werden kann.

Vertraulichkeit: Der Begriff beschreibt, dass „nur diejenigen Personen (und Systeme) Kenntnisse von dem Inhalt der Daten erhalten, die dazu befugt sind“ (vgl. [SR05]). In diesem Zusammenhang werden nicht nur sensible Benutzerdaten verstanden, sondern auch Datenbanken oder Dokumente, die der betreffenden Person oder Firma Schaden bringen können, wenn diese in die Hände von Unbefugten geraten.

Darüber hinaus werden in einem erweiterten Modell die Aspekte *Authentifizierung* und *Verbindlichkeit* hinzugenommen [QTKJ08]. Die *Verbindlichkeit* gibt an, dass eine Person nicht abstreiten kann, dass sich ein Vorfall ereignet hat. Auf die Authentifizierung wird in den nächsten Abschnitten im Bereich des Identitätsmanagements weiter eingegangen.

2.2 Identitätsmanagement

Bei dem Identitätsmanagement geht es um das Organisieren von Personen und deren Zugriff auf Objekte. Diese Zugriffe werden im Folgenden

genauer definiert, bevor anschließend direkt auf den Teilprozess der Authentifizierung eingegangen wird.

2.2.1 Zugriff auf Objekte

Das Identitätsmanagement für den Zugriff auf Objekte besteht aus vier verschiedenen Phasen. Diese werden in Abbildung 2.1 mit ihrer Reihenfolge dargestellt und im Anschluss detailliert beschrieben.

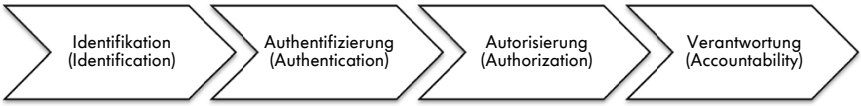


Abbildung 2.1: Prozess: Zugriff auf ein Objekt (nach [Har10, S. 157])

Identifizierung: Bei dem Prozess der Identifizierung gibt eine Person mit Informationen an (z. B. Benutzername oder Benutzer-ID), um wen es sich handelt [Har10].

Authentifizierung: Bei dem zweiten Schritt, der Authentifizierung, wird systemseitig überprüft, ob es sich wirklich um die Person handelt, für die sie sich ausgibt. Dafür können verschiedene Authentifizierungsfaktoren verwendet werden (siehe Abschnitt 2.2.2).

Autorisierung: Nach der Authentifizierung kennt das System die Person, die das System bedient. Möchte diese Person Zugriff auf ein Objekt erhalten, muss überprüft werden, ob sie die Berechtigung besitzt.

Verantwortung: Sämtliche Zugriffe müssen vom System protokolliert werden. So kann immer nachgewiesen werden, welche Aktivitäten von einer Person mit bestimmten Objekten durchgeführt wurden.

In der Biometrie werden die beiden ersten Phasen durch ein anderes Konzept zusammengefasst. Dabei erfolgt die Differenzierung zwischen Verifikation und Identifikation [JFR08a, S. 6].

Bei der Verifikation wird anhand von Informationen über die Person und den Authentifizierungsfaktor entschieden, ob es sich um eine bestimmte Person handelt oder nicht. Hierbei wird nur verglichen, ob die Person zu dem Faktor passt [JFR08b].

Dem gegenüber steht die Identifikation, bei der versucht wird, die biometrischen Eigenschaften einer Person mit allen gespeicherten Modellen zu vergleichen. Die Identität, die am besten zu den biometrischen Daten passt, wird im weiteren Verlauf verwendet. Einige biometrische Verfahren können jedoch nicht zur Identifikation verwendet werden, da die Unterschiede zwischen den Merkmalen mehrerer Personen nicht ausreichend sind. Dazu zählt u. a. der Handabdruck [Rob06]. In diesem Fall kann nur eine Verifikation stattfinden.

2.2.2 Authentifizierungsfaktoren

In der Authentifizierung werden drei Faktoren (Wissen, Besitz und Biometrie) unterschieden [Har10]. Zur Authentifizierung kann sowohl ein Faktor allein genutzt werden als auch verschiedene Kombinationen der unterschiedlichen Faktoren. Dabei müssen alle verwendeten Faktoren vorhanden sein. Die einzelnen Faktoren werden wie folgt definiert:

Faktor WISSEN („was ich weiß“): Die am weitesten verbreitete Methode zur Authentifizierung ist der Faktor Wissen. Neben dem Benutzernamen können u. a. die PIN oder das Passwort, aber auch das Zeichnen einer vorher bestimmten Geste genutzt werden. Nur die entsprechende Person darf Kenntnis über das Passwort haben.

Es gibt verschiedene Techniken, mit denen ein Passwort ermittelt werden kann. Hierzu zählen u. a. Social Engineering (Technik zur zwischenmenschlichen Beeinflussung/Kommunikation, wodurch unwissend das Passwort an Unbefugte verraten wird) oder Brute-Force-Attacken (alle Passwörter nacheinander ausprobieren), die entsprechende Gegenmaßnahmen notwendig machen, wie z. B. das Sperren eines Nutzerkontos nach mehrmaliger falscher Eingabe. Social Engineering kann nur durch geeignete Sensibilisierungsmaßnahmen

verhindert werden. Brute-Force-Attacken hingegen können nicht verhindert werden. Es ist nur möglich ein komplexes Passwort mit ausreichender Länge (in der ISO/IEC 27001 von International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC) wird ein alpha-numerisches Passwort mit einer Länge von acht Zeichen vorgeschrieben [II05]) zu nutzen oder ein Sperren des Benutzerkontos nach drei Fehlversuchen zu erzwingen. Die Begründung hierfür liegt in der großen Zeitspanne bis zum Erhalt des Passwortes (Berechnungsdauer), sodass der Versuch aus Rentabilität vom Angreifer eingestellt wird. Gleichzeitig sollte das Passwort innerhalb einer bestimmten Zeit neu gesetzt (vgl. [Bun11a]) und für verschiedene Systeme unterschiedliche Passwörter verwendet werden. Damit kann sich ein Angreifer, der zu einem System Zugriff hat, nicht dauerhaft bei diesem oder anderen Systemen authentifizieren.

Faktor BESITZ („was ich besitze“): Der Faktor Besitz bezeichnet die Methode, dass sich eine Person mit einem physischen Objekt authentifiziert. Das kann sowohl eine Smartcard, wie eine Kreditkarte oder ein Firmenausweis mittels einer PKI, als auch ein Generator für OTP sein.

Ein großer Nachteil ist, dass bei dem Verfahren der Besitz immer während der Authentifizierung gegeben sein muss. Wenn er gestohlen wird oder verloren geht, kann sich die Person nicht mehr authentifizieren. Damit eine unbefugte Person, die in den Besitz des Mediums gekommen ist, sich nicht sofort authentifizieren kann, wird oft eine Kombination des Faktor Wissens mit dem Faktor Besitz genutzt.

Faktor BIOMETRIE („wer ich bin“): Die Biometrie beschreibt das Erkennen einer Person anhand von individuellen physischen, chemischen oder verhaltensbasierten Eigenschaften [JFR08b, S. 1]. Im Gegensatz zum Faktor Besitz kann die Biometrie nicht verloren, gestohlen oder vergessen werden [DG04, S. 185]. Aufgrund dessen, dass sie sich immer bei dem Benutzer befindet, ist das Verfahren überall einsetzbar. Die bekanntesten Verfahren sind Fingerabdruck und Gesichtserkennung [Rob06], die als biometrische Faktoren über

Sensoren aufgenommen werden. Im Falle eines Smartphones ist es dabei möglich, die eingebaute Hardware zu benutzen, sodass keine weiteren Geräte notwendig sind [KAK11, S. 1572]. Auf die Nachteile (u. a. die existierenden Fehlerkennungen) wird in Abschnitt 2.6 eingegangen.

Es ist erkennbar, dass kein Faktor für sich allein gestellt ausreichend ist. Daher wird für Smartphones eine geeignete Kombination in dieser Arbeit vorgestellt. Die generellen Anforderungen an dieses System werden im folgenden Abschnitt definiert.

2.3 Qualitätsanforderungen und -kriterien

Für die biometrische Authentifizierung müssen eine Reihe von Qualitätsanforderungen eingehalten werden, damit die Systemsicherheit gewährleistet ist. Diese werden im Folgenden zunächst definiert. Im Anschluss daran werden Kriterien vorgestellt, die es ermöglichen, verschiedene Ergebnisse bzw. Studien miteinander zu vergleichen, welche besser geeignet sind.

2.3.1 Anforderungen an die Systemsicherheit

Die Systemsicherheit ist im weitesten Sinne an die Anforderungen der biometrischen Authentifizierungsmethode gekoppelt. Allgemein existiert eine Vielzahl von verschiedenen Anforderungen, die ein Authentifizierungssystem erfüllen muss. In der Literatur werden sieben Anforderungen definiert, die zueinander disjunkt sind. Diese werden in dem ersten Abschnitt beschrieben. Danach folgen weitere notwendige Aspekte, die durch das Umfeld mit Smartphones und Tablets existieren.

In unterschiedlichen wissenschaftlichen Artikeln wurde eine Reihe von Anforderungen definiert, die ein biometrisches Verfahren haben sollte. Das sind: *Allgemeingültigkeit*, *Einzigartigkeit*, *Dauerhaftigkeit*, *Messbarkeit*, *Effizienz*, *Akzeptanz* und *Umgehen des Verfahrens* [PPJ03, JBP02, Cla94, IEE10]. Die sieben Anforderungen werden im

Folgenden detailliert beschrieben, um sie voneinander abzugrenzen (vgl. [JBP02]). Es ist dabei zu beachten, dass jedes biometrische Merkmal verwendet werden kann, welches ein physiologisches Muster oder Verhaltensmuster aufweist (siehe Abschnitt 2.4.2).

Allgemeingültigkeit: Die Eigenschaft einer Person sollte generell bei allen Personen existieren [JBP02]. Wenn nur eine geringe Anzahl an Personen das Verfahren nutzen kann, ist das Verfahren nicht einsetzbar. Einige Merkmale sind in verschiedenen religiösen Kulturkreisen nicht möglich zu extrahieren, z. B. verhindert eine Verschleierung, bei der nur die Augen erkennbar sind, eine Gesichtserkennung.

Einzigartigkeit: Die Charakteristik sollte über ausreichend individuelle Eigenschaften in der Bevölkerung verfügen [JBP02]. Dabei muss eine Person an den Charakteristiken eindeutig erkennbar sein und gleiche Merkmalskombinationen nicht für mehrere Personen existieren, damit Personen besser auseinander gehalten werden können [DG04, S. 185].

Dauerhaftigkeit: Die Eigenschaft sollte konstant über den Zeitraum aller Authentifizierungen sein [PPJ03]. Wenn sich ein Merkmal über die Zeit stark verändert, ist es als biometrische Eigenschaft ungeeignet. Dazu zählen unter anderem Alterserscheinungen beim Menschen, die Merkmale verändern und die Authentifizierung ohne Anpassung des Referenzmodells über einen längeren Zeitraum erschweren.

Messbarkeit: Das biometrische Verhalten sollte aufnehmbar und digitalisierbar sein [RNJ06, S. 19]. Weiterhin muss es möglich sein, aus dem Verhalten geeignete Merkmale zu extrahieren, wobei diese quantitativ messbar sein sollten [TM12].

Effizienz: Die Erkennungsgenauigkeit mit den dafür erforderlichen Ressourcen, um diese Genauigkeit zu erreichen, sollte den Einschränkungen durch die Umgebung gerecht werden.

Akzeptanz: Personen, die die Anwendung nutzen sollen, müssen ihre Einwilligung zur Verwendung des Verfahrens geben. Gleichzeitig

benötigen die Nutzer genaue Informationen über das Verfahren. Die Akzeptanz eines Verfahrens ist ebenso aus der Sicht des Anwenders von der Dauer der Erkennung abhängig. Einige Erkennungsprozesse benötigen mehrere Stunden [Che03]. Das ist eine nicht akzeptable Authentifizierungsmethode und würde von jeder Person abgelehnt werden. Teilweise gibt es aber auch Vorschriften, dass eine Person das Verfahren nutzen muss (z. B. weil sie sonst nicht auf das Betriebsgelände oder in das Flugzeug gelangt).

Umgehen des Verfahrens: Die Eigenschaften einer Person sollten schwer zu imitieren sein (z. B. das Nachstellen des Fingerabdrucks) [JBP02].

Darüber hinaus existieren noch weitere Anforderungen, die aber nur bei Clarke [Cla94] definiert werden und teilweise überlappend mit den vorher definierten sind: *Unentbehrlichkeit* (die Kennung sollte eine oder mehrere natürliche Eigenschaften besitzen, die jeder Mensch besitzt und behält – ähnlich zu Allgemeingültigkeit), *Lagerfähigkeit* (die Merkmale sollten in manuellen und automatisierten Systemen speicherbar sein), *Uneingeschränktheit* (keine andere Form der Identifizierung sollte zusätzlich erforderlich sein), *Präzision* (jede Kennung sollte ausreichend anders sein als jede andere, sodass Fehler unwahrscheinlich sind – analog Einzigartigkeit), *Bequemlichkeit* (Messung und Speicherung der Identifizierung sollte nicht unnötig umständlich oder zeitaufwendig sein), *Einfachheit* (Aufzeichnung und Übertragung sollte einfach und nicht fehleranfällig sein) und *Kosten* (Messen und Speichern der Merkmale sollte nicht übermäßig teuer sein).

Die in Abschnitt 1.1 vorgestellten Anforderung für die Authentifizierung am Smartphone (geräteunabhängig, geräteübergreifend, unabhängig und universell anwendbar) werden im Folgenden genauer beschrieben:

Transparenz: Eine Authentifizierung ist ein Sicherheitsmechanismus, der in vielen Fällen eine Interaktion des Benutzers notwendig macht. Um die Sicherheit zu erhöhen, werden zusätzliche Authentifizierungsmechanismen benötigt. Deshalb müssen diese Mechanismen

transparent sein, sodass Ablenkungen reduziert werden und der Nutzer nicht gestört wird. Die Authentifizierung muss daher implizit sein, z. B. im Hintergrund laufen (analog zu der von Clarke definierten Anforderung *Bequemlichkeit* [Cla94]).

Kontinuität: Die Sicherheit muss während der gesamten Nutzung gewährleistet sein und nicht nur zum Zeitpunkt der initialen Authentifizierung [TM12]. Die initiale Authentifizierung stellt das Entsperren eines Gerätes dar.

Geräteunabhängigkeit: Aktuell existieren diverse mobile Endgeräte (siehe Abschnitt 4.2 und Abschnitt 6.1) mit unterschiedlichen Sensoren. Wichtig ist daher, dass eine Authentifizierung generell funktioniert, unabhängig davon, welches Gerät verwendet wird. Bisherige Studien beruhen auf nur einem Authentifizierungsgerät. Ein Vergleich der Algorithmen in Bezug auf unterschiedliche Geräte wurde noch nicht durchgeführt.

Geräteübergreifend: Durch die Existenz einer Vielzahl von Gerätetypen ist gleichzeitig gegeben, dass ein Gerät häufig gewechselt wird oder ein Nutzer mehrere Geräte verwendet, z. B. ein Smartphone und ein Tablet oder mehrere Smartphones. In diesem Fall müsste auf jedem Gerät am Anfang ein Training/Enrolment eines benutzerspezifischen Modells durchgeführt werden. Somit wird ein Modell des Benutzers von jedem Gerät neu angelernt. Aus diesem Grund ist es sinnvoll, dass nur ein Enrolment notwendig ist, welches ein Modell erzeugt, das von sämtlichen Geräten verstanden und verwendet wird.

Unabhängigkeit: Es ist relevant, dass keine Zusatzgeräte benötigt werden. Diese würden die Benutzerfreundlichkeit negativ beeinflussen.

Universell: Mobile Endgeräte werden über den ganzen Tag verteilt genutzt. Daher muss die Authentifizierung in jeglichen Situationen anwendbar sein.

2.3.2 Vergleichsraten

Biometrische Verfahren sind nicht exakt, darum werden verschiedene Fehlerraten verwendet, um unterschiedliche Studien bzw. Experimente miteinander vergleichen zu können. Je kleiner diese Fehlerraten sind, desto genauer ist ein Verfahren. Diese Maße werden in dem Abschnitt vorgestellt: False Acceptance Rate (FAR), False Rejection Rate (FRR) und Equal Error Rate (EER). Diese Fehlerraten sind in Abbildung 2.2 zu erkennen und werden im Folgenden genauer definiert.

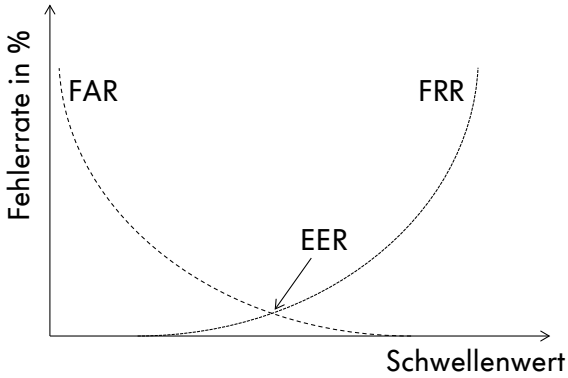


Abbildung 2.2: Zusammenhang unterschiedlicher Fehlerraten

Als Schwellenwert wird die Grenze von Merkmalen bezeichnet, die erreicht werden muss, damit eine Person erkannt wird. Je geringer der Schwellenwert ist, desto mehr Personen werden falsch erkannt. Ein höherer Wert begrenzt die Anzahl an korrekten Authentifizierungen der eigentlichen Person. Viele Verfahren berechnen dafür einen numerischen Wert für die Übereinstimmung des aktuell aufgenommenen und gespeicherten Merkmals. Somit wird mit dem konfigurierbaren Schwellenwert bestimmt, wie stark das Maß der Übereinstimmung sein muss, um als gleiche Person zu gelten. Die Wahl des Schwellenwertes hat gegenläufige Konsequenzen für FAR und FRR, daher muss ein Kompromiss gefunden werden.

False Acceptance Rate (FAR): Die FAR gibt die Wahrscheinlichkeit an, wie viele Angreifer sich an dem System anmelden können (siehe Formel 2.1). Deshalb ist diese Fehlerrate ein Maß für die Sicherheit des Systems.

$$FAR = \frac{\text{Anzahl an falsch akzeptierten Personen}}{\text{Anzahl aller Anmeldeversuche unautorisierter Personen}} \tag{2.1}$$

Je mehr Angreifer sich authentifizieren können, desto größer wird die FAR. Diese liegt zwischen 0 % und 100 %.

False Rejection Rate (FRR): Genau wie die FAR ist auch die FRR eine Fehlerrate, die bei der Authentifizierung zur Aussage der Qualität eines Verfahrens verwendet wird. Im Gegensatz zur FAR wird bei der FRR angegeben, wie viele Personen abgewiesen wurden, obwohl sie die korrekten Personen sind (siehe Formel 2.2). Diese Fehlerrate repräsentiert Informationen über die Benutzerfreundlichkeit des Systems.

$$FRR = \frac{\text{Anzahl an falsch zurückgewiesenen Personen}}{\text{Anzahl aller Anmeldungen von autorisierten Personen}} \tag{2.2}$$

Equal Error Rate (EER): Sowohl FAR als auch FRR hängen von dem Schwellenwert ab (siehe Abbildung 2.2). Der Punkt, an dem sich beide Graphen schneiden, wird als EER bezeichnet. Oft wird diese EER zum Vergleich von Studien herangezogen. Doch werden Authentifizierungssysteme meist in eine Richtung (entweder Sicherheit oder Benutzerfreundlichkeit) ausgerichtet, sodass der Schwellenwert diesbezüglich angepasst werden muss.

Des Weiteren wird der Begriff Akzeptanzrate (Erkennungsrate) verwendet, der vergleicht, wie viel Prozent der Personen richtig authentifiziert wurde:

$$Akzeptanzrate = \frac{\text{Anzahl an falschen Entscheidungen}}{\text{Gesamtanzahl aller Anmeldungen}} \tag{2.3}$$

Wie in Formel 2.3 dargestellt (vgl. [SZ09] wird das Verhältnis zwischen falschen Entscheidungen (falsch akzeptierten bzw. zurückgewiesenen Personen) zu allen Entscheidungen verglichen. Diese Rate kann irreführend sein, da eine hohe FRR (70 %) und eine geringe FAR (0,5 %) eine Akzeptanzrate von 98 % erreichen können. Dennoch ist dieses System benutzerunfreundlich, da nur in 3 von 10 Fällen eine Person richtigerweise erkannt wird. Konkret hängt dieser Wert immer von der Anzahl der Probanden in der Studie ab, wie in Abbildung 2.3 zu erkennen ist.

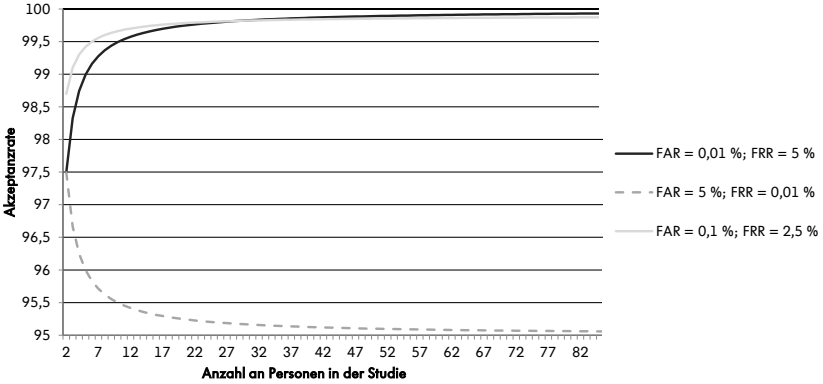


Abbildung 2.3: Die Akzeptanzrate für drei verschiedene Konfigurationen

Die Akzeptanzrate steigt bei 100 Personen im Fall einer FAR von 0,01 % und einer FRR von 5,00 % auf über 99,94 %. Schon bei 6 Personen liegt die Rate bei über 99,00 %. Dagegen sinkt die Akzeptanzrate bei größerer FAR im Verhältnis zur FRR mit steigender Probandenzahl. In dieser Arbeit wird die Akzeptanzrate nicht für das Tippverhalten verwendet.

2.4 Bestandteile der Authentifizierung mittels Biometrie

Dieser Abschnitt beschäftigt sich mit dem allgemeinen Aufbau der biometrischen Authentifizierung. Dazu werden zuerst die zwei Phasen im Authentifizierungsprozess vorgestellt. Im Anschluss werden die unterschiedlichen Authentifizierungsmodalitäten beschrieben. Als Letztes wird auf das Konzept einer Fusion von biometrischen Methoden eingegangen.

2.4.1 Prozess während der Authentifizierung

Es existieren im kompletten Authentifizierungsverlauf zwei unterschiedliche Phasen. In der ersten Phase werden Referenzmerkmale von einer Person in der Datenbank gespeichert. Diese Phase wird als *Enrolment* bezeichnet. In der zweiten Phase wird die Person authentifiziert, damit sie den Zugriff zu einem System erhält (*Authentifizierung*). Beide Phasen bestehen aus mehreren Schritten, die in Abbildung 2.4 dargestellt sind.

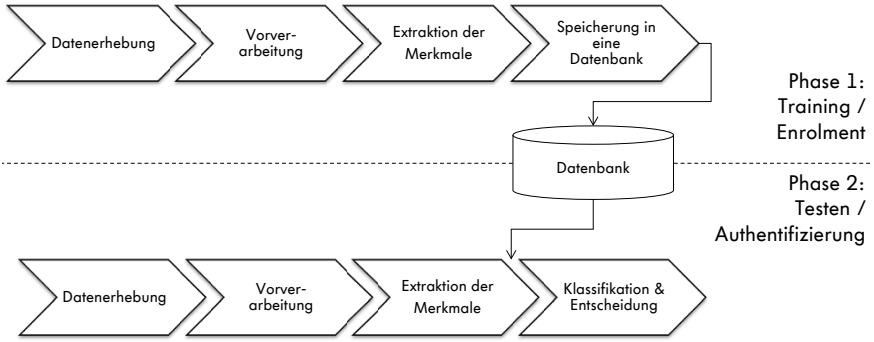


Abbildung 2.4: Ablauf des Authentifizierungsprozesses (nach [KAK11, S. 1566])

Abbildung 2.4 zeigt, dass sowohl bei dem Enrolment als auch der eigentlichen Authentifizierung (Verifizierung oder Identifizierung) drei

Schritte existieren, die während beider Phasen ausgeführt werden. Dazu zählen die Datenerhebung, Vorverarbeitung und die Extraktion der Merkmale [DG04, S. 185]. Anschließend erfolgen bei dem Enrolment eine Speicherung der Daten sowie eines Benutzermodells in einer Datenbank und bei der Authentifizierung eine Klassifikation und Entscheidung. Die Beschreibung der einzelnen Schritte wird im Folgenden vorgenommen.

Datenerhebung: Bei der Datenerhebung müssen entsprechende Sensoren verwendet werden, um die biometrischen Daten zu extrahieren [JFR08a, S. 3–4]. Bei dem Tippverhalten werden z. B. Datenströme von der Tastatur (Hardware oder virtuell) aufgezeichnet und als ein Datenstrom von unterschiedlichen Ereignissen gespeichert. Diese Rohdaten werden bereits in einer Datenbank abgelegt.

Vorverarbeitung: Die Daten werden nicht immer in der gleichen Qualität von den Sensoren aufgenommen. So können Einflüsse aus der Umwelt qualitätsmindernd wirken. Bei der Gesichtserkennung kann dies z. B. zu geringe Lichtintensität oder Kontrast sein. Diese Nebeneffekte müssen vor dem Extrahieren der Daten entfernt werden, um einen besseren Vergleich zu ermöglichen. Wenn die Qualität der Daten zu gering ist, muss der Benutzer unter Umständen sein biometrisches Merkmal erneut eingeben [JFR08a, S. 3–4].

Extraktion der Merkmale: Die Extraktion von Merkmalen stellt die Generierung von Eigenschaften aus den Daten und einen zentralen Punkt während des Authentifizierungsprozesses dar, da die Fehlerraten stark von der geeigneten Auswahl der Merkmale abhängen [TO12]. Daher wird im Abschnitt 5.2.3 genauer auf diese Merkmale eingegangen.

Generierung eines Nutzermodells (beim Enrolment): Biometrische Charakteristiken sind nicht immer identisch, wodurch bei dem Enrolment mehrere Wiederholungen der Eingabe vorgenommen werden müssen. Aus diesen Wiederholungen wird ein Modell erzeugt (um Ausreißer zu extrahieren), mit dem die späteren Authentifizierungsversuche verglichen werden. Diese Daten werden im Anschluss in der

Datenbank oder Datei gespeichert. Von Benutzern wird eine Zeit von bis zu zwei Minuten für ein Enrolment (Eingabe bis zur Speicherung der Daten) als akzeptabel empfunden [Olz06, S. 4].

Klassifikation & Entscheidung (bei der Authentifizierung): Bei der Klassifikation für die biometrische Authentifizierung handelt es sich um eine Funktion, die einem Objekt eine Klasse aus einer Menge zuordnet. Diese Menge wird durch Modelle einzelner Personen dargestellt, die während des Enrolments trainiert wurden. Anhand dieser Klassifizierung wird entschieden, ob die Person den Zugriff erhält oder abgewiesen wird.

Bestehende Studien nutzen vor allem neuronale Netze oder statistische Klassifikatoren (siehe Abschnitt 3.1.1).

Statistische Klassifikatoren: Der relativ einfache Ansatz einer statistischen Klassifikation führt zu einer häufigen Verwendung dieser Klassifikationsmethode bei Studien [UW85, LW88, BC08]. Hierbei wird ein Distanzmaß zwischen einem bekannten und einem unbekannten Datensatz erzeugt, bei dem die unbekannte Datenmenge dem Datensatz mit dem geringsten Distanzunterschied zugeordnet wird. Hierzu werden die k-Nearest-Neighbor (kNN) gesucht. Die k Klassen, die am nächsten zu dem unbekannten Datensatz stehen, werden nach ihrer Entfernung sortiert und mit einer Zugehörigkeitswahrscheinlichkeit versehen. Häufig verwendete Distanzmaße in den genannten Studien (Darstellung in Abbildung 2.5) sind die euklidische Distanz (h = 2) oder Manhattan-Distanz (h = 1), deren Berechnung in Formel 2.4 verdeutlicht wird (x und y stellen die zu vergleichenden Vektoren dar).

$$d_h(\vec{x}, \vec{y}) = \left(\sum_{i=1}^{n} (x_i - y_i)^h \right)^{\frac{1}{h}} \tag{2.4}$$

Der geringe Berechnungsaufwand des statistischen Klassifikators erlaubt es, diesen Klassifikator auf einem Smartphone zu verwenden

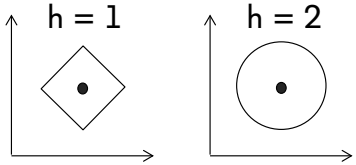


Abbildung 2.5: Darstellung verschiedener Abstandsfunktionen [BKKN03, S. 77]

[BC08, S. 7]. Das gilt sowohl für das Enrolment (Generierung des Modells) als auch für die eigentliche Verifizierung.

Neuronales Netz: Ein künstliches neuronales Netz ist ein mathematisches Modell adaptiert vom biologischen Konzept der neuronalen Netze [BKKN03, S. 8]. Das Netz besteht aus einzelnen Neuronen/ Schwellenwertelementen (grafisch: Knotenpunkte), die mithilfe von gewichteten (w_1 bis w_n) Eingangsleitungen einen spezifischen Schwellenwert überschreiten müssen (siehe Abbildung 2.6).

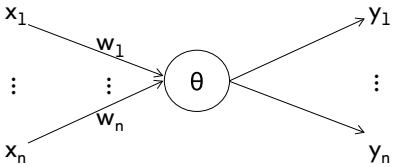


Abbildung 2.6: Schwellenwertelement bei neuronalen Netzen (angelehnt an [BKKN03, S. 9])

Wenn der Schwellenwert θ überschritten wird, wird eine 1 über die Ausgangsleitungen weitergeleitet (siehe Formel 2.5 (angelehnt an [BKKN03, S. 8])). Das gesamte Netz besteht aus mehreren miteinander verbundenen Knotenpunkten. Im weiteren Verlauf dieser Arbeit wird das künstliche Netz als neuronales Netz bezeichnet.

$$y_{1..n} = \begin{cases} 1, & wenn\ \theta \leq \sum_{i=1}^{n}(x_i * w_i) \\ 0, & sonst \end{cases} \tag{2.5}$$

Ein neuronales Netz basiert auf verschiedenen Schichten bzw. Layern, die aus einem oder mehreren Neuronen bestehen. Diese können wie folgt klassifiziert werden: eine Eingabeschicht (Neuronen, die Informationen aus der Umwelt aufnehmen), eine Ausgabeschicht (Neuronen, die Informationen an die Umwelt abgeben) und eine verborgene Schicht. Der Aufbau der verborgenen Schicht hängt von der Art des Netzes ab. Beim „Feed Forward"-Ansatz gibt es mehrere eindimensionale Schichten, die nacheinander aufgebaut sind. Jeder Knotenpunkt ist mit der darauffolgenden Schicht verbunden [Kri12]. Im Gegensatz dazu kann bei einem rückgekoppelten Netz die Ausgangsleitung eines Neurons in ein Neuron einer vorhergehenden Schicht als Eingang fungieren. Zu diesen Arten existieren weitere Unterarten. In dieser Arbeit wird der klassische „Feed Forward"-Ansatz verwendet.

Als Eingabeschicht sind die extrahierten Merkmale gegeben. Die Definition der Ausgabeschicht ist von der Art der Authentifizierung abhängig. Bei der Verifizierung gibt es nur ein Ausgabeneuron und für jede Person muss ein eigenes Netz trainiert werden. Abhängig von der Erkennung der Person erfolgt eine entsprechende Ausgabe. Ziel der Klassifikation, bei Dateneingabe einer Person in das neuronale Netz, ist es, dass nur, wenn es die Person ist, für die das Netz trainiert wurde, der Ausgabeknoten aktiviert wird.

Für das Training eines neuronalen Netzes ist neben den Daten (sowohl positive als auch negative Beispiele) auch die Wahl der zwei Steuerparameter (Lernrate und Momentterm (engl. *momentum*)) entscheidend. Positive Beispiele sind Daten, die dazu führen sollen, dass das Netz ausgibt, ob es die spezielle Person ist. Bei negativen Beispielen, wenn z. B. ein Angreifer versucht an das System zu gelangen, darf das Ausgabeneuron des Netzes nicht aktiviert werden. Damit das System diese Unterscheidung treffen kann, benötigt es vorher Daten, bei denen bekannt ist, wie die Klassifikation ausgeht.

2.4.2 Authentifizierungsmodalitäten

Bei der biometrischen Authentifizierung werden zwei Gruppen von Methoden voneinander unterschieden: aktive und passive Verfahren. Diese werden in den folgenden Abschnitten genauer erläutert. In Abbildung 2.7 werden verschiedene Verfahren der zwei Gruppen aufgelistet. Jedes Verfahren stellt eine Authentifizierungsmodalität dar.

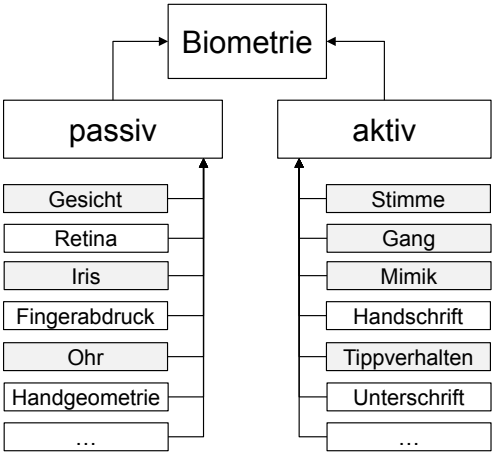


Abbildung 2.7: Modalitäten für die biometrische Authentifizierung

Im Zusammenhang mit Smartphones können nicht alle Verfahren eingesetzt werden, da verschiedene Hardwarevoraussetzungen (spezielle Sensoren) existieren. Heutige Smartphones besitzen meist Sensoren wie Global Positioning System (GPS) Sensor, visueller Sensor (z. B. Kamera), Audiosensor (z. B. Mikrofon), kapazitives Display, Lichtsensor, Temperatursensor, Richtungssensor (z. B. magnetischer Sensor) und den Beschleunigungssensor [KWM11]. In Abbildung 2.7 sind die Authentifizierungsmethoden grau hervorgehoben, welche durch diese Sensoren erfasst werden können. In den folgenden Unterpunkten werden die verschiedenen Verfahren genauer erläutert.

Passive Verfahren

Im Folgenden werden verschiedene passive (physische) Verfahren vorgestellt. Diese stellen vor allem Körperteile einer Person dar.

Gesichtserkennung: Die Gesichtserkennung ist eine Methode, die einen optischen Sensor benötigt. Für die Gesichtserkennung werden bestimmte Charakteristika z. B. vom Auge, Augenbrauen oder Nase des Benutzer extrahiert und als Merkmale für die Authentifizierung verwendet [STS10, BP93].

Diese Technik wird bereits von verschiedenen Smartphoneherstellern für die Authentifizierung von Personen benutzt. Bei dem Betriebssystem Android konnte z. B. eine Authentifizierung erfolgen, indem die Person in die Frontkamera schaut. Dieses Verfahren ist anfällig gegen Angriffe, bei denen ein Foto der Person vor die Kamera gehalten wird. Es gibt jedoch Vorgehensweisen, mit denen dieses Problem gelöst werden kann, bspw. durch das Blinzeln mit einem Auge. Somit wird erkannt, dass die Person real ist. Darüber hinaus hat die Apple Inc. [SK12] eine Methode zur 3D Erkennung patentieren lassen. Verschiedene existierende Studien am Computer erreichten bereits eine Akzeptanzrate von über 90 % mittels 3D Erkennung [LJ05, ML07, HBGM05]. Bei der Verwendung einer 2D- und 3D-Erkennung kann eine Akzeptanzrate von über 99 % gemessen werden [CBF03, TTS03].

Die Verarbeitung der 3D Gesichtserkennung verbraucht jedoch so viel Rechenleistung, dass eine Authentifizierung am Smartphone laut Anjos et al. [AM11] 3,7 Sekunden benötigt. Ein weiterer Nachteil besteht darin, dass unterschiedliche Blickwinkel die Authentifizierung erschweren, ebenso eine unzureichende Lichtquelle [JHP00, S. 95]. Dadurch benötigen die meisten Verfahren eine Vielzahl von Trainingsdaten, um die Nachteile auszugleichen [ZG09, S. 2895]. Außerdem bietet dieses Verfahren keine ausreichenden Erkennungsunterschiede zwischen Zwillingen, laut Jain et al. [JNN08, S. 2]. Zudem ist es in Sicherheitsbereichen nicht anwendbar oder nicht verfügbar (z. B. abgeklebte Kameras).

Iriserkennung: Die Iriserkennung kann auch dann verwendet werden, wenn große Teile des Gesichts, z. B. aus religiösen Gründen, verdeckt sind. Laut einer Marktstudie empfanden 44 % der befragten Personen dieses Verfahren als komfortabel [CAJ03].

Die Iriserkennung hat jedoch den Nachteil, dass eine Infrarotkamera erforderlich ist, um spezielle Merkmale, die in vielen Studien verwendet werden, zu extrahieren [Dau02, KHA+05]. Daher ist es für Standard Smartphones nicht geeignet.

Retina: Die Struktur der Blutgefäße auf der Rückseite des Auges wird als die genaueste biometrische Eigenschaft bezeichnet [Hil99].

Nachteilig sind die Kosten für einen speziellen Sensor und die notwendige Kooperation des Benutzers [Vie06].

Die speziellen Sensoren sind zudem in den meisten Smartphones nicht verbaut.

Fingerabdruck: Vor allem in der Forensik wird der Fingerabdruck zur Identifizierung von Personen verwendet. Dabei werden Informationen über die Oberfläche der Haut genutzt (u. a. Minutien, die Muster der Papillarlinien darstellen).

Ein Nachteil ist, dass der Fingerabdruck von sämtlichen Oberflächen mit einem dünnen Silikonfilm von Angreifern extrahiert werden kann und von vielen Sensoren als solcher erkannt wird [DPS05, S. 2]. Durch Alterung des Scanners (z. B. Kratzer) [Olz06, S. 8] oder des Fingers können sich die Fehlerraten erhöhen, die Dauerhaftigkeit wird damit verringert. Über die Nutzerakzeptanz gibt es unterschiedliche Meinungen. Laut Sasse [Sas05, S. 9] zeigt der Fingerabdruck eine gute Benutzerfreundlichkeit und wird von den Nutzern auch akzeptiert. Demgegenüber steht die Aussage von Esposito [Esp12, S. 11] und Jain et al. [JHP00, S. 96], dass der Fingerabdruck nicht komfortabel sei, da er u. a. an Kriminalität erinnere.

Handabdruck: Dieses Verfahren ähnelt dem Fingerabdruck, wobei hier vor allem die drei Linien (Herz-, Kopf- und Lebenslinie) berücksichtigt werden. Ein Nachteil besteht darin, dass das Scannen

und Identifizieren 6 bis 10 Sekunden benötigt [Rob06]. Gleichzeitig bietet diese Methode keine ausreichenden Unterscheidungsmerkmale, sodass nur eine Verifikation durchgeführt werden kann [Rob06].

Aktive Verfahren

Im Gegensatz zu den passiven Verfahren wird bei aktiven Verfahren das Verhalten einer Person analysiert und zur Authentifizierung verwendet.

Tippverhalten: Beim Tippverhalten werden Daten bei der Eingabe von Wörtern in die Tastatur analysiert. Es gibt zum einen die textunabhängige Authentifizierung, bei der eine beliebige Zeichenfolge eingegeben wird und zum anderen die textabhängige Authentifizierung.

Auf der Tastatur gibt der Nutzer sein Passwort ein. Die korrekte Eingabe des Passwortes und des dazugehörigen Tippverhaltens entscheiden, ob es sich um die zugangsberechtigte Person handelt oder nicht [CTL12, S. 1157].

Dieses Verfahren ist implizit, da der Nutzer keine zusätzliche Aktivität unternehmen muss [KAK11, S. 1572]. Ein weiterer Vorteil ist, dass keine zusätzliche Hardware benötigt wird und die Eingabe nur über die Tastatur erfolgt [MR00, S. 352] bzw. an neuen mobilen Endgeräten über das kapazitive Display extrahiert werden kann. Laut Studien kann das Authentifizierungsverfahren nur zur Verifikation von Personen verwendet werden, da sonst die Fehlerraten zu hoch sind [Olz06, S. 8]. Nachteilig ist, dass bisherige Studien nur klinisch getestet wurden und keine Alltagstauglichkeit nachweisen (siehe Abschnitt 3.1.1).

Gangerkennung: Biometrische Charakteristiken, wie die Fortbewegung einer Person, können mittels Gangerkennung extrahiert und evaluiert werden.

Zuerst erfolgte dies über die optische Erkennung einer menschlichen Silhouette während des Gehens [RNJ06]. Weitere Experimente

wurden mit akustischer Analyse durchgeführt [Ote05]. Mit dem Aufkommen von modernen Smartphones, die sowohl Accelerometer als auch Gyroskop enthalten, können Analysen mit diesen Geräten durchgeführt werden [TM12]. Während beim Gyroskop die Rotation bestimmt wird, können mit dem Accelerometer weitere Bewegungen analysiert werden [CC11, ANB+01]. Diese beiden Sensoren extrahieren Sensorwerte, die zu bestimmten Aktivitäten/Events zugeordnet werden können (siehe Abbildung 2.8). Diese werden zur Authentifizierung mittels des Ganges genutzt.

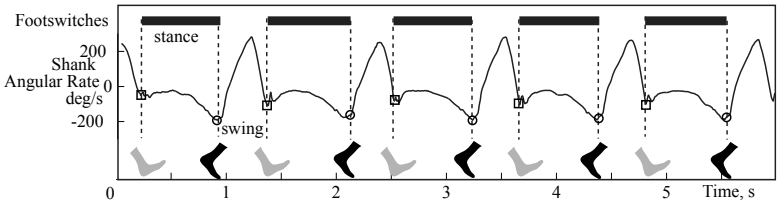


Abbildung 2.8: Erkennung des Ganges mithilfe des Gyroskops [ANB+01]

Wie in Abbildung 2.8 zu erkennen, können sowohl das Auftreten mit der Hacke als auch das Abrollen über die Fußspitze mit dem Gyroskop erkannt und u. a. die Zeiten zwischen mehreren Schritten berechnet werden.

Nachteilig sind die schlechten Erkennungsraten, die bei den bisherigen Studien analysiert wurden (siehe Abschnitt 3.1.2).

Sprache bzw. Sprechererkennung: Über ein Mikrofon kann eine Erkennung der Sprache bzw. eines Sprechers unter Beachtung wie und was eine Person sagt, erfolgen. Die Spracherkennung basiert auf einem bestimmten Text, wobei die Sprechererkennung von der Art, wie gesprochen wird, abhängig ist [STS10]. Grundsätzlich können, wie bei den anderen Methoden, u. a. zeitliche Merkmale extrahiert werden, aber auch Muster mit den Höhen und Tiefen der Stimmlage [SYY+11].

Die Beeinflussung der Aufnahme mit Mikrofon durch Rauschen oder das wiederholte Abspielen zu einem späteren Zeitpunkt stellen entscheidende Nachteile dar, da diese die Sicherheit und Benutzerfreundlichkeit beeinträchtigen.

Unterschriftenerkennung: Bei der Unterschriftenerkennung handelt es sich nicht nur um den optischen Vergleich einer Unterschrift, sondern auch darum, wie sie ausgeführt wurde.

Über ein sensitives Display wird erkannt, wo und mit welcher Druckstärke die Linien gezeichnet wurden. Zusammen mit dem Winkel, mit dem der Stift aufdrückt, kann klassifiziert werden, ob die eigentliche Person die Unterschrift vorgenommen hat.

2.5 Multi-biometrische Verfahren

Die einzelnen biometrischen Verfahren haben verschiedene Nachteile, z. B. Unterschiede zwischen den Versuchen einer Person (Intra-Personen-Unterschiede) oder Gleichheit zwischen verschiedenen Personen (zu geringe Inter-Personen-Unterschiede). Aufgrund dessen existieren Ansätze verschiedene biometrische Verfahren zu kombinieren [SBD+09], somit zu fusionieren. Eine Beschreibung dieser Kombinationen und deren mögliche Verknüpfung miteinander wird in diesem Abschnitt gegeben.

2.5.1 Vor- und Nachteile der Fusion

Neben der Reduktion der Nachteile einzelner biometrischer Verfahren reduziert die Fusion die Fehlerraten (z. B. die Benutzung nur der anderen Verfahren zur Authentifizierung). Diesen Punkt stellte bereits Ross und Jain [RJ03] mithilfe einer Receiver Operator Characteristic (ROC)-Kurve dar. Diese Kurve repräsentiert den Zusammenhang zwischen FAR und Genuine Accept Rate (GAR), wobei die GAR aus der FRR berechnet werden kann: $GAR = 1 - FRR$. In Abbildung 2.9 werden die Auswirkungen einer Fusion mittels der ROC-Kurve aufgezeigt.

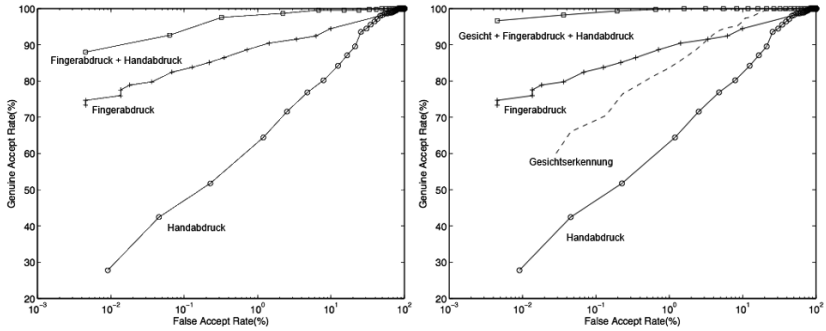


Abbildung 2.9: ROC-Kurve: (links) Kombination aus Fingerabdruck und Handgeometrie. (rechts) Kombination aus Fingerabdruck, Gesicht und Handgeometrie [RJ03]

Auf der linken Seite der Abbildung sind die Resultate für den Fingerabdruck und die Handgeometrie zu sehen. Dabei wird deutlich, dass die Fehlerraten für die einzelnen Verfahren verbessert werden können, indem eine Fusionierung der beiden Authentifizierungsmethoden (Fingerabdruck und Handabdruck) erfolgt. In Abbildung 2.9 wird auf der rechten Seite die Methode der Gesichtserkennung hinzugenommen. Obwohl diese Fehlerraten bei der Gesichtserkennung höher als die des Fingerabdrucks sind, führt die Fusion aller drei Methoden zu kleineren Werten als die Fusion von nur zwei Methoden. Je mehr Methoden für eine Fusion verwendet werden, desto geringere Ergebnisse können erzielt werden. Das gilt für ganze Methoden als auch für die Verwendung von zusätzlichen Merkmalen.

Der einzige Nachteil einer Fusion besteht darin, dass viele Daten aufgenommen werden müssen und damit die Auswertung umfangreicher ist, als wenn nur einzelne Methoden verwendet werden. Daher muss bei der Verwendung eines Smartphones die Bearbeitungsdauer bei einer Fusion geprüft werden.

2.5.2 Arten multi-biometrischer Verfahren

Biometrische Verfahren können auf unterschiedlichste Arten kombiniert werden. Eine biometrische Methode wird als multi-biometrisches Verfahren bezeichnet, wenn mindestens eine der folgenden Eigenschaften zutrifft:

- Verschiedene biometrische Merkmale (multi-modal),
- Verschiedene Instanzen (multi-instance),
- Verschiedene Sensoren (multi-sensorial) oder
- Verschiedene Darstellungen (multi-repräsentation).

Diese vier vorgestellten Eigenschaften werden wie folgt definiert (nach [II06]):

multi-modal: Es wird die Verwendung von mehreren biometrischen Verfahren beschrieben, die über einen oder mehrere Sensoren aufgenommen wurden.

multi-instance: Bei der Verwendung eines biometrischen Verfahrens mit verschiedenen Aufnahmen der Daten handelt es sich um multi-instance. Dazu zählt die Aufnahme von mehreren Fingerabdrücken unterschiedlicher Finger.

multi-sensorial: Ein einziges biometrisches Verfahren kann über verschiedene Sensoren aufgenommen werden. Dieses multi-sensoriale Verfahren ist z. B. bei der Gangerkennung möglich, bei der durch den optischen und den akustischen Sensor Merkmale des Ganges aufgenommen werden.

multi-repräsentation: Ein Verfahren, das auf einer multi-repräsentation von Methoden basiert, bezeichnet ein System, bei dem mehrere Darstellungsformen für ein biometrisches Merkmal genutzt werden. Dazu zählen die Verwendung von mehreren Bildern des Gesichtes, die bei einem Video aufgenommen wurden oder die Darstellung des Gesichtes zusätzlich durch ein Amplitudenspektrum.

2.5.3 Stufen bei Fusion von multi-biometrischen Verfahren

Bei der Verwendung eines multi-biometrischen Verfahrens müssen die Informationen zusammengetragen werden, die für die Bestimmung der Person entscheidend sind. Dabei wird von der Fusion der unterschiedlichen Informationen gesprochen. Im ersten Schritt wird für jedes Verfahren der Authentifizierungsprozess einzeln durchlaufen. Nach der Fusion gibt es nur einen Informationspfad, für den der Prozess weitergeführt wird.

Diese Fusion kann auf vier verschiedenen Ebenen erfolgen, welche in Abbildung 2.10 aufgezeigt werden (abgeleitet aus dem Modell in Abbildung 2.4).

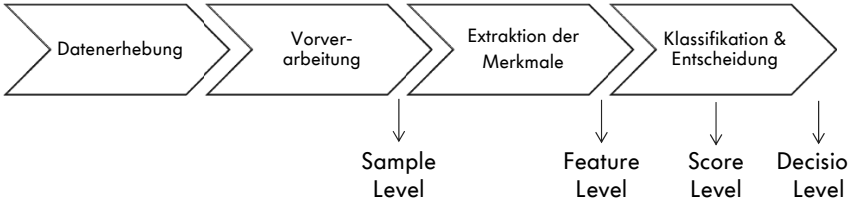


Abbildung 2.10: Ebenen der Fusion

Sample Level: Bei dieser Art der Fusion werden mehrere Bilder/Daten miteinander verglichen, um sie qualitativ aufzubereiten. Hierzu zählen die Ergänzung von fehlenden Bildbereichen oder die Aufnahme von zusätzlichen Informationen in einem Bild (was eine 3D-Darstellung ermöglicht) [Rad07].

Feature Level: Die nach der Merkmalsextraktion agierende Feature Level Fusion verbindet die verschiedenen Merkmalsvektoren zu einem Vektor.

Score Level: Für jedes Merkmal wird ein Match Score generiert, der angibt, wie gut das Merkmal mit dem aus der Datenbank übereinstimmt. Die verschiedenen Match Scores müssen zunächst normalisiert werden, bevor sie mit einer Funktion (z. B. einfache oder

gewichtete Summierung) fusioniert werden. Nach dieser Fusion erfolgt der Vergleich des Wertes mit dem vorher definierten Schwellenwert.

Decision Level: Bei der Fusion auf dem Decision Level wird zuerst für jede Methode anhand des Schwellenwertes entschieden, ob es sich um eine bestimmte Person handelt oder nicht. Diese Entscheidungen werden genutzt, um eine Gesamtentscheidung aggregiert zu treffen.

2.6 Herausforderungen bei biometrischen Authentifizierungssystemen

Es gibt eine Reihe von Herausforderungen, die im Zusammenhang mit der Authentifizierung bei biometrischen Merkmalen adressiert werden müssen. Folgende Punkte repräsentieren diese und müssen bei der Generierung eines Authentifizierungssystems beachtet werden [IEE10, Vie06, RNJ06]:

Fehlerraten: Die FAR und FRR stellen das größte Problem aus Sicherheits- und Benutzersicht dar. Bei einer FAR von mehr als 1 % wird das Verfahren von Sicherheitsabteilungen teilweise abgelehnt. Jedoch wollen die Nutzer durch das zusätzliche Verfahren nicht gestört werden, sodass auch die FRR nicht zu hoch sein darf.

Intra-Klassen-Unterschiede und Inter-Klassen-Ähnlichkeiten: Ein Grund für die hohen Fehlerraten können die Intra-Klassen-Unterschiede (Unterschiede einzelner Merkmale zwischen den verschiedenen Versuchen einer Person) und Inter-Klassen-Ähnlichkeiten sein. Je größer die Unterschiede zwischen Versuchen einer Person sind, desto kleiner muss der Schwellenwert gesetzt werden. Das erhöht gleichzeitig die Chance, dass andere Personen bei diesen Schwellenwerten erkannt werden. Das trifft vor allem dann zu, wenn zwischen den Personen eine hohe Anzahl an Ähnlichkeiten im Muster bestehen (Inter-Klassen-Ähnlichkeiten).

Störungen bei der Eingabe: Durch Beschädigungen des Gerätes, z. B. durch Kratzer, kann sich ein Fingerabdruck verändern, ebenso wie

die Stimme bei einer Erkältung. Das sind Beispiele für Störungen [RNJ06, S. 25]. Dadurch kann das Resultat bei der Authentifizierung beeinflusst und die Erkennung einer Person erschwert werden.

Replay Attacken: Die meisten Angriffe auf das Authentifizierungssystem erfolgen auf die Benutzeroberfläche, wobei der Sensor nicht zwischen Original und Fälschung unterscheiden kann [JNN08]. Das kann z. B. mit einem Bild einer Person vor der Kamera erreicht werden. Um dieses Problem zu beheben, muss eine Erkennung der Lebendigkeit erfolgen, wofür zusätzliche Hardware- oder Software-Lösungen benötigt werden [LWTJ04].

2.7 Zusammenfassung

In diesem Abschnitt werden die zuvor vorgestellten Grundlagen zusammenfassend dargestellt und ihr Nutzen für diese Dissertation aufgezeigt.

Der Grundgedanke der Dissertation basiert auf einem erweiterten Konzept der Grundwerte für die IT-Sicherheit, bei dem der Punkt der Authentifizierung aufgegriffen wird. Dieser kann in Bezug auf den Zugriff auf Systeme oder Objekte (siehe Abschnitt 2.2.1) dargestellt werden. Nach der Identifikation ist die Authentifizierung der zweite Schritt, um Zugriff auf Systeme zu erhalten. Diese Authentifizierung kann über mehrere Faktoren erreicht werden (Wissen, Besitz oder Biometrie), wobei die Biometrie u. a. den Vorteil der Flexibilität aufweist, da das Merkmal immer personengebunden verfügbar ist und nicht vergessen werden kann.

Daraufhin wurden der Ablauf einer biometrischen Authentifizierung genauer betrachtet und die einzelnen Prozesse beschrieben sowie die Vor- und Nachteile verschiedener Authentifizierungsmethoden.

Ausgehend von den Nachteilen der Verfahren wurde gezeigt, wie mehrere biometrische Verfahren gemeinsam genutzt bzw. fusioniert werden können. Dazu erfolgte eine genauere Untersuchung der Fusionsarten und -stufen, die geeignet sind.

Als ein Nachteil wurden die Fehlerraten beschrieben, die bei einer Authentifizierung auftreten können. Dies ist eine von vielen Anforderungen an die Systemsicherheit, die in diesem Kapitel definiert wurden.

Der letzte Abschnitt benennt allgemeine Probleme, die bei einem Authentifizierungssystem auftreten können, z. B. Störungen oder Angriffe auf das System. Diese Grundlagen werden für die in der Arbeit vorgestellten Konzepte und Vorgehensweisen benötigt.

Im folgenden Kapitel wird der Stand der Forschung auf dem Gebiet der biometrischen Authentifizierung, im Speziellen das Tippverhalten, aufgezeigt. Anschließend werden Lösungsideen für die in diesem Kapitel beschriebenen Probleme definiert.

3 Forschungslücken und Lösungskonzept

Dieses Kapitel beschäftigt sich mit der existierenden Forschungslücke, wofür zuerst auf den Stand der Technik für biometrische Authentifizierung am Smartphone eingegangen wird. Danach erfolgen die Abgrenzung des Untersuchungsbereiches und eine Einordnung der Forschungsarbeiten sowie eine Vorstellung des Konzeptes der Authentifizierung mittels des Tippverhaltens.

3.1 Stand der Technik für biometrische Authentifizierung am Smartphone

In diesem Abschnitt wird auf den Stand der Technik der Authentifizierung am Smartphone bezüglich der Sensoren eingegangen. Es werden das Tippverhalten, die Gangerkennung und die Bewegungserkennung genauer betrachtet und durch Daten von weiteren Sensoren (u. a. kapazitives Display und Bewegungssensor) ergänzt.

3.1.1 Tippverhalten

Zunächst werden die allgemeinen Grundlagen des Tippverhaltens analysiert und im Anschluss detaillierter auf die verschiedenen Tastaturarten (Hardware- bzw. Softwaretastatur) eingegangen.

Allgemeine Grundlagen des Tippverhaltens

Die Extraktion vom Tippverhalten existierte schon weit vor den Standard-Computer-Tastaturen. Bereits früher, als Telegramme ver-

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_3

schickt wurden, konnten sich unterschiedliche Vermittler, die oft zusammenarbeiteten, am Stil bzw. Rhythmus der Übertragung erkennen [BH97]. Durch die Verwendung eines Computers sind weitere Möglichkeiten für die Erkennung von Personen hinzugekommen, die verglichen werden können. Der Rhythmus des Tippens kann dabei durch verschiedene Zeitabstände analysiert werden [MFM+09]. Abbildung 3.1 zeigt unterschiedliche Aktivitäten und Möglichkeiten, welche Zeitintervalle extrahiert werden können.

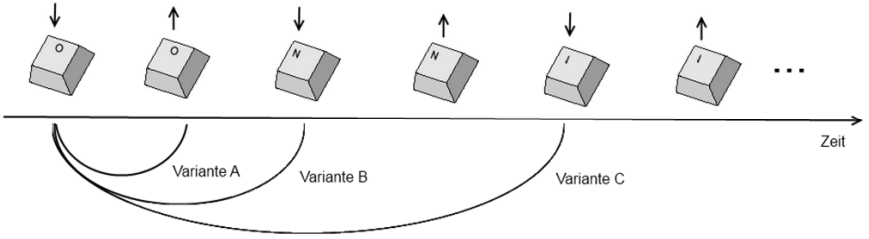


Abbildung 3.1: n-Graphen

Zum einen kann die zeitliche Differenz zwischen zwei aufeinander folgenden Events (Interaktionen mit dem Gerät) betrachtet werden [ELM11]. Dabei wird die Zeitdifferenz zwischen dem Drücken und dem Loslassen einer Taste verwendet, das als *Verweildauer* bezeichnet wird (Variante A). Zum anderen kann die Zeitdauer zwischen dem Drücken der ersten Taste und dem Drücken einer zweiten Taste extrahiert werden. In diesem Fall wird von *Bewegungszeit* oder vom *Digraph* gesprochen (Variante B) [KC07]. Laut der Studie von Karatzouni et al. [KC07] hat die *Verweildauer* geringere Fehlerraten als die *Bewegungszeit*. Der *Digraph* ist des Weiteren nur eine spezielle Form des *n-Graphen* [MFM+09], wodurch die Zeitdauer zwischen n aufeinander folgenden Tasten-Events repräsentiert wird. Zusätzlich wurde in einigen Studien die Kombination aus drei Tastenanschlägen verwendet, was als *Trigraph* bezeichnet wird (Variante C) [CM07]. Prinzipiell sind alle Werte für $n > 1$ möglich, um die Zeitdifferenzen zu bestimmen. Je höher der Wert ist, desto weniger Informationen

können aus einem Text der Länge m gezogen werden, da es sich um einen Durchschnittswert über n Events hinweg handelt. Die Berechnung der Anzahl der Merkmale (m), basierend auf der Wortlänge (n) für die einzelnen Zeitintervalle, wird in Formel 3.1 dargestellt.

$$m = \begin{cases} n-2, & wenn(feature\ group = Trigraph) \\ n-1, & wenn(feature\ group = Digraph) \\ n, & wenn(feature\ group = Verweildauer) \end{cases} \tag{3.1}$$

Die Verweildauer entspricht dabei der Anzahl der getippten Zeichen. Die anderen beiden Merkmale besitzen ein bzw. zwei Merkmale weniger.

Neben den *n-Graphen* gibt es weitere Möglichkeiten an einem Computer oder an Mobiltelefonen mit den 12 Hardwaretasten mehrere Merkmale zu extrahieren. Dazu zählen die Anzahl wie oft ein Buchstabe gelöscht wurde [ZSKF09] oder, an der Computer-Tastatur, welche Shift-Taste (links oder rechts) im Allgemeinen oder für bestimmte Buchstaben bevorzugt wird.

Als Klassifikatoren werden im Bereich des Tippverhaltens vor allem statistische Klassifikatoren (wie das Euklid- oder das Mahalanobis-Distanzmaß) [UW85], Support Vector Machines (SVM) [MCGCN11] oder neuronale Netze [ACS08, Fz05] verwendet. Die open-source Data Mining Software Waikato Environment for Knowledge Analysis (Weka) [HFH+09] beinhaltet eine Vielzahl von Klassifikatoren, die für eine Klassifikation verwendet werden können.

Für die textunabhängige Authentifizierung wurden eine Reihe von Merkmalen von der textabhängigen Authentifizierung adaptiert, wie die Nutzung von Verweildauer und Digraphen [DK09]. In diesem Zusammenhang wird mit dem gemittelten Wert über alle Verweildauern und Digraphen der gleichen Buchstaben/Buchstabengruppen verglichen. Bei nicht existierenden Digraphen wird über das relative Distanzmaß der Buchstaben der Vergleichswert berechnet.

Hardwaretastatur

Das Tippverhalten an herkömmlichen Tastaturen ist bereits Bestandteil zahlreicher wissenschaftlicher Arbeiten. In diesen wurden sowohl die Verweildauer [CHHK00, Lin97, OS97] als auch die Bewegungszeit [MR97, OM93, HAZ00] als Merkmal des Tippverhaltens untersucht. Auch das Tippverhalten zur Authentifizierung auf Mobiltelefon-Tastaturen wurde bereits untersucht [BC08, ZSKF09], wofür Geräte mit 12 Hardwaretasten verwendet wurden.

Die Untersuchung von Banerjee und Woodard [BW12] zeigt einen Überblick über die unterschiedlichen Experimente und die dabei entstandenen Resultate. Laut Karnan et al. [KAK11, S. 1572] ist es jedoch schwierig, die Studien mit unterschiedlichen Untersuchungsteilnehmern, Merkmalen und Klassifikationsmethoden zu vergleichen. Ein Auszug aus der Veröffentlichung von Banerjee und Woodard soll im Folgenden zeigen, welche Erkenntnisse momentan existieren.

Bei einer der ersten Studien am Computer wurde von Umphress und Williams [UW85] bereits eine FAR von 11,7 % und eine FRR von 5,8 % erreicht. Auch Joyce und Gupta [JG90] erreichten ähnliche Werte (FAR: 0,3 %, FRR: 16,4 % mit 33 Testpersonen). In beiden Studien wurden nur Digraphen mit einem statistischen Klassifikator verwendet. Später verwendeten Ord und Furnell [OF00] ein neuronales Netz bei 14 Testpersonen (9,9 % FAR und 30,0 % FRR). Auf den Mobiltelefonen wurden von Clarke und Furnell [CF06] erste Ergebnisse durch ein neuronales Netz mit einer EER von 15,2 % (25 Testpersonen) erzielt. Es ergab, dass die Nutzung eines Passwortes bessere Ergebnisse erzeugt als die Eingabe eines PINs. Insbesondere ein vierstelliger PIN ist zu kurz [BC08, S. 6-7].

Für die textunabhängige Authentifizierung wurde von Davoudi und Kabir [DK09] eine FAR von 9 % und eine FRR von 5 % erreicht, basierend auf einer Studie mit 21 Personen, die jeweils 15 Texte mit 700 bis 900 Zeichen eingeben mussten. Je mehr Daten von den Personen vorhanden sind, desto geringere Fehlerraten können berechnet werden. Die Eingaben erfolgten auf Computertastaturen. Eine der wenigen Studien auf einem Mobiltelefon ist von Zahid et al. [ZSKF09], bei

dem mit einem neuronalen Netz eine FAR von 11 % und eine FRR von 9,22 % mit 30 Testpersonen erreicht wurde.

Touchscreen Display mit weiteren Sensoren

Wenige Publikationen beschäftigen sich bisher mit der Authentifizierung mithilfe des kapazitiven Displays. Diese Art von Display ermöglicht es, neben den Zeitstempeln einer Aktion, weitere Merkmale zu extrahieren. Die Druckstärke, die Größe des Fingers und die x/y-Koordinaten wurden bereits in einer Studie von De Luca et al. [DLHB+12] verwendet. In dieser Studie haben die Testpersonen Punkte einer 3x3 Punktematrix (analog zu dem Entsperrmuster beim Android OS) auf dem Display miteinander verbunden. Mittels des Dynamic Time Warping (DTW) Klassifikationsalgorithmus wurden eine FAR von 21 % und eine FRR von 19 % für diese Methode ermittelt. Es stellte sich heraus, dass eine Verwendung der Daten der Sensoren zur Authentifizierung im Vergleich zur Authentifizierung nur mit der Punktematrix die Sicherheit erhöht. Diese Studienergebnisse wurden parallel mit den ersten eigenen Publikationen veröffentlicht, basieren aber nicht auf dem eigentlichen Tippen, sondern dem Wischen über das kapazitive Display.

Zu dem Touchscreensensor können weitere Sensoren verwendet werden, wie in der Studie von Miluzzo et al. [MVBC12] beschrieben. Dabei wurde gezeigt, wie ein Angriff auf die Passworteingabe bei der Verwendung von Sensoren durchzuführen ist, die im mobilen Betriebssystem als nicht kritisch deklariert sind. Mittels einer Applikation, die die Gyroskop Daten während der Eingabe des Passwortes speichert, konnte mit einer Zuverlässigkeit von über 60 % gesagt werden, welche Taste gedrückt wurde. Das bedeutet, dass das Gyroskop gleichzeitig genutzt werden kann, um biometrische Charakteristiken einer Person aufzunehmen.

3.1.2 Gangerkennung und Bewegungserkennung

Der Vorteil der Gang- und Bewegungserkennung besteht darin, dass diese bei Nutzung eines Smartphones im Hintergrund durchgeführt werden kann, ohne dass der Benutzer eine spezielle Interaktion durchführen muss. Diese Informationen können gleichzeitig genutzt werden, um eine Person mit geringeren Fehlerraten und kontinuierlich authentifizieren zu können.

Die Gangerkennung wurde für medizinische Zwecke untersucht z. B. zur Analyse von Methoden zur Verbesserung des Ganges bei Parkinsonerkrankungen [SKBD+01]. Dabei wird auf Bewegungssensoren, Videoaufnahmen sowie Druck- und Kraftmessungen zurückgegriffen. Bei Videoaufzeichnungen können verschiedene Merkmale extrahiert werden (z. B. Gehgeschwindigkeit, Schrittlänge, Hüftstreckung und -beugung usw.). Neben dem gradlinigen Gehen wurde in diesem Umfeld auch die Erkennung von Aktivitäten, wie das Rennen oder Treppensteigen, analysiert.

Die Gangerkennung kann zudem zur Authentifizierung einer Person auf anderen Gebieten eingesetzt werden. Für diesen Zweck wurden Accelerometer an verschiedenen Punkten einer Person (z. B. an den Schuhen, in Taschen oder am Körper) angebracht und mittels Histogrammgleichheiten und Zyklen zur Auswertung verglichen [Gaf08]. Heutzutage können dafür bereits Smartphones eingesetzt werden, die neben dem Accelerometer auch ein Gyroskop besitzen. Eine Übersicht verschiedener Studien auf diesem Gebiet ist in Tabelle 3.1 zusammengefasst.

Die Studie von Ailisto et al. [ALM+05] ist eine der ersten, die eine Ganganalyse mit tragbarem Accelerometer an der Taille zur Authentifizierung verwendet hat. Es wurden Daten von 36 Probanden in der Studie gesammelt und eine FAR von 6,4 % und eine FRR von 5,4 % erreicht. In der Studie von Mantyjarvi et. al [MLV+05] wurde bei der Nutzung des Accelerometers an der Taille ein ähnliches Ergebnis generiert.

Zuvor wurde in der Studie von Morris [Mor04] bei 10 Personen ein Accelerometer am Schuh befestigt. Bei der Auswertung konnte eine Er-

Tabelle 3.1: Übersicht über tragbare Sensoren (angelehnt an Gafurov [Gaf08, S. 13]

Studie	**Anzahl Probanden**	**Befestigung**	**EER (in %)**	**Erkennung (in %)**
Sprager et al. [SZ09]	14	Hüfte	-	90,3
Thang et al. [TVTC12]	11	Hosentasche	-	92,7
Derawi et al. [DNBB10]	51	Hüfte	20,1	-
Gafurov [Gaf08]	30	Fußgelenk	5,0	-
	50	Hosentasche	7,3	-
	100	Hüfte	13,0	-
	30	Arm	10,0	-
Morris [Mor04]	10	Schuh	-	97,40
Huang et al. [HCHX07]	9	Schuh	-	96,93
Ailisto et al. [ALM+05]	36	Taille	FAR=6,4; FRR=5,4	-
Mäntyjärvi et al. [MLV+05]	36	Taille	7,0 - 19,0	-
Rong et al. [RZJM07]	35	Taille	6,7	-
Rong et al. [RJMX07]	21	Taille	5,6	-
Vildjiounaite et al. [VML+06]	31	Hand	17,2; 14,3	-
	31	Hüfte	14,1; 16,8	-
	31	Brusttasche	14,8; 13,7	-

kennungsrate von 97,40 % erreicht werden. Das Ergebnis wurde in der Studie von Huang et al. [HCHX07] bestätigt. Neun Probanden trugen in dem Experiment spezielle Schuhe, an denen die Sensoren befestigt waren. Der Gang von acht Probanden wurde mit dem Gang einer einzelnen Person verglichen, um zu prüfen, ob sie als nicht autorisiert erkannt werden. Für alle Personen ergab sich eine Erkennungsrate von 96,93 %.

Eine weitere Befestigungsmöglichkeit für das Accelerometer ist die Hosentasche mit einer speziellen Vorrichtung. Die Erkennungsrate mit dem Accelerometer in der Hosentasche liegt bei 92,7 % (siehe Thang et al. [TVTC12]). Bei der Befestigung an der Hüfte ergab die Studie von Derawi et al. [DNBB10] eine EER von 20,1 %, bei 51 Testpersonen. Bei diesem Test wurde erkannt, dass eine höhere Abtastrate die Fehlerraten verringert.

Zur besseren Vergleichbarkeit dieser verschiedenen Positionen wurde in zwei Studien (Vildjiounaite et al. [VML+06] und Gafurov [Gaf08]) analysiert, wie der Einfluss der Lage des Gerätes sich auswirkt. In der Studie von Vildjiounaite et al. [VML+06] wurden zwei verschiedene Auswertungsprinzipien verwendet, mittels einer Korrelation und einer Fast Fourier-Transformation (FFT). In der Hüfttasche wurden kleinere Fehlerraten durch die Korrelation erzeugt (14,1 %), in den restlichen Fällen durch die FFT. In der Brusttasche wurden generell kleinere Fehlerraten erzeugt als in der Hand. Gafurov [Gaf08] testete mit vier verschiedenen Positionen (Fußgelenk, Hosentasche, Hüfte, Arm) und erzielte eine EER zwischen 5,0 % und 13,0 % je nach Position des Sensors, wobei am Fußgelenk und in der Hosentasche kleinere Fehlerraten abzulesen waren.

Es zeigte sich, dass die Gangerkennung ausreichend Ergebnisse liefert, sodass eine Authentifizierung erfolgen kann, wenn die Position des Gerätes an der Person herausgefunden werden kann. In den letzten Jahren wurde die Gangerkennung mit einer Aktivitätserkennung erweitert, wobei eine Reihe von Aktivitäten miteinander verglichen wurden, wie z. B. das Liegen, Klettern, Fahrrad fahren oder Kochen [DDK+12]. Hierfür wird eine Reihe an Aggregation für die einzelnen Sensoren durchgeführt, um Merkmale für die Erkennung

zu erhalten. Dazu zählen u. a. Minimum, Maximum, Mittelwert und Standardabweichung sämtlicher Sensoren [DDK+12]. Die verschiedenen Klassifikatoren wurden mittels dieser Merkmale trainiert. Doch besonders bei ähnlichen Aktivitäten (z. B. Kochen und Wischen) ist diese Herangehensweise bei einer Erkennungsrate von 52 % bis 78 % Genauigkeit noch nicht ausgereift.

3.2 Abgrenzung des Untersuchungsbereiches und Einordnung der Forschungsarbeiten

Die existierenden Studien zum Tippverhalten analysieren die Authentifizierung an Tastaturen von Computern oder an mobilen Telefonen mit 12 Hardwaretasten (12-Tastenlayout) [BC08, ZSKF09]. Mit Einsatz der neuen Generation von mobilen Telefonen, den Smartphones, hat sich eine andere Art von Eingabetechnik für Zeichen entwickelt: das Display mit Touchscreen, welches heute in den meisten Smartphones verbaut ist. Der daraus resultierende Forschungsbedarf und weitere Punkte, die analysiert werden müssen, sind in Tabelle 3.2 verdeutlicht.

Sowohl für die Personal Computer (PC)-Tastaturen als auch bei den mobilen Geräten mit einem 12-Tastenlayout wurden bereits Studien durchgeführt. Die Studien reichen jedoch nicht aus, da sich, wie schon erwähnt, die Eingabetechnik verändert hat. Das bedeutet, dass noch nicht gezeigt wurde, wie und ob ohne physikalisches Feedback eine korrekte Authentifizierung erfolgen kann. Gleichzeitig können andere Eigenschaften durch das kapazitive Display und die weiteren Sensoren genutzt werden, womit die Generierung potenzieller neuer Merkmale möglich ist, die für die Authentifizierung genutzt werden können. Die neuen Merkmale bieten eine Möglichkeit der Verbesserung der Fehlerraten und zudem können Adaptionen bei weiteren Schritten im Authentifizierungsprozess durchgeführt werden. Die unterschiedliche Länge oder Komplexität eines Passwortes stellt ein zusätzliches Mittel dar, welches bereits hinreichend für Hardwaretastaturen analysiert wurde. Dennoch muss eine Überprüfung erfolgen, ob eine Adaption auf das kapazitive Display durchführbar ist. Für die

Tabelle 3.2: Erkannter Forschungsbedarf bei der Authentifizierung mittels des Tippverhaltens

Einflussgrößen der Problemstellung	Mittels bestehender Methoden lösbar	Forschungsbedarf
Tippverhalten an Hardwaretastatur	x	
Tippverhalten an kapazitivem Display		x
Zu hohe Fehlerraten (über 5 %)		x
Unterschiedliche Länge des Passwortes	x	
Unterschiedliche Komplexität des Passwortes	x	
Generierung negativer Beispiele für Klassifikation		x
Unterschiedlicher Einfluss von Situationen während der Authentifizierung		x
Skalierbarkeit des Authentifizierungsverfahrens		x
Kontinuierliche Überprüfung		x
Veränderung durch den Lernprozess		x

Klassifikatoren (Erkennungsalgorithmus, bei dem mit einem Muster verglichen wird) muss ein Konzept entwickelt werden, das die negativen Beispiele für das Training von Klassifikatoren generiert. Aufgrund

des unterschiedlichen Einflusses von verschiedenen Situationen bei der Authentifizierung müssen neue Modelle generiert werden, die das Modell einer Person flexibel der Situation anpasst, sodass das Verfahren auch hier benutzerfreundlich bleibt. Durch eine zu geringe Probandenanzahl in den bestehenden Studien existiert bisher keine Möglichkeit, eine Skalierbarkeit bezüglich der Anzahl der Personen für die Authentifizierungsmethode sowie die Allgemeingültigkeit der Aussagen zu erreichen.

Ein weiterer Punkt ist die kontinuierliche Authentifizierung während der Nutzung eines Gerätes. Ein Modell soll die Möglichkeit zeigen, wie über die komplette Nutzungsdauer des Gerätes eine Überprüfung der Identität durchzuführen ist.

Gleichzeitig verändert sich das Tippverhalten mit zunehmender Erfahrung der Nutzer mit dem Authentifizierungssystem. Der daraus resultierende Einfluss kann das Merkmalmodell stark verändern, sodass die Person nicht mehr erkannt wird. Dieser Aspekt wird von den bestehenden Studien nicht aufgegriffen und berücksichtigt.

3.3 Konzept der Authentifizierung mittels des Tippverhaltens

Für die Lösung einer biometrischen Authentifizierung mittels des Tippverhaltens wird aufbauend auf dem ermittelten Forschungsbedarf in Abbildung 3.2 ersichtlich, welche Bestandteile essenziell für das Konzept dieser Dissertation sind.

Wie in Abbildung 3.2 zu erkennen ist, wird ein Framework definiert, das spezifische Anpassungen des biometrischen Authentifizierungsprozesses für das Tippverhalten einführt. Grundlegend für diese Erweiterungen ist die Adaption des Tippverhaltens in eine andere Umgebung. Es sind bereits verschiedene Möglichkeiten in Studien nachgewiesen, wie das Tippverhalten als Authentifizierungsmethode angewendet werden kann [BC08, ZSKF09]. Diese Studien beziehen sich allerdings alle, wie in der Motivation (siehe Abschnitt 1.1) bereits beschrieben, auf reine Hardwaretastaturen. Heutzutage sind Smart-

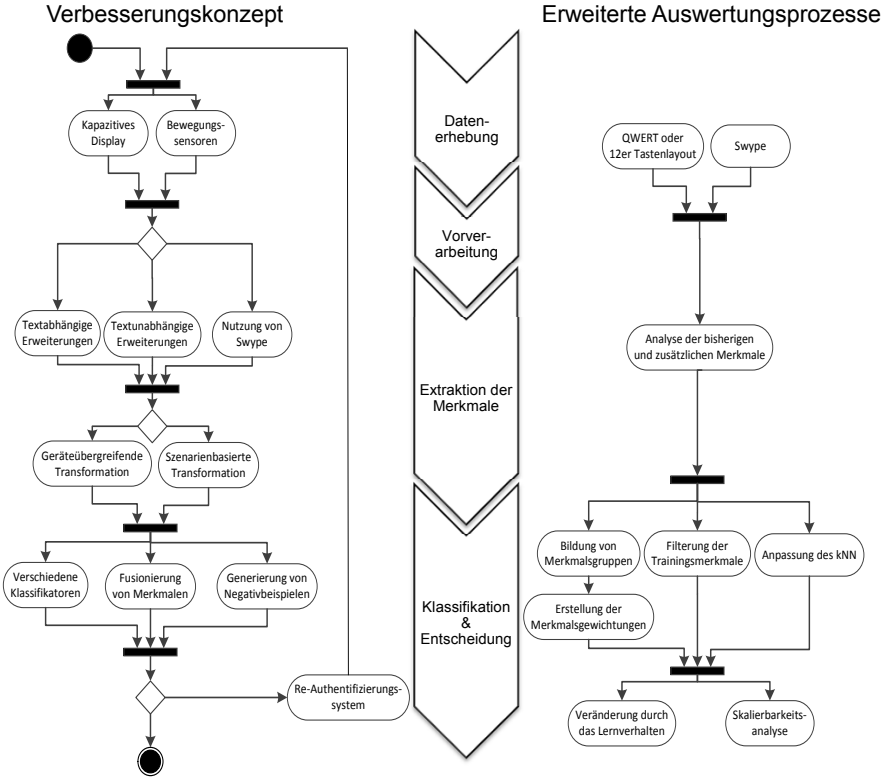


Abbildung 3.2: Grundlegende methodische Erweiterungen

phones mit kapazitiven Displays verbreitet [HYJ+12], bei denen die Tasten dargestellt werden, aber physisch nicht vorhanden sind. Ein naiver Ansatz wäre, die bestehende Authentifizierungsmethode mittels des Tippverhaltens für Smartphones identisch zu übernehmen. Prinzipiell ist diese Übertragung möglich (mit höheren Fehlerraten), doch können diese Fehlerraten durch neue Daten des kapazitiven Displays verringert werden. Die Analyse für diese Daten erfolgt mit einer Standard QWERT-Tastatur. Darüber hinaus erfolgt ein Vergleich zu einem Tastaturlayout mit 12 Tasten, das vor allem bei Mobiltelefonen

mit Hardwaretasten verwendet wird. Gleichzeitig wird die Erkennung auf einer QWERT-Tastatur mittels Wischmuster betrachtet, das eine Erweiterung der 3x3 Punktematrix von De Luca et al. [DLHB+12] aus Abschnitt 3.1.1 darstellt.

Aus den Daten werden neue Merkmale extrahiert, die in Abschnitt 6.2 genauer beschrieben und deren Vorteile in Abschnitt 5.3.1 durch einen Vergleich aufgezeigt werden. Gleichzeitig wird gezeigt, dass nicht nur eine textabhängige Authentifizierung durchgeführt wird, sondern auch eine textunabhängige Authentifizierung, bei der kein spezielles Passwort abgefragt wird. Zudem werden neue Merkmale für die Erkennung des Wischmusters vorgestellt und analysiert.

Die Merkmale sind gerätespezifisch, weswegen ein Konzept vorgestellt wird, mit dem es möglich ist, eine geräteübergreifende Authentifizierung durchzuführen (siehe Kapitel 6). Im ersten Schritt erfolgt eine gerätespezifische Authentifizierung, bei der zunächst analysiert wird, welche Abhängigkeiten die entsprechenden Geräte auf die Fehlerraten besitzen. Aufbauend auf diesem Ergebnis erfolgt die geräteübergreifende Authentifizierung, bei der das Enrolment auf einem Gerät und durch eine Transformation des Merkmalmodells für ein anderes Gerät durchgeführt wird, um sich an diesem zu verifizieren. Bei erfolgreicher geräteübergreifender Authentifizierung wird nur ein Enrolment benötigt, andernfalls muss für jedes Gerät (aufgrund der unterschiedlichen Sensoren) ein individuelles Enrolment erfolgen.

Ein weiterer wichtiger Bestandteil des Konzeptes ist die Erkennung von Szenarien, die eine Veränderung des Tippverhaltens bewirken (siehe Kapitel 7). Daher wird analysiert, welchen Einfluss die Szenarien auf das Tippverhalten haben und wie hoch die Fehlerraten sind, wenn ein Enrolment und eine Verifizierung im gleichen Szenario erfolgen. Gleichzeitig wird eine Transformation vorgestellt, in der ein Enrolment im Sitzen erfolgt und dieses Merkmalmodell in andere Szenarien überführt wird.

Während des letzten Prozessschrittes der biometrischen Authentifizierung werden verschiedene Klassifikatoren für die Authentifizierung betrachtet. Dazu werden Verbesserungen u. a. eines statistischen Klassifikators vorgestellt. Des Weiteren wird auf die Fusion der Merkmale

eingegangen, wobei analysiert wird, welche der bisherigen und der zusätzlichen Merkmale geeignet sind, um die Qualität der Authentifizierung zu verbessern. Diese Betrachtung erfolgt aufgrund der statistischen Daten und den errechneten Fehlerraten. Darauf aufbauend erfolgen die Gewichtung und die Bildung von Gruppen für die Fusion der Merkmale, wodurch die Fehlerraten bei der Klassifikation verringert werden können. Die Klassifikation erfolgt in dieser Arbeit auf Basis einer Verifikation einer Person, da die Fehlerraten bei einer Identifikation höher sind (laut Olzak [Olz06, S. 8]). Darüber hinaus erfolgt eine Filterung der Merkmale während des Trainings, damit Ausreißer eliminiert werden.

In den bisherigen Studien existieren immer Negativbeispiele, die genutzt werden, damit ein System trainiert wird, unter welchen Bedingungen es eine Person ablehnen soll. Für eine reale Situation, bei der diese Negativbeispiele nicht existieren, wird eine Generierung dieser Negativbeispiele vorgestellt.

Ein weiterer Punkt, der im Anschluss analysiert werden muss, ist u. a. das Lernverhalten, da sich das Tippverhalten über die Zeit verändert. Trotz dieser Veränderung wird gezeigt, wie sich eine Person dennoch weiter authentifizieren kann. Zusätzlich wird eine Skalierbarkeitsanalyse durchgeführt, um zu zeigen, welche Auswirkung eine große Personenmenge auf die Fehlerrate besitzt.

Abschließend wird auf die Generierung eines Re-Authentifizierungsprozesses eingegangen (siehe Kapitel 8). Der Hauptteil bisheriger Studien bezieht sich auf die initiale Authentifizierung vor der eigentlichen Nutzung. Der vorgestellte Prozess (siehe Abschnitt 8.2.4) liefert eine höhere Sicherheit während der Benutzung des Gerätes, da dauerhaft eine Überprüfung der Identität im Hintergrund erfolgt. Dieses Teilkonzept wurde bereits im Rahmen einer Publikation vorgestellt [TO13a]. Der Abschnitt 8.2 bezieht sich größtenteils auf diese Veröffentlichung. Bausteine für diesen Prozess sind die Authentifizierungen mittels einer textunabhängigen Authentifizierung und die Bewegungserkennung mithilfe der verbauten Sensoren.

Damit dieses Gesamtkonzept analysiert werden kann, wird im nächsten Kapitel auf die durchgeführten Studien eingegangen.

4 Struktur zur Versuchsdurchführung

Für die Erreichung der Ziele aus Abschnitt 1.2 wurden neun Studien durchgeführt. Die Unterschiede der Datenerhebung dieser Studien werden im Folgenden definiert. Des Weiteren wird auf die Teilnehmer der Studien eingegangen und abschließend der Bezug zu den durchgeführten Analysen hergestellt. Als Letztes wird ein Überblick über die Studienapplikationen gegeben.

4.1 Aufbau des Hauptteils der Studien

Es wurden acht Studien durchgeführt, bei denen verschiedene Passwörter mit klein geschriebenen Buchstaben analysiert wurden (bis auf eine Studie, bei der zusätzlich Zahlen verwendet wurden). Bei einer weiteren Studie wurden nur Bewegungen aufgenommen. Grundlegend sollen keine wirklich zu verwendenden Passwörter dargestellt werden, da diese einen zu langen Lernprozess benötigt hätten (Verinnerlichung, welche Buchstaben nacheinander folgen), sondern Wörter, die jeder Proband kennt. Die groben Unterschiede in der Hauptphase werden im Folgenden beschrieben, wobei die detaillierten Informationen dem Anhang (siehe Abschnitt A.2) in der Tabelle A.1 zu entnehmen sind.

Für die ersten acht der zuvor genannten Studien wurden mithilfe des kapazitiven Displays die Zeitmerkmale (Verweildauer, Di- bzw. Trigraph) sowie Auflagefläche und Druckstärke und die genauen Koordinaten (x und y) der Berührung des Displays aufgenommen.

S1_Merkmale: Eine erste Studie wurde durchgeführt, um die neue Art von Display mit ihren Merkmalen zu testen, die über das kapa-

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_4

zitive Display extrahiert werden können (Verwendung der Daten in mehreren Veröffentlichungen [TO13c, TO13b]). Der Datenbestand umfasst 148 Tippproben des Eingabetexts *hello world*. Dieser Text wurde von 18 Probanden eingegeben, die bei ihren 10 Eingaben jeweils am Ende einer Eingabe eine Korrektur vornehmen durften. Für die Auswertung wurden nur die 148 korrekt geschriebenen Tippproben verwendet.

S2_PINPasswort: Die zweite Studie befasste sich mit der Untersuchung, wie stark die Unterschiede zwischen einem 12er-Tastaturenlayout und dem QWERT-Layout sind. Insbesondere wurde bei dieser Studie auf die numerische und alphabetische Eingabe geachtet [TO12]. 35 Testpersonen erzeugen 385 Eingaben (11 Eingaben pro Person); einmal für das Passwort *mein telefon* und einmal für die Nummer *1864559*. Eine Überprüfung des Wortes und der Nummer erfolgte nach jeder Eingabe und Korrekturen waren möglich.

S3_Text: Im dritten Schritt wurde eine Studie mit 152 Testpersonen durchgeführt, um die Skalierbarkeit dieses Verfahrens besser zu adressieren (Teilergebnisse siehe Veröffentlichung [TAO13]). Zudem wurden während dieser Studie zusätzlich die Daten des Gyroskops für die Authentifizierung verwendet.

Die Studie bestand aus zwei Teilen. Im ersten Teil wurden die Probanden in drei Gruppen aufgeteilt. Jede Gruppe bekam den identischen Text mit 306 Zeichen (siehe Abschnitt A.1), der von allen Teilnehmern einzugeben war. Die erste Gruppe hatte dafür ein Zeitlimit von 5 Minuten, die zweite 3:30 Minuten und die letzte Gruppe kein Zeitlimit. Sobald das Zeitlimit abgelaufen war, wurden keine Eingaben mehr zugelassen, sodass teilweise nicht der komplette Text eingegeben wurde. Ziel war es, die Testpersonen auf verschiedene Stresslevel zu bringen, um den Einfluss auf das Tippverhalten zu analysieren. Dieses wurde bereits in der veröffentlichten Publikation [TAWO13] und der betreuten wissenschaftlichen Arbeit [Arn12] präsentiert. Gleichzeitig wird dieser Teil der Studie für die textunabhängige Authentifizierung verwendet. Der zweite Teil der Studie

beschäftigte sich mit der klassischen, wiederholenden Eingabe eines Passwortes. Der Datenbestand beläuft sich auf 1520 Eingaben des Passwortes „koloss von rhodos“ (zweiter Teil der Studie).

S4_Lernen: Die vierte Studie befasste sich mit der Veränderung des Tippverhaltens durch wiederholte Eingabe (Effekt des Lernverhaltens). Dazu sollten die Testpersonen über 10 Tage täglich jeweils 40 Eingaben von einem Wort tätigen. Mit den 20 Probanden wurden insgesamt 8000 korrekte Tippproben für das Wort *donnerwetter* im Rahmen der Studie abgegeben.

S5_Swype: In dieser Studie wurde nicht nur das Tippen betrachtet, sondern auch die Eingabemethode Swype (siehe Abschnitt 5.2.3), bei der die einzelnen Buchstaben eines Wortes mit dem Finger bewegt werden, indem eine Linie von dem ersten bis zum letzten Buchstaben gezogen wird.

Eine Vorstudie mit gleicher Konfiguration wurde dabei durch eine betreute wissenschaftliche Arbeit mit 16 Testpersonen durchgeführt [Gra12], eine erweiterte Studie mit 42 Testpersonen im Anschluss. Bei beiden Studien wurden jeweils fünf verschiedene Wörter (*wert*, *test*, *qwertz*, *passwort* und *monogamie*) 10 Mal nacheinander geswypt. Der daraus resultierende Datenbestand für die erste Teilstudie beläuft sich pro Wort jeweils auf 160 und bei der zweiten auf 420 Tippproben.

S6_Geräte: Um den Einfluss von unterschiedlichen Smartphones zu betrachten, wurde im Vorfeld zur sechsten Studie eine Analyse von unterschiedlichen Geräten durchgeführt. Bei den 65 dafür verwendeten unterschiedlichen Gerätetypen (Gesamtzahl an Geräten: 91) konnten drei Gruppen von Geräten anhand der Druckstärke und Auflagefläche differenziert werden (siehe Abschnitt 6.1). Jeweils ein Vertreter jeder Gruppe wurde in der Hauptstudie (*Galaxy Nexus*, *Samsung Galaxy S II* und *Samsung Galaxy S III*) nacheinander von 66 Testpersonen verwendet. Bei allen 20 Eingaben pro Passwort (*treter*, *sommer*, *module*) und Gerät wurden die Orientierungsdaten während des Tippens aufgenommen. Gleichzeitig erfolgte eine Überprüfung, ob die Wörter vollständig korrekt eingegeben wurden.

Andernfalls musste der Versuch wiederholt werden. Korrekturen waren nicht möglich, da sie den Schreibfluss verändern. Daraus ergibt sich, dass alle 20 Eingaben korrekt waren und dass pro Wort und Gerät 1320 Datensätze aufgenommen wurden.

S7_Szenarien: In der siebten Studie wurde der Einfluss durch fünf unterschiedliche Szenarien auf das Tippverhalten betrachtet. Alle 80 Testpersonen hatten die Passwörter für die Studie im Stehen, im Gehen, im Sitzen, im Sitzen mit der nicht-dominanten Hand und im Sitzen unter Musikeinfluss einzugeben. Gleichzeitig wurde bei dieser Studie die Wichtigkeit der Länge eines Passwortes für die Authentifizierung mittels des Tippverhaltens analysiert. Mit den Passwörtern *anna*, *sommer*, *donnerwetter* wurden für die 20 korrekten Eingaben je Wort und Szenario 1600 Datensätze aufgenommen. Die Passwörter mussten hier korrekt und ohne zwischenzeitliche Korrekturen geschrieben werden.

S8_EigenesPasswort: Für alle Klassifikatoren werden Negativbeispiele benötigt, bei dem die Person abgelehnt werden sollte. Diese können aber nicht durch Eingaben von anderen Personen generiert werden, da sonst der WISSENS-Faktor preisgegeben wird. Das Modell muss daher aus anderen Daten generiert werden (siehe Ansatz Abschnitt 5.2.4). In der Studie konnten sich die 40 Probanden eigene Wörter wählen und mussten diese jeweils 40 Mal eingeben. Die Wörter sollten 6 bis 10 Zeichen lang sein und aus kleinen Buchstaben bestehen. Es wurde darauf geachtet, dass jeder Proband ein anderes Passwort wählte.

S9_Bewegungen: In der letzten Studie wurden Bewegungen mit dem Gerät (z. B. Gerät auf den Tisch ablegen) durchgeführt, die in der Analyse erkannt werden sollten. Es wurden dafür 19 verschiedene Bewegungen aufgenommen. Eine Liste mit allen Bewegungen und welche Rahmenbedingungen vorherrschten, wird im Abschnitt A.3 genauer definiert. Die 40 Probanden haben an einer von fünf Teilstudien teilgenommen, die unterschiedliche Aktivitäten beinhaltete. Jede Aktivität wurde mindestens sechsmal pro Proband entsprechend

den Rahmenrichtlinien ausgeführt. Für die Auswertungen wurden die Bewegungen zwischen Aktivitäten und Zuständen (z. B. wenn sich das Gerät am Ohr befindet) unterschieden.

Die bei dieser Studie verwendeten Geräte werden im nächsten Abschnitt genauer beschrieben.

4.2 Verwendete Geräte

Für die Studien wurden vier unterschiedliche Smartphones mit Android Betriebssystem verwendet: HTC Desire [CHI09], Galaxy Nexus [Sam11a], Samsung Galaxy S II [Sam11b] und Samsung Galaxy S III [Sam12]. In der folgenden Übersicht (Tabelle 4.1) werden die für die Analysen wichtigen Unterschiede zwischen den Geräten verdeutlicht:

Tabelle 4.1: Vergleich der verwendeten Geräte

Name	Display Art	Display Größe	Display Auflösung (Pixel)	Android-Version
HTC Desire	OLED	9,4 cm (3,7 Zoll)	480x800	2.2.2
Galaxy Nexus	AMOLED	11,81 cm (4,65 Zoll)	1280x720	4.0-4.2.2
Samsung Galaxy S II	Super AMOLED Plus	10,8 cm (4,27 Zoll)	480x800	4.1.2
Samsung Galaxy S III	Super AMOLED HD	12,2 cm (4,8 Zoll)	1280x720	4.1.2

Die unterschiedlichen Displayarten wurden im Laufe der Zeit weiterentwickelt und verbessert und in den folgenden Smartphones eingebaut:

HTC Desire (Veröffentlichungsjahr: 2010) – OLED; Samsung Galaxy Nexus (2011) - AMOLED; Samsung Galaxy S II (2011) – Super AMOLED Plus; Samsung Galaxy S III (2013) – Super AMOLED High Definition (HD). AMOLED steht für Active Matrix Organic Light Emitting Diode. Dieser Diode-Typ hat eine geringere Strom- und Leuchtdichte als die anorganischen Light Emitting Diode (LED) [Bun12]. Das begünstigt eine kosteneffizientere Herstellung, wobei es aktuell eine geringere Lebensdauer als bei den LEDs bedeutet. Im Vergleich zur Organic Light Emitting Diode (OLED), die eine passive Matrix verwendet, wurde u. a. die Reaktionszeit verbessert. Beide Displayarten, ebenso wie die Derivate des AMOLED, sind touchscreenfähig. Die einzelnen Arten von AMOLED können laut Smith [Smi12] wie folgt unterschieden werden: Super AMOLED hat den Berührungssensor direkt in das Display integriert und nicht in einer darüber liegenden Schicht. Gleichzeitig ist das Display bei Sonnenlichteinstrahlung besser lesbar. Super AMOLED Plus ist energiesparender und heller im Gegensatz zu AMOLED und Super AMOLED. Das Super AMOLED HD besitzt dagegen eine höhere Auflösung.

4.3 Implementierung der Prototypen

Der folgende Abschnitt präsentiert das Konzept der Umsetzung zur Authentifizierung und den Aufbau der Authentifizierungsanwendungen.

4.3.1 Software-Architektur

Das Konzept für die Umsetzung einer Authentifizierung mittels des Tippverhaltens wird anhand von Abbildung 4.1 detailliert erklärt.

Im Rahmen der Datenerfassung wurden die Daten von der Applikation (App), die für jede Studie angepasst bzw. neu generiert wurde, mit den Daten von der Softwaretastatur in einer Datei auf dem Gerät gespeichert. Es wurden zwei Anwendungen entwickelt, um die Tastatur appübergreifend nutzen zu können. Somit haben Updates der Tastaturanwendung einen Einfluss auf alle Auswertungen und

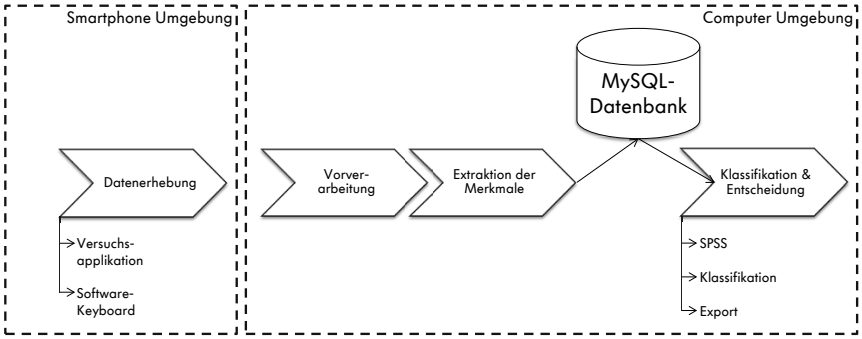


Abbildung 4.1: Genereller Aufbau des Authentifizierungsprogrammes

ermöglichen den besseren Vergleich zwischen den unterschiedlichen Studien.

Die weiteren Schritte des biometrischen Authentifizierungsprozesses, beginnend mit der Vorverarbeitung, erforderten einen klassifikationsabhängigen Berechnungsaufwand, sodass eine Weiterverarbeitung am Computer erfolgt. Grund dafür war die Prozessorleistung, insbesondere zum Ausführen der Klassifikation mit neuronalen Netzen, auf einem Smartphone der heutigen Generation. Alle Algorithmen wurden in Java programmiert, damit später eine Portierung auf ein Smartphone mit dem Betriebssystem Android [Ope08] möglich ist. Nach der Vorverarbeitung erfolgte die Extraktion von Merkmalen mit der anschließenden Speicherung in die Datenbank.

Als Auswertungstools wurden sowohl statistische Tools, wie Statistical Package for Social Scientists (Statistik- und Analyse-Software) (SPSS) als auch der abstrakte Klassifikator (siehe Abschnitt 5.2.4) sowie weitere Exports (z. B. der deskriptiven Daten) verwendet.

4.3.2 Aufbau und Ablauf der Authentifizierungsanwendungen

Grundlage für das Konzept ist das Betriebssystem Android. Dieses ist ein Betriebssystem für mobile Endgeräte, welches von der Open

Handset Alliance (OHA) entwickelt und u. a. von Google Inc. mitgegründet wurde [CBS07]. Das auf einen Linux-Kernel basierende Android wurde als quelloffene Software entwickelt [Ope13a]. Das erste Smartphone mit diesem Betriebssystem erschien im Oktober 2008 (HTC Dream [Ope08]). Heute sind iOS von Apple Inc. und Android, das von mehreren Herstellern verwendet wird, die meistgenutzten Betriebssysteme [GCML13].

Das weiterentwickelte System und alle Studienanwendungen wurden für die Version Android 4.2 (JELLY_BEAN_MR1) mit den Application Programming Interface (API) Version 17 entwickelt. Bei der Entwicklung ist eine Aufwärtskompatibilität ab Android API Version 8 gegeben, um mit möglichst vielen unterschiedlichen Geräten eine Analyse durchzuführen. Der grundsätzliche Aufbau aller Studien wird in Abbildung 4.2 ersichtlich.

In jeder Durchführung betreute der Versuchsleiter den Probanden. Während der Ausführung wurde das Gerät zwischen dem Probanden und dem Versuchsleiter gewechselt. Am Anfang und am Ende führte der Versuchsleiter dabei folgende Aktionen durch:

Einweisung: Nachdem der Proband sich bereiterklärt hat, freiwillig an der Studie teilzunehmen, erfolgte eine Studieneinweisung. Dabei wurde auf generelle und studienspezifische Aspekte eingegangen. Dazu zählten u. a. Hintergrund der Untersuchung und worauf sich der Proband einstellen muss.

Vorkonfiguration: Anschließend wurde das Gerät für die Testperson vorkonfiguriert. Je nach Studie wurde u. a. ein Zeitlimit eingestellt. Nach diesem Schritt erhält der Proband das Gerät zur weiteren Durchführung.

Beenden des Experimentes: Bei den ersten Studien wurde nach der Rückgabe des Gerätes abschließend eingetragen, welche Hand der Proband verwendet hat. In späteren Studien füllte der Proband diese Abfrage selber unter dem Punkt Abschlussfragen aus.

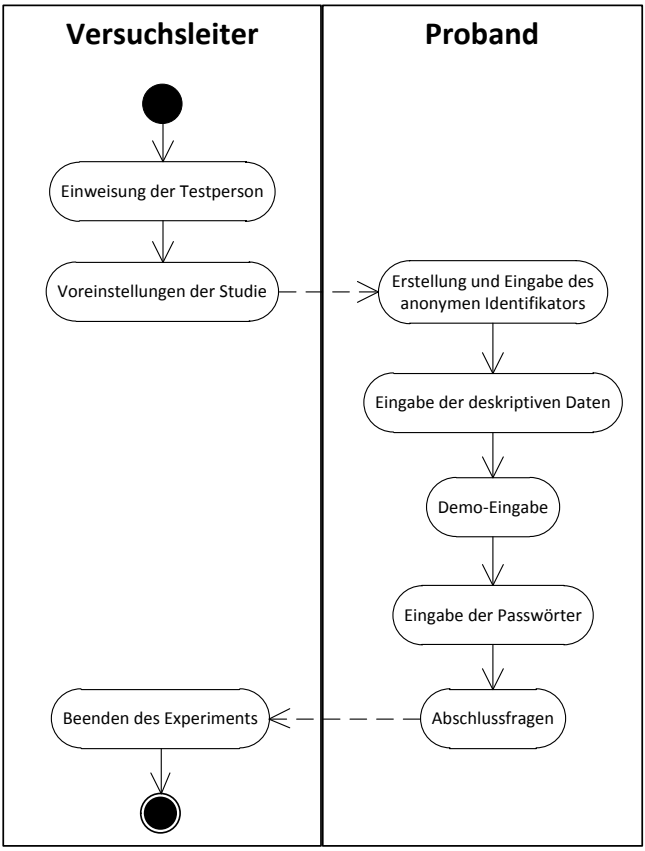


Abbildung 4.2: Genereller Ablauf der Experimente

Nach der Vorkonfiguration des Gerätes wurde das Testgerät an den Probanden übergeben. Dieser führte unter Anweisung folgende Schritte auf dem Gerät durch:

Anonymer Identifikator: Damit ein Vergleich zwischen den Studien erreicht wird, müssen die Probanden wiedererkannt werden. Um dabei die personenbezogenen Daten zu schützen, muss diese Identifizierung anonymisiert durchgeführt werden.

Das wurde durch einen anonymen Identifikator erreicht. Es muss mit diesem möglich sein, eine Person wiederzuerkennen, aber von einem Identifikator nicht auf eine Person zurück schließen zu können. Als Werkzeug kann dafür ein Code generiert werden, der aus Buchstaben und Zahlen besteht und von der Testperson selber erstellt wird [GOM02]. Gleichzeitig darf sich dieser Identifikator nicht über den Zeitraum aller Studien verändern, da sich die Person den Code sonst nicht merken kann. Der Identifikator ist in Zusammenarbeit mit F. Arndt [Arn12] entstanden. Die komplette Erklärung, die jeder Proband erhalten hat, ist in Abschnitt A.4 zu finden.

Deskriptive Daten: Auf die Eingabe des anonymen Identifikators erfolgte die Eingabe der deskriptiven Daten. Dazu zählten Geschlecht, Alter, Bildungsniveau, Erfahrung mit einem Touchscreen beim Smartphone, Erfahrung mit verschiedenen Betriebssystemen und drei Fragen zur Motivation. Sowohl eine Vorauswahl als auch Freitexte wurden dabei verwendet. Dem Anhang (siehe Abschnitt A.5) können genauere Informationen über die Form und genaue Fragen entnommen werden.

Training (Demo-Eingabe): Um für die Probanden eine möglichst gleiche Situation zu generieren, müssen alle Personen vorher mit dem jeweiligen Untersuchungsgerät die vorgegebenen Passwörter trainieren und sich somit an das Gerät gewöhnen. Gleichzeitig sollten die Passwörter geübt werden.

Hauptteil (Eingabe der Passwörter): Hier handelt es sich um den Teil der Studie, bei dem die Daten für die Klassifikation verwendet werden. Dabei werden die verschiedenen Passwörter wiederholt eingegeben. Die Anzahl der Gesamteingaben ist neben den Passwörtern und den jeweiligen Wiederholungen auch von den verwendeten Geräten, Szenarien und Eingabeformen abhängig.

Abschlussfragen: Nach der letzten Eingabe wurde der Proband gebeten anzugeben, mit welcher Hand bzw. mit wie vielen Fingern die Eingabe erfolgte.

4.4 Deskriptive Daten der Probanden

In diesem Abschnitt wird auf die Teilnehmer und deren eingegebene deskriptive Daten genauer eingegangen. Die Daten werden über die Studien akkumuliert.

Es wird auf allgemeine Informationen der Probanden eingegangen und deren Erfahrung mit mobilen Geräten, die ein Touchscreen besitzen. Der letzte Abschnitt adressiert Punkte zum Tippverhalten auf einem Touchscreen.

4.4.1 Teilnehmer der Studien

Über den Zeitraum von einem Jahr wurden 249 verschiedene Personen über die Nutzung von Smartphones mit kapazitiven Displays befragt. Abbildung 4.3 präsentiert die Verteilung von weiblichen und männlichen Probanden in Relation zu unterschiedlichen Altersgruppen.

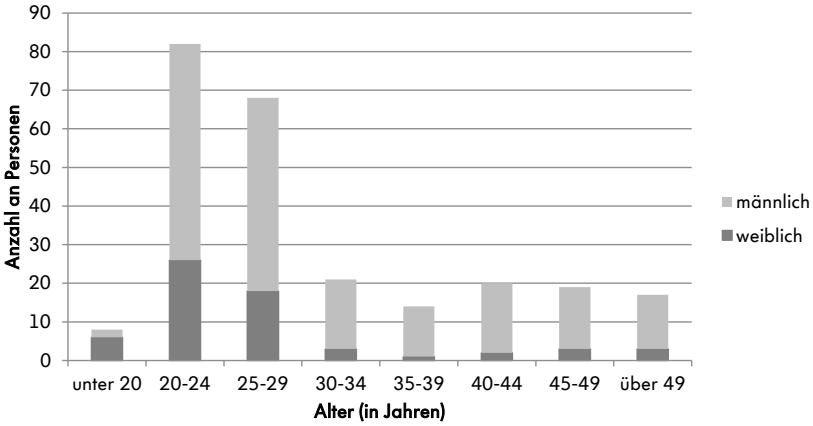


Abbildung 4.3: Verteilung der Personenaltersgruppen

Die hohe Konzentration in der Altersgruppe zwischen 20 und 29 Jahren mit einer höheren Prozentzahl an männlichen Teilnehmern lässt sich dadurch erklären, dass die meisten Testpersonen Studenten oder Mitarbeiter von IT-Abteilungen unterschiedlicher Firmen

waren. Insgesamt haben 62 weibliche Personen (25 %) an den Studien teilgenommen. Die restlichen 187 Personen sind männlich.

4.4.2 Erfahrung mit einem Touchscreen

Tabelle 4.2 zeigt die Verteilung der Erfahrung mit Smartphones in verschiedenen Altersgruppen. Zudem wird die durchschnittliche Nutzungsdauer pro Tag in der Tabelle dargestellt.

Tabelle 4.2: Verteilung der Personen mit Erfahrung mit Smartphones und deren Nutzungsdauer pro Tag.

Altersgruppe	< 20	20-29	30-39	40-49	> 49	insgesamt
Teilnehmer	8	150	35	39	17	249
Personen mit Smartphone Erfahrung	7	106	31	20	5	169
Durchschnittliche Nutzungsdauer pro Tag (in Stunden)	6,9	3,4	2,3	2,4	1,2	3,1

Insgesamt haben 169 der 249 befragten Personen Erfahrung mit einem Smartphone. Die Relation zwischen Alter und Erfahrung ist gleich. Lediglich die Personen über 49 Jahre besitzen weniger Erfahrung mit einem Smartphone. Die Dauer der Benutzung ist altersabhängig. Mit steigendem Alter nimmt die durchschnittliche Benutzungsdauer ab. Im Alter zwischen 20 und 29 Jahren haben die Probanden angegeben, mehr als drei Stunden am Tag ihr Smartphone zu nutzen, während die über 49 Jährigen das Gerät nur eine Stunde am Tag verwenden.

Die Testpersonen bevorzugen unterschiedliche Geräte. In der Tabelle 4.3 wird aufgezeigt, welche Betriebssysteme von den Testpersonen verwendet werden.

Die Personen im Test nutzen überwiegend ein Smartphone mit Android oder dem iOS Betriebssystem, was einer aktuellen Studie

Tabelle 4.3: Unterschiedliche Betriebssysteme, die von den Testpersonen genutzt werden (Mehrfachantworten sind möglich)

Betriebssystem	Anzahl	Prozent
Android OS	112	66 %
iOS	60	36 %
BlackBerry OS	17	10 %
Symbian	11	7 %
Windows Phone	7	4 %

zur Verteilung von mobilen Betriebssystemen [GCML13] sowie den Verkaufszahlen beider Systeme entspricht.

4.4.3 Einstellung der Probanden gegenüber der eingesetzten Technik

Überwiegend werden von den Teilnehmern Smartphones mit Touchscreen-Displays benutzt. Diese Geräte werden nicht nur zum Telefonieren verwendet, sondern auch, um E-Mails zu schreiben oder Anwendungen zu nutzen. In der ersten Frage mussten die Testpersonen, die ein Smartphone mit einem Touchscreen haben, ihre Erfahrung mit diesem bewerten. Dabei ging es um die Komplexität des Schreibens von langen Texten mit dieser Art von Display. Die Abbildung 4.4 beinhaltet das Umfrageergebnis, wie viele Probanden der Aussage zugestimmt haben.

Es wird sichtbar, dass die Mehrheit der befragten Personen keine Probleme mit dem Schreiben von langen Texten auf einem Touchscreen haben. Auf der einen Seite hatten 43 % keine oder wenige Probleme mit einem kapazitiven Display zu schreiben. Auf der anderen Seite hatten 28 % Schwierigkeiten mit dem Schreiben langer Texte.

Abbildung 4.5 zeigt, wie gerne die Probanden ein Touchscreen nutzen. Diese Frage wurde von mehr als dreiviertel der Probanden (76 %) mit „ja“ beantwortet. Lediglich 11 % mögen diese Art von

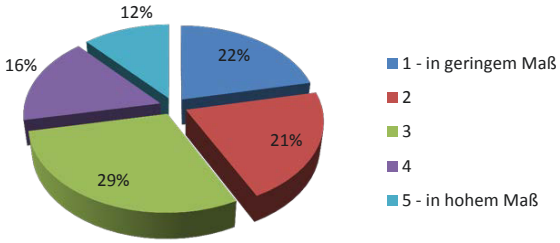


Abbildung 4.4: Aussage 1: „Texte wie E-Mails und SMS auf einem Touchscreen zu schreiben dauert mir zu lange und ist zu umständlich."

Display nicht und bevorzugen auf einem Telefon mit physikalischen Tasten zu interagieren.

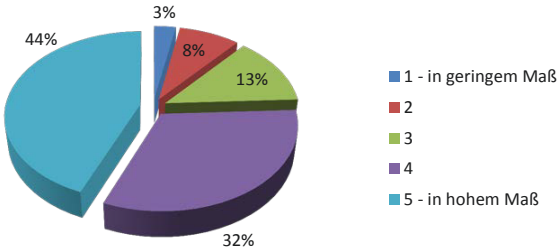


Abbildung 4.5: Aussage 2: „Ich nutze gerne das Touchscreen meines Smartphones."

Die dritte Aussage adressiert Schwierigkeiten beim Schreiben ohne physikalische Tasten. Die Ergebnisse werden in Abbildung 4.6 veranschaulicht.

60 % der Personen haben keine Schwierigkeiten mit dem Schreiben ohne physikalisches Feedback. Der Wert ist kleiner als bei dem Ergebnis für die zweite Frage, liegt aber trotzdem über 50 %. Daraus kann geschlussfolgert werden, dass mehr Personen ein Smartphone

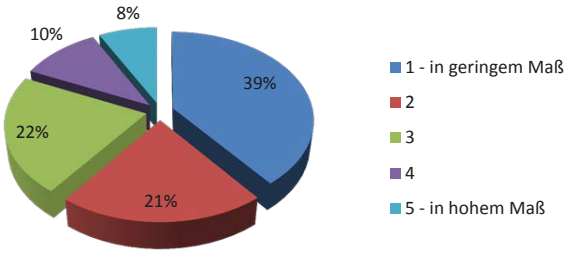


Abbildung 4.6: Aussage 3: „Es fällt mir schwer, mich ohne physikalische Tastatur beim Tippen zu orientieren."

mit Touchscreen bevorzugen als mit Hardwaretasten. Nur 18 % haben Schwierigkeiten ohne physikalische Tasten zu schreiben. Das betrifft vor allem die Altersgruppe über 40 Jahre.

4.5 Zusammenfassung

Das Tippverhalten wird durch unterschiedliche Faktoren beeinflusst. Die Entwicklung eines Authentifizierungsmechanismus mittels des Tippverhaltens kann daher nicht auf rein theoretischen Überlegungen basieren. Um die Faktoren zu analysieren, wurden eine Vielzahl von Untersuchungen in der vorliegenden Arbeit durchgeführt, deren Erläuterung im ersten Teil dieses Kapitels erfolgte. Der Datenbestand variierte dabei von kleinen Studien, wie auch viele existierende Veröffentlichungen, bis hin zu großen Studien mit Datenmengen von über 150 Personen. Neben dem großen Datenbestand wurde auf eine entsprechende Qualität der Daten durch die Analyse unterschiedlicher Eckpunkte (z. B. Geräte oder Szenarien) geachtet. Das repräsentiert viele alltägliche Situationen, die es möglich machen, eine umfassende Nutzung des Verfahrens darzustellen. Gleichzeitig konnte damit analysiert werden, wie stark sich das Tippverhalten dabei verändert.

Die verwendeten Geräte wurden definiert und ihre Unterschiede erläutert. Nicht nur die Größe des Displays ist bei der Authentifizierung

von Bedeutung. Insbesondere die Daten der unterschiedlichen Sensoren spielen eine Rolle und werden in Kapitel 6 genauer betrachtet, da diese Einfluss auf die zu exportierenden Daten während des Tippens besitzen.

Unterstützt wurden die Daten der Experimente durch die angegebenen deskriptiven Daten der Probanden, die verschiedene statistische Analysen und eine Verallgemeinerung ermöglichen. Gleichzeitig wurden bei den Studien Daten über das Nutzerverhalten der Probanden an Touchscreen-Displays aufgenommen, um die Zufriedenheit der Testpersonen mit dieser Art von Technik darzustellen.

5 Anpassungen am bisherigen Authentifizierungsprozess

Wie in Abschnitt 1.2 erläutert, existieren vier Hauptziele, die im Rahmen der Authentifizierung mittels des Tippverhaltens am kapazitiven Display erreicht und umgesetzt werden müssen. Diese vier Ziele bauen aufeinander auf, wobei die Anpassungen (Modifizierungen und Verbesserungen) am allgemeinen biometrischen Authentifizierungsprozess Grundlage für die anderen Ziele darstellen.

Dazu müssen im ersten Schritt das neue Umfeld für das Tippverhalten analysiert und die Zuverlässigkeit des Verfahrens überprüft werden. Es erfolgt ein Vergleich der Standardmerkmale und der Merkmale der neuen Sensoren sowie des alten und neuen Tastaturlayouts (12-Hardwaretasten bzw. QWERT) bzw. des Swype-Layouts. Ergänzt wird diese Analyse durch den Vergleich von unterschiedlichen Klassifikatoren und Fusionsebenen. Weiterhin wird die Veränderung durch das Lernverhalten vorgestellt. In den folgenden Kapiteln werden die drei weiteren Ziele genauer betrachtet, die auf die Erkenntnisse des ersten Ziels aufbauen.

5.1 Zielstellung für die Authentifizierung mittels Smartphone

Aktuell existieren nicht nur Smartphones mit Hardwaretasten. Durch die Weiterentwicklungen am Smartphone gibt es zusätzliche Daten, die es ermöglichen eine Authentifizierung durchzuführen. Dazu zählen unterschiedliche Displays, wie das kapazitive Display. Diese Displayart ist ein Vertreter des Touchscreens, bei dem über eine Interaktion mit der Oberfläche das Gerät gesteuert wird.

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_5

Mit der Art von Display werden Änderungen der Kapazität detektiert. Eine Unterscheidung zwischen einer gewollten Berührung oder einem Auslösen durch Schmutz oder Wasser ist schwierig [Fra11]. Daher müssen Algorithmen entwickelt werden, die diesem entgegen wirken. Ungewollte Kapazitätsänderungen, wie z. B. Kondensation im Millisekundenbereich, können als Berührungen angenommen werden und somit eine negative Auswirkung auf die Erkennungsrate haben [Fra11].

Der Vorteil beim kapazitiven Display besteht darin, dass kein Druck notwendig ist, um das Display zu bedienen: Es muss lediglich ein leitfähiger Gegenstand verwendet werden. Dabei ist das Bedienen des Displays mit Stoff-/Lederhandschuhen oder normalem Stift nicht möglich.

Bestehende Authentifizierungsmechanismen auf Basis der Analyse des Tippverhaltens wurden bisher nur auf Hardwaretastaturen (bei Computer-Tastaturen mit einem QWERT-Layout und bei den Mobiltelefonen mit einem 12er-Layout) durchgeführt. Es ergeben sich, für die im Abschnitt 1.3 vorgestellten Rahmenbedingungen folgende Ziele und Herangehensweisen, die überprüft werden müssen, wenn die Authentifizierung mittels des Tippverhaltens auf einem Smartphone mit kapazitiven Display mit einem QWERT-Layout übertragen werden soll:

- Die Fehlerraten dürfen sich zu den bestehenden Auswertungen nicht verschlechtern, sondern müssen besser, also kleiner werden. Im Umfeld der Analyse des Tippverhaltens bedeutet das, dass die Fehlerraten unter 5 % bleiben (siehe Abschnitt 3.1.1). Darüber hinaus wird in einer skandinavischen Bank von der Firma BehavioSec [Beh13a] ein System verwendet, dass sogar eine EER von nur 3,9 % aufweist.

- Damit die Fehlerraten unter der Grenze bleiben, müssen neue Daten der Sensoren extrahiert und anhand von Klassifikatoren auf ihre Eignung überprüft werden. Es muss gezeigt werden, wie stark der Einfluss der neuen Merkmale auf die Klassifikation ist und ob sich durch die neuen Merkmale die Fehlerraten verringern. Gleichzeitig

ist es erforderlich neben den Fehlerraten eine Analyse auf Basis der Bearbeitungsdauer durchzuführen, damit nachgewiesen werden kann, wie in dem vorgestellten Szenario die Authentifizierung erfolgt.

- Der Einfluss der Größe der Tasten und somit des Tastaturenlayouts muss analysiert werden. Es ist zu klären, ob die Fehlerraten durch das Tastenlayout beeinflusst werden und ob diese durch das QWERT-Layout verringert werden.

- Eine alternative Eingabemethode stellt die Eingabe eines Wischmusters dar. Es soll gezeigt werden, ob eine Authentifizierung mittels dieses Verfahrens identisch gute Fehlerraten erzeugt, wie das Tippverhalten.

- Einen weiteren Punkt stellt die Erkennung der Veränderungen des Tippverhaltens im Laufe der Zeit dar. Bei einer Veränderung soll gezeigt werden, dass eine Anpassung des Merkmalmodells einer Person erfolgen muss, um dem Lernverhalten einer Person entgegenzuwirken und weiterhin ähnliche Fehlerraten zu erzeugen.

Um diese Ziele und Herangehensweisen nachzuweisen, wird im ersten Schritt das Konzept beschrieben, welche Modifikationen am allgemeinen Authentifizierungsprozess vorgenommen werden müssen. Danach werden die einzelnen Unterziele anhand der Studien nachgewiesen, bevor sie bewertet werden.

5.2 Konzept für die Anpassungen am allgemeinen Authentifizierungsprozess

Dieser Abschnitt definiert die einzelnen Verbesserungen im Authentifizierungsprozess für biometrische Verfahren. Dafür wird zuerst auf die neuen Sensoren und deren Daten eingegangen. Folgend werden die Vorverarbeitung und insbesondere die Datenextraktion beschrieben, bevor die Klassifikationsmethoden definiert werden.

5.2.1 Datenerhebung mittels Sensoren

Smartphones besitzen neben dem kapazitiven Display auch Bewegungs- und Lagesensoren, die Daten erzeugen. Es existiert die Möglichkeit diese zur Authentifizierung zu verwenden. Dazu wird im Folgenden genauer auf die Daten dieser Sensoren eingegangen.

Kapazitives Display

Wie auch bei den Hardwaretastaturen können durch das kapazitive Display die bereits in Abschnitt 3.1 definierten Daten pro Aktion extrahiert werden. Dazu gehören der Zeitpunkt sämtlicher Aktionen, Art der Aktion (Drücken oder Loslassen) und die gewählte Taste. Diese Daten werden in der Reihenfolge ihres Auftretens als Datenfluss/Stream gespeichert.

Ein Aspekt, um die Zeit beim Enrolment zu verkürzen, ist die Extraktion von unabhängigen Daten während der Eingabe. Somit müssen die Passwörter nicht mehr so umfangreich sein, damit die gleichen Fehlerraten erreicht werden. Durch das kapazitive Display können weitere Daten aufgenommen werden. Dazu zählen die Druckstärke während der Berührung des Displays sowie die Auflagefläche und die genauen Koordinaten der Berührung. Diese werden im Folgenden genauer beschrieben. Die benötigten Informationen können beim Drücken bzw. Loslassen einer Taste, aber auch bei Bewegungen mit dem Finger auf dem kapazitiven Display extrahiert werden.

x/y-Koordinaten: Eine Standard-Computertastatur, auch als Standard Tastaturenlayout (QWERT) bezeichnet, besitzt verschiedene Hardwaretasten, bei denen analysiert werden kann, welcher Buchstabe gedrückt wurde. Im Gegensatz dazu kann bei einer virtuellen Tastatur auf einem Smartphone oder Tablet zusätzlich ermittelt werden, wo genau die Berührung auf dem Touchscreen stattgefunden hat, was in Abbildung 5.1 dargestellt wird.

Durch die genaue Bestimmung der Position des Tastendrucks besteht die Möglichkeit, die genauen Strecken zu analysieren, die der Nutzer mit dem Finger/Stift zwischen zwei Tasten zurückgelegt hat. Für n

Abbildung 5.1: Tastaturenlayout mit den x- und y-Koordinaten

Zeichen können die Koordinaten *coordX* und *coordY* mathematisch wie folgt dargestellt werden:

$$coordX = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} \in (\mathbb{N})^n \tag{5.1}$$

$$coordY = \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} \in (\mathbb{N})^n \tag{5.2}$$

Die Koordinate $(X, Y) = (0, 0)$ von einem Event stellt die untere linke Ecke des Koordinatensystems (den Ursprung) dar.

Druckstärke: Während des Berührens des Displays kann die Druckstärke, die auf das Gerät wirkt, extrahiert werden. Diese Daten wurden bereits für andere Authentifizierungsmethoden verwendet. Bei dem Experiment von De Luca et al. [DLHB+12] wurden sowohl die Druckstärke als auch die Auflagefläche verwendet, um eine Authentifizierung durchzuführen. Bei diesem Experiment musste der

Benutzer Linien ohne Absetzen zeichnen, die Punkte in einer 3x3 Matrix verbinden sollten.

Die Daten werden generell als reelle Zahlen ausgegeben, die zwischen 0,0 (niedriger) und 1,0 (höher) liegen. Dennoch ist es möglich, dass in Abhängigkeit von der Auflösung des Bildschirmes Werte über 1,0 extrahiert werden können.

$$P = \begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} \in \mathbb{R}^n \tag{5.3}$$

Ein großer Nachteil besteht darin, dass die Werte sehr stark von den unterschiedlichen Geräten abhängig sind. Verschiedene Sensoren und unterschiedliche Konfiguration der Geräte führen zu Abweichungen. Für eine geräteübergreifende Authentifizierung muss eine Normierung der Werte erfolgen.

Auflagefläche: Neben der Druckstärke kann gleichzeitig die Auflagefläche analysiert werden. Hierbei wird extrahiert, wie viele Zellen von dem aufliegenden Finger berührt werden. Äquivalent zu der Druckstärke wurde auch die Auflagefläche auf Werte zwischen 0,0 und 1,0 normiert. Tests zeigen, dass die Werte durch die Bildschirmauflösung variieren und teilweise größer werden (eigene Tests, siehe Abschnitt 6.2).

$$S = \begin{pmatrix} S_1 \\ \vdots \\ S_n \end{pmatrix} \in \mathbb{R}^n \tag{5.4}$$

Es wird deutlich, dass sowohl die Druckstärke als auch die Auflagefläche von den Gerätetypen abhängig sind. In Abschnitt 6.1 wird dies spezifiziert.

Zusätzliche Arten an Aktionen: Neben den bereits erwähnten Aktionen (das Drücken auf das Display und das Loslassen des Fingers)

gibt es weitere Aktionen, die analysiert werden. Dazu zählen unter anderem die Bewegungen auf dem Display beim Drücken mit einem Finger (siehe Abbildung 5.2). Die Anzahl dieser aufgenommenen Aktionen (*move*) ist geräteabhängig, da die Sensoren unterschiedlich konfiguriert sind.

Berühren dagegen mehrere Finger gleichzeitig das Display (Multitouch), z. B. beim schnellen Tippen von Buchstaben, gibt es weitere Aktionen insbesondere dann, wenn zwei Tasten gleichzeitig gedrückt werden. In Abbildung 5.2 werden diese Aktionen anhand des HTC Desire aufgezeigt.

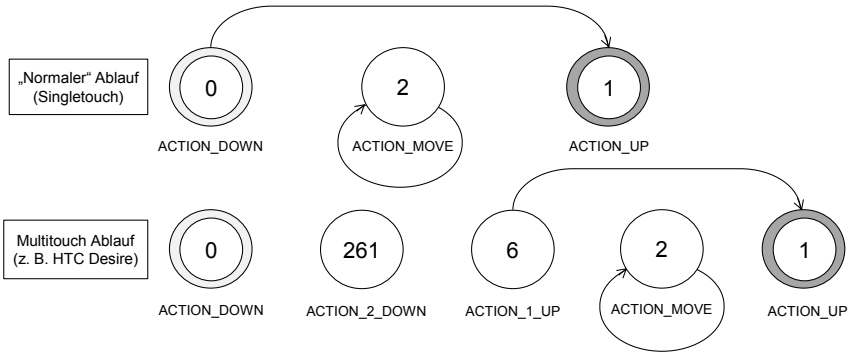


Abbildung 5.2: Verschiedene Kennzeichnungen für Aktionen

Hierbei ist zu erkennen, dass, nachdem die erste Taste gedrückt wurde, zuerst eine zweite gedrückt wurde, bevor die erste wieder losgelassen wurde. Damit in diesem Fall erkannt werden kann, welche Taste zuerst losgelassen wurde, gibt es verschiedene Codes, die jeweils eine Taste repräsentieren.

Alle Merkmale, die vom kapazitiven Display extrahiert werden können, sind die x/y-Koordinaten, Druckstärke, Auflagefläche und die Zeitstempel, die pro Event aufgenommen werden.

Lage- und Bewegungssensoren

Der Bewegungssensor (Accelerometer) gibt drei Werte mit der Einheit ($\frac{m}{s^2}$) zurück. Jeder dieser Werte entspricht einer der drei Achsen im 3-dimensionalen Raum (siehe Abbildung 5.3).

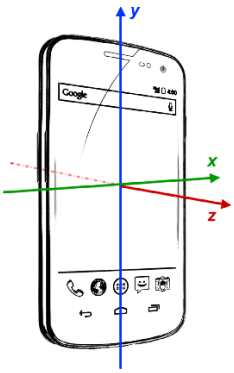


Abbildung 5.3: Das Koordinatensystem des Gerätes (Vgl. [Bee10, S. 222])

Jeder Wert des Accelerometers gibt die Bewegungsänderung für die entsprechende Achse an. Es handelt sich um die translatorische Bewegungsänderung. Für die rotatorischen Bewegungen wird das Gyroskop verwendet. Dieser 3-dimensionale Raum gilt für alle physikalischen und virtuellen Bewegungs- und Lagesensoren.

Ein weiterer Sensor ist das Gyroskop, durch das drei Werte erzeugt werden. Dieser Sensor gibt die Änderung der Geräteneigung in Form von Winkelgeschwindigkeiten ($\frac{rad}{s}$) an. Dabei wird das gleiche Koordinatensystem wie bei der Orientierung verwendet (Abbildung 5.3). Eine Rotation, die im Uhrzeigersinn durchgeführt wird, erzeugt negative Werte.

Zusätzlich können in bestimmten Szenarien die Annäherungs- und Lichtsensoren verwendet werden. Bei dem Annäherungssensor erfolgt ein Impuls, wenn sich das Gerät nah genug an einer Oberfläche befindet. In eigenen Tests, wurde je nach Gerät eine Schwankung zwischen 2 und

5 cm beobachtet. Der Lichtsensor hingegen misst die Lichtintensität der Umgebung. Insbesondere für die Bewegungserkennung kann dieser Sensor verwendet werden (siehe Abschnitt 8.3.4).

5.2.2 Vorverarbeitung

Während der Vorverarbeitung (siehe Abschnitt 2.4.1) werden verschiedene Schritte durchgeführt, wie u. a. das Analysieren der Multitouch-Events, das schon im vorherigen Abschnitt beschrieben wurde. Damit im folgenden Schritt die Merkmale für die einzelnen Tasten extrahiert werden können, müssen die entsprechenden Touch-Events einander zugeordnet werden. Für die Authentifizierung ist es notwendig, die Events (Drücken, Bewegen und Loslassen) für jede Taste aufzuteilen, so können mehr Merkmale aus den Informationen extrahiert werden (vgl. Abbildung 5.2).

Beim Prozess der Säuberung werden vor allem die Daten anhand der ActionCodes vorverarbeitet. Diese müssen überprüft werden, ob es zu jedem Drücken auf das Gerät (ActionCode = 0) auch ein Event gibt, bei dem der Finger keinen Druck ausführt (ActionCode = 1). Des Weiteren müssen die Multitouch-Events, die bei gleichzeitiger Berührung mit mehreren Fingern auftreten, in verschiedene Events und die dazugehörigen Informationen aufgelöst werden. Dazu wurde bereits in Abbildung 5.2 gezeigt, wie die Auflösung der Kennzeichnungen erfolgen muss. Der dritte Schritt ist das Extrahieren/Filtern von falschen Eingaben. Das geschieht anhand des Vergleiches mit dem einzugebenden Text.

5.2.3 Extraktion der Merkmale

Aus den extrahierten Rohdaten werden verschiedene Merkmale generiert. Die Merkmale hängen von den unterschiedlichen Anwendungsfällen ab. Diese können mithilfe des verwendeten Eingabeschemas (Tippen oder Wischen der Buchstaben) und der Textabhängigkeit, ob ein spezieller Text erwartet wird, definiert werden.

Als Eingabeform wird das Tippen oder das Wischmuster verwendet. Je nach Eingabeart werden daraus verschiedene Merkmale extrahiert. Dementsprechend werden diese zwei verschiedenen Möglichkeiten, um Merkmale bei einer textabhängigen Authentifizierung zu extrahieren, unterschieden.

Merkmalmodell für die Verarbeitung der Daten

Um das gleiche Merkmalmodell generisch für die textabhängige und textunabhängige (kein spezielles Passwort/Zeichenabfolge – siehe Abschnitt 8.2.1) Authentifizierung zu verwenden, wurde die folgende Baumstruktur entworfen (Abbildung 5.4).

Auf die textunabhängige Authentifizierung wird in Abschnitt 8.2 genauer eingegangen. Dennoch ist es unwesentlich, ob ein vorgegebener Text oder das allgemeine Tippverhalten eines nicht definierten Textes, z. B. während des Schreibens einer E-Mail [MR00, S. 353], betrachtet wird.

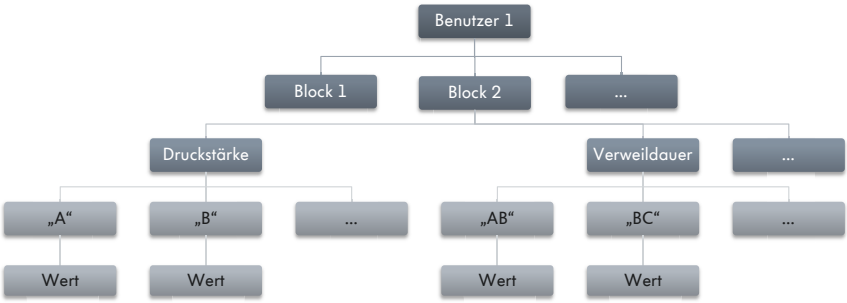


Abbildung 5.4: Baumstruktur des Merkmalmodells

Für jeden Nutzer, der auf einem Gerät verifiziert werden soll, muss ein Baum für die eigenen Merkmale generiert werden. Die verschiedenen Blöcke stellen die einzelnen Authentifizierungsversuche bei der textabhängigen Authentifizierung dar. Diese können zur Historisierung verwendet werden. Bei der textunabhängigen Authentifizierung

repräsentiert jeder Block die Eingaben in einem vorher definierten Zeitintervall. In der dritten Ebene stehen die Merkmale. Eine Ebene darunter sind die im Block auftretenden Zeichen bzw. Zeichengruppen enthalten. Nur wenn ein Zeichen getippt wird, wird es im Merkmalmodell aufgenommen. Die letzte Ebene beinhaltet die einzelnen Werte.

Textabhängige Erweiterungen beim Tippen

In dem Fall der textabhängigen Authentifizierung muss eine vorher definierte Sequenz/Passwort von einem Benutzer eingetippt werden, z. B. für die initiale Authentifizierung an einem Gerät. Das heißt, dass nicht nur die verwendeten Buchstaben, sondern auch deren Reihenfolge definiert werden müssen.

Daraus ergibt sich, dass für jeden einzelnen Buchstaben und Buchstabenfolge Merkmale extrahiert werden können. Dazu zählen sowohl die bereits verwendeten Merkmale wie Verweildauer sowie Bewegungszeit zwischen zwei oder drei Buchstaben (Di- und Trigraphen – siehe Abschnitt 3.1.1) als auch Merkmale, die durch die neuen Sensoren extrahiert werden können (Druckstärke, Auflagefläche, genaue Koordinaten sowie die Gyroskop-Daten) – siehe Abbildung 5.5.

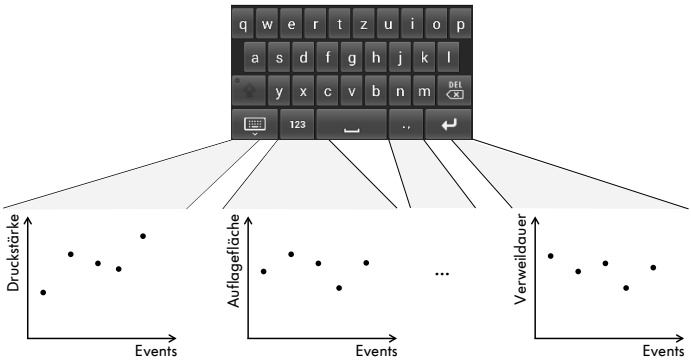


Abbildung 5.5: Extraktion verschiedener Merkmale.

Es können aus den genannten Merkmalen (z. B. bei einem fünfstelligen Passwort) 32 Werte extrahiert werden. Für jeden weiteren Buchstaben kommen dabei sieben zusätzliche Merkmale hinzu. Eine weitere Möglichkeit sind die Druckstärke, die Auflagefläche sowie die x- und y-Koordinaten nicht nur beim Drücken der Tasten zu nutzen, sondern auch während des Loslassens. Somit würden je Buchstabe zusätzlich vier weitere Merkmale hinzukommen. Eine genaue Beschreibung, welche Merkmale einen Mehrwert für die Authentifizierung haben, erfolgt in Abschnitt 5.3.1.

Die beschriebene Anzahl der Merkmale betrifft jedoch nur die Daten vom Touchscreen Sensor. Gleichzeitig können, zusätzlich über andere Sensoren, weitere Informationen entnommen werden, z. B. Daten vom Gyroskop (x, y und z) oder die der Accelerometer – siehe Abschnitt 5.2.1.

Neben den physikalischen Sensoren existieren auch virtuelle Sensoren. Diese werden aus den physikalischen Daten berechnet. Zu diesen Merkmalen zählen die Orientierungs- und DeltaRotations-Werte.

Bei den heutigen Smartphones wird die absolute Neigung durch den Erdmagnetfeldsensor und den Beschleunigungssensor (Accelerometer) berechnet [Ope13c, Ope13b]. Bei der Orientierung können die Werte Azimuth, Pitch und Roll, wie in Abbildung 5.6 zu sehen, extrahiert werden.

Die drei Werte aus Abbildung 5.6 für die Orientierung wurden bereits von Meier [Mei13] beschrieben:

Azimuth: Dieser Wert stellt den Winkel zwischen dem magnetischen Nordpol und der y-Achse (siehe Abbildung 5.3) des Geräts dar. Der Wert liegt dabei zwischen 0° bzw. 360° (Gerät zeigt Richtung Norden) und 180° (Richtung Süden) und funktioniert wie ein Kompass. Dadurch, dass sich die Himmelsrichtung bei jeder Eingabe ändern kann und nicht benutzerabhängig ist, ist es nicht als einzelnes Merkmal für die Authentifizierung geeignet.

Pitch: Der zweite Wert (Pitch) stellt die Drehung um die x-Achse des Gerätes dar. Dabei liegt der Wertebereich zwischen -180° und 180°. Bei einem positiven Wert wird die positive z-Achse in Richtung der

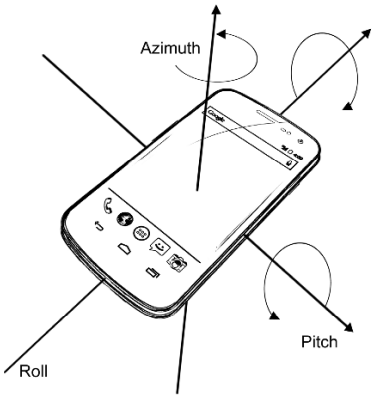


Abbildung 5.6: Die drei Neigungsachsen eines Gerätes (Vgl. [Bee10, S. 222])

positiven y-Achse gedreht. Wenn der Wert negativ ist, dann wurde die positive z-Achse in Richtung der negativen y-Achse gedreht.

Roll: Bei dem Roll-Wert handelt es sich um eine Bewegung, bei der das Gerät um die eigene y-Achse gedreht wird. Der Wertebereich liegt hier zwischen -90° und 90°. Positive Werte werden extrahiert, wenn sich die positive z-Achse in Richtung der positiven x-Achse dreht. Die negativen Werte erfolgen analog zum Pitch-Wert (positive z-Achse in Richtung der negativen x-Achse).

Inclination: Zusätzlich kann über die Methode *getInclination* der Neigungswinkel des Gerätes bestimmt werden.

Weitere Merkmale stellen die DeltaRotation Vektoren dar. Diese werden aus den Gyroskop-Daten berechnet (siehe Abschnitt 5.2.3). Im weiteren Verlauf werden diese als Delta0, Delta1, Delta2 und Delta3 bezeichnet.

Mit diesen Merkmalen erfolgt im nächsten Authentifizierungsschritt eine Klassifikation für die textabhängige Authentifizierung.

Merkmale beim Wischen

Swype ist eine Eingabemethode, die für Touchscreen Displays von der Swype Inc. entwickelt wurde. Grundsätzlich wird hierbei ein Wort auf dem Display durch Wischen über die Tasten erzeugt. Dabei wird der erste Buchstabe des Wortes gedrückt und danach ohne Loslassen des Fingers zum nächsten Buchstaben gezogen, bis der letzte Buchstabe des Wortes erreicht ist. Die Buchstaben werden durch Richtungsänderungen erreicht. Nach dem letzten Buchstaben kann der Finger das Display wieder loslassen. Dieser Ablauf wird in Abbildung 5.7 sichtbar. Doppelte Buchstaben können dabei durch Verweilen auf diesen Buchstaben erzeugt werden oder durch Zeichnen eines Kreises auf dem Buchstaben. Die Sensorik des kapazitiven Displays, die im Hintergrund arbeitet und zyklisch Daten aufnimmt, versucht das Wort mithilfe eines Wörterbuches zu erkennen. Am Anfang muss das System noch trainiert werden, indem der Benutzer dem System die Information gibt, welches Wort gemeint ist.

Abbildung 5.7: Swypen des Wortes „hello“ [Swy12]

Swype ist im Gegensatz zum reinen Tippen eine Eingabeform, bei der der Finger nur einmal pro Wort auf das Display gedrückt und wieder losgelassen wird. Daher sind bei dieser Eingabemethode andere Merkmale notwendig, um die Fehlerraten zu minimieren. Ein erster Ansatz ist es, verschiedene statistische Werte von den einzelnen Sensordaten zu extrahieren. Dazu zählen:

- Minimum,

- Maximum,
- Durchschnitt sowie
- Varianz.

Diese können z. B. auf die Eingabe der Druckstärke angewendet werden. Dabei wird der Druck von jedem einzelnen Event genommen und zusätzlich der Durchschnitt aller Druckwerte gebildet. Diese Methode wäre für die Druckstärke, Auflagefläche sowie die genauen Koordinaten x und y möglich. Für die Zeit kann dagegen nur ein Wert (Länge der Eingabe) extrahiert werden. Zusätzlich ist eine Gesamtlänge der Linie, die gezogen wurde, über die x- und y-Koordinaten berechenbar. Selbst bei gleichen Wörtern weicht dieser Wert jedoch stark voneinander ab, u. a. durch die unterschiedliche Art, wie Doppelbuchstaben gewischt werden. Daraus ergibt sich eine Summe von 18 Werten, die extrahiert werden können.

Darüber hinaus kann Swypen nicht nur als reines Tippverhalten gesehen werden, sondern eher als eine Kombination des Tippverhaltens mit einer Unterschriftenerkennung (siehe Abschnitt 2.4.2). Daraus ergeben sich weitere Möglichkeiten mithilfe der Unterschriftenerkennung bzw. Handschrifterkennung Merkmale zu extrahieren.

5.2.4 Klassifikatoren und Entscheidung

Bei der Klassifikation ist neben der Wahl des richtigen Klassifikators auch dessen Konfiguration entscheidend. Darüber hinaus wird in diesem Abschnitt eine Methode vorgestellt, wie die Trainingsdaten gefiltert werden und welche Klassifikatoren eingesetzt werden können. Mit der geeigneten Wahl der Klassifikation, kann zur Laufzeit eine Authentifizierung durchgeführt werden.

Klassifikationsauswahl

Es existieren bereits eine große Anzahl an validierten Klassifikatoren. Viele Klassifikatoren werden dabei von Weka (siehe Abschnitt 3.1)

abgebildet. Bei Nutzung von Weka können unterschiedliche Klassifikatoren verwendet werden. Der entscheidende Nachteil für die Authentifizierung mit diesem Tool ist aber, dass bei der Berechnung von FAR und FRR für jeden der n Nutzer ein eigenes Modell erzeugt werden muss, wenn verifiziert wird. Gleichzeitig ist es dadurch kompliziert, unterschiedliche Merkmalskombinationen für einen Testfall abzubilden oder aber auch verschiedene Verhältnisse zwischen Trainings- und Testdaten darzustellen.

Die Lösung dafür ist, die Klassifikatoren von Weka zu nutzen und sich einen eigenen, abstrakten Klassifikator zu generieren, der verschiedene Operationen vor der eigentlichen Klassifikation durchführt. Als Eingabe sollten dabei generell alle extrahierten Merkmale mit folgenden Punkten dienen:

Klassifikator: Es ist sinnvoll, unterschiedliche Klassifikatoren zu verwenden, aber es sollte auch möglich sein, mehrere Klassifikatoren gleichzeitig auszuwählen.

Authentifizierungsmodus: Je nach verwendeten Klassifikator kann gewählt werden, ob eine Verifikation oder Identifikation durchgeführt werden soll.

Passwort: Genau wie bei Weka sollten alle Daten nacheinander gelistet sein. Damit der abstrakte Klassifikator einfacher erkennen kann, welcher Wert zu welchem Merkmal gehört, sollte das verwendete Passwort angegeben werden.

Datensplittung: Das Aufsplitten in Trainings- und Testdaten sollte u. a. in Abhängigkeit der Wiederholungen erfolgen. In den vorgestellten Szenarien (siehe Abschnitt 7.1) müssen die Testpersonen, je nach Studie, eine größere Menge an Wiederholungen eingeben, wodurch mehr Testdaten verwendet werden können. Gleichzeitig sollte es möglich sein, eine reale Situation darzustellen, bei der eine Person ein Enrolment von drei bis fünf Wiederholungen vollzieht und die Wiederholungen danach als Authentifizierungsversuche gelten können.

Merkmalssplittung: Durch die Verwendung von mehreren neuen Merkmalen ist es wichtig, diese und auch die bestehenden separat sowie in einzelnen Kombinationen testen zu können. Deswegen muss die Auswahl der Merkmale für einen Klassifikationszyklus flexibel sein.

Merkmalsgewichtung: Dadurch, dass einzelne Merkmale unterschiedlich zur Authentifizierung geeignet sind, sollten diese Merkmale differenziert gewichtet werden. Damit kann bei der Authentifizierung ein besseres Ergebnis (kleinere Fehlerraten) erreicht werden.

Fusionsebene: Die Entscheidung, auf welcher Ebene die Fusion geschehen soll, muss durch eine Analyse, gerade mit Fokus auf multibiometrische Verfahren, durchgeführt werden. Daher ist es wichtig, dies im abstrakten Klassifikator zu konfigurieren.

Mit diesem abstrakten Klassifikator kann nachgewiesen werden, welche Klassifikatoren für die Authentifizierung mittels des Tippverhaltens an einem Smartphone mit kapazitivem Display besser geeignet sind. Doch die Fehlerraten sind nicht das einzige Kriterium zur Entscheidung für einen Klassifikator. In dem vorgestellten Szenario ist es entscheidend, dass das Verfahren direkt auf dem Gerät durchgeführt werden kann. Dadurch muss die Bearbeitungszeit für Enrolment und Verifikation so gering sein, dass der Benutzer nicht gestört wird. Anhand dieser Kriterien muss ein Klassifikator ausgewählt werden, der im Weiteren für die Authentifizierung verwendet wird (Auswertung siehe Abschnitt 5.3.2).

Der nächste Schritt ist die Analyse, welche Merkmale verwendet werden sollen. Durch die Bestimmung der Fehlerraten für die einzelnen Merkmale kann auf eine Gewichtung der Merkmale geschlossen werden. Merkmale mit geringeren Fehlerraten sollten generell höher gewichtet werden als Merkmale mit einer höheren Fehlerrate, damit bei einer Fusion bessere Ergebnisse erreicht werden können. Besonders bei statistischen Klassifikatoren ist dabei ein Augenmerk auf diese Gewichtungen zu legen. Eine manuelle Konfiguration sollte für Pre-Tests existieren. Für eine Gesamtauswertung empfiehlt sich jedoch ein automatisierter Prozess. Eine Brute-Force-Methode (vollständige

Suche) benötigt für die Generierung einer optimalen Konfiguration der Gewichtungen für die Merkmale zu lange und ist zu rechenaufwendig. Merkmale, die separat eine bessere Fehlerrate erzeugen als andere, sollten dabei von Anfang an eine höhere Gewichtung erhalten. Somit ist es notwendig, im Vorfeld die besten Konfigurationen für eine Merkmalsgruppe zu bestimmen. Die daraus resultierenden Fehlerraten müssen sortiert und gewichtet werden. Dabei ist zu betrachten, dass die guten Merkmale (geringe Fehlerraten) nicht linear stärker gewichtet werden als Gruppen mit hohen Fehlerraten. In Abschnitt 5.3.1 wird daher gezeigt, welchen Einfluss eine Gewichtung hat. Insbesondere wird dazu eine Gewichtung eingeführt, die Merkmale mit niedrigen Fehlerraten höher gewichtet. Dazu soll experimentell die folgende Formel analysiert werden:

$$f(x) = \left(\frac{1}{x}\right)^{y} \text{ für y} \geq 1, \text{ y } \in \mathbb{R} \tag{5.5}$$

Der x-Wert in der Funktion stellt die EER eines Merkmales dar. Der Exponent (y-Konstante) gibt an, wie stark die Gewichtung reduziert wird. Je höher der Wert wird, desto höher werden die Merkmale mit den besseren EER's gewichtet. Es muss bei der Evaluation nachgewiesen werden, ob dieses Verfahren geringere Fehlerraten erzeugt als eine klassische Fusion ohne Gewichtung und als eine Fusion mit der Brute-Force Methode (die wegen ihrer Berechnungsdauer auf Gewichtungen von null bis acht minimiert wird).

Verbesserung der Klassifikation durch Filterung der Trainingsmerkmale

Zusätzlich zu den zuvor beschriebenen Aspekten muss eine Anpassung des Enrolmentprozesses u. a. für den statistischen Klassifikator erfolgen. Im Gegensatz zu passiven Verfahren existieren bei aktiven Verfahren größere Unterschiede zwischen den einzelnen Authentifizierungsversuchen. Es ist sinnvoll, Fehlereingaben oder ein untypisches Verhalten beim Training des Modells nicht zu berücksichtigen. So können kurzzeitige Ablenkungen des Nutzers eine größere Pause zwischen

zwei Buchstaben bewirken. Das würde die Daten für eine statistische Klassifikation besonders verzerren. Extremwerte bzw. Ausreißer bei der Eingabe sollten daher entfernt werden und nicht in das Modell einfließen (in beide Richtungen, sowohl Minimum als auch Maximum). Jedes Merkmal wird zuerst einzeln klassifiziert und danach werden die Daten fusioniert. Damit wird das Problem von zu vielen Dimensionen bei der Klassifikation umgangen.

Der Ablauf erfolgt für jedes vorgestellte Merkmal x_i mit den Wiederholungen n:

1. Berechnung des Mittelwerts $\varnothing x$
2. Berechnung der Standardabweichung s
3. Extrahierung der Werte, wenn diese außerhalb der Standardabweichung liegen:

$$isInArea(x_i) = \begin{cases} wahr, & wenn\ ((x_i > (\varnothing x_i + \lambda * s_i)) \\ & oder\ (x_i < (\varnothing x_i - \lambda * s_i))) \\ falsch, & sonst \end{cases} \quad (5.6)$$

Mit der Variable λ kann das Intervall verkleinert bzw. vergrößert werden. Diese Variable muss in einer Voruntersuchung bestimmt werden.

Erweiterungen des kNNs

Für die Erstellung des Merkmalmodells werden nur die noch verbliebenen Werte verwendet. Für den in Abschnitt 2.4.1 vorgestellten kNN wurden zwei eigene Klassifikatoren im Rahmen dieser Arbeit für die Authentifizierung entwickelt. Besonders in Bereichen, in denen die Benutzerfreundlichkeit eine große Rolle spielt (kleine FRR), ist der kNN anfällig, wenn die Merkmale für eine Person stark variieren.

kNN zum Verifizieren: Für das Training werden die Datensätze für eine Klasse in einer Liste mit den entsprechenden Merkmalen gesammelt. Für jedes Merkmal wird ein Mittelwert bestimmt. Bei

der Evaluation wird über jede einzelne Klasse in der Liste iteriert und bestimmt, welche dem zu evaluierenden Datensatz sie am ähnlichsten ist. Es wird die Distanz für jedes Merkmal berechnet und damit jeweils eine Klassifikation durchgeführt. Bei dem Vergleich für die Evaluation wird für jedes Merkmal die Klassifikation mit 0,0 (nächstgelegenen) bis 1,0 (am weitesten weg gelegenen) klassifiziert. Diese einzelnen Bewertungen für die zu verifizierende Klasse werden zusammengefasst. Nur bei Erreichen eines vorher definierten Schwellenwertes ist die Verifizierung erfolgt.

Schwellenwertbereich um den Mittelwert: Aufbauend auf das Entfernen der Ausreißer erfolgt die Generierung des Modells auf Grundlage des neuen Mittelwertes und der Standardabweichung. Diese Daten werden für jedes einzelne Merkmal pro Benutzer gespeichert. Mittels der Negativbeispiele (Authentifizierungsversuche anderer Personen mit dem gleichen Passwort) werden die Inter-Klassen-Unterschiede analysiert, wie in Abbildung 5.8 zu erkennen ist.

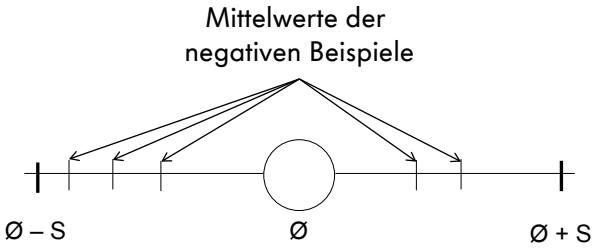


Abbildung 5.8: Inter-Klassen-Unterschiede

Sind die Unterschiede kleiner als die Standardabweichung des Modells, wird für beide Seiten ausgehend vom Mittelpunkt des Modells die durchschnittliche Entfernung der Mittelwerte der Negativbeispiele gebildet und als oberer und unterer Schwellenwert in dem Modell eines Benutzers gespeichert. Bei der Evaluation werden die aktuellen Werte mit dem in dem Modell gespeicherten überprüft. Damit wird eine bessere Genauigkeit bei der Erkennung gewährleistet.

5.3 Evaluierung des Konzeptes

Der Einfluss der Eingabeform mittels neuer Sensoren wird in diesem Abschnitt anhand der in Abschnitt 4.1 vorgestellten Studien dargestellt. Dazu erfolgt eine Analyse der zu verwendenden Merkmale und Klassifikatoren. Zusätzlich werden die verschiedenen Eingabeformate bzw. -techniken präsentiert.

5.3.1 Merkmalvergleich für die Klassifikation

In Studien wurde bereits die Güte der existierenden Merkmale analysiert. Die Studie von Karatzouni et al. [KC07] zeigt, dass der Digraph eine Person besser charakterisiert als die Verweildauer. Die Bestätigung der Aussage für das kapazitive Display und welche Merkmale geringe Fehlerraten aufweisen, beschreibt der folgende Abschnitt.

Fehlerraten einzelner Merkmale

Um die Frage zu beantworten, welche Merkmale für die Klassifikation geeignet sind, wurden die Daten aus der Studie **S6_Geräte** mit dem Passwort *sommer* auf dem Gerät Galaxy Nexus verwendet. Die extrahierten Merkmale wurden separat mit dem statistischen Klassifikator (Verifikation) evaluiert. Merkmale mit einer „2“ am Ende stellen (außer bei Delta) Merkmalsausprägungen während des Loslassens der Taste dar. Die Resultate der beiden Fehlerraten (Durchschnitt $\varnothing x$ und Varianz s) sind in Tabelle 5.1 dargestellt.

Anhand Tabelle 5.1 ist zu erkennen, dass die Fehlerraten sehr stark von den verwendeten Merkmalen abhängig sind. Im Wesentlichen können die Merkmale anhand der Fehlerraten in zwei Klassen bezüglich der Qualität der Fehlerraten eingeteilt werden. Die Standardmerkmale (Di-, Trigraph und Verweildauer) bilden zusammen mit den Merkmalen des kapazitiven Displays die erste Klasse, die eine hohe Erkennungsrate einer Person mit einer kalkulierten EER bis zu 10,6 % hat. Für die Merkmale des kapazitiven Displays sind zusätzlich die Werte während des Loslassens der Taste mit aufgeführt. Diese bieten eine ähnlich gute Erkennung der Person. Die zweite Klasse stellen die Bewegungs- und

Tabelle 5.1: Unterschiede in den Fehlerraten bei den verschiedenen Merkmalen (in %), die besten FAR und FRR sind grau markiert.

Merkmal	Anzahl Werte	Anzahl der Ausprägungen	Kalkulierte EER	FAR		FRR	
				$\varnothing x$	s	$\varnothing x$	s
Verweildauer	6	138	14,2	14,1	0,3	14,2	19,2
Digraph	5	740	14,1	14,1	0,3	14,3	17,3
Trigraph	4	1130	17,0	15,7	0,3	18,6	21,2
Druckstärke	6	132	10,6	12,4	0,2	9,0	13,3
Druckstärke2	6	128	23,8	21,9	0,3	26,0	22,7
Auflagefläche	6	10	17,4	23,3	0,3	11,7	16,6
Auflagefläche2	6	8	17,4	21,7	0,3	13,2	16,7
x-Koordinaten	6	292	18,7	17,2	0,3	19,9	20,9
x2-Koordinaten	6	1348	17,6	20,2	0,3	14,7	16,5
y-Koordinaten	6	254	21,3	23,4	0,3	19,1	18,1
y2-Koordinaten	6	1135	20,2	21,8	0,3	18,6	17,6
Pitch	6	3116	36,4	23,8	0,5	49,4	34,6
Roll	6	3010	39,6	36,1	0,5	43,4	31,2
Inclination	6	6988	37,0	40,5	0,4	33,4	23,7
GyroX	6	1868	39,7	40,6	0,3	38,8	22,0
GyroY	6	1858	43,9	25,6	0,4	62,4	25,5
GyroZ	6	1855	40,7	36,1	0,4	45,2	25,5
Delta0	6	1492	42,2	31,6	0,4	52,8	26,9
Delta1	6	1485	44,9	30,2	0,4	60,4	27,5
Delta2	6	1479	43,3	16,5	0,4	70,3	23,4
Delta3	6	1480	43,9	34,7	0,5	53,2	35,0

Lagesensoren dar, die eine kalkulierte EER von mindestens 36,4 % besitzen. Dabei wurde der Azimuth nicht mit aufgeführt, da er die Richtung, in die das Gerät zeigt, repräsentiert. Aber selbst Merkmale, die basierend auf den Fehlerraten (kalkulierte EER zwischen 35 % und 50 %) nicht geeignet sind, können während der Fusion zu einer Verbesserung der Ergebnisse führen.

Allgemein ist zu erkennen, dass die Standardabweichung bei der FAR deutlich kleiner ist als bei der FRR. Dennoch sind die Standardabweichungen für beide Fehlerraten konstant beim Vergleich zwischen den Merkmalen. Es existieren deutlich mehr Angriffsversuche als ordentliche Authentifizierungsversuche (65:1), da die Evaluierungsdatensätze von allen 66 Personen für jede Person getestet werden. Die kleine Anzahl an Versuchen der zu authentifizierenden Person führt dazu, dass bei einer oder zwei falschen Eingaben die FRR für die Person sehr stark ansteigt, somit sind die größeren Unterschiede der Standardabweichung bei der FRR zu erklären. Bei einer oder zwei falsch authentifizierten Personen hingegen verändert sich die Gesamtfehlerrate kaum. Bei einer gleich großen Testmenge von Angreifern und ordentlichen Anmeldungen sollten die Ergebnisse gleich stark schwanken.

In Tabelle 5.1 ist zudem erkennbar, dass die Menge unterschiedlicher Werte für diese Merkmale keinen direkten Einfluss auf die Fehlerraten besitzt. Die Auflagefläche hat acht bzw. zehn unterschiedliche Ausprägungen, bietet aber deutlich bessere Fehlerraten als die Bewegungs- und Lagesensoren.

Im nächsten Abschnitt wird eine Begründung für diese Ausprägungen anhand von Intra- und Inter-Personen-Unterschieden der Merkmale (somit über statistischen Kenngrößen) dargestellt.

S6_Geräte – Auswertung der Güte einzelner Merkmale

Eingabedaten:

- Passwort: *sommer*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Je Untersuchung ein Merkmal des kapazitiven Sensors, Bewegungs- oder Lagesensors

- Klassifikator: kNN

  Ergebnis:

- Einzelne Merkmale weisen unterschiedliche Fehlerraten auf.
- Kapazitive Daten eignen sich besser als Daten von Bewegungs- und Lagesensoren.

Statistische Kenngrößen einzelner Merkmale

Wie im vorherigen Absatz bereits beschrieben, ist nicht die Anzahl von unterschiedlichen Merkmalen das entscheidende Kriterium, ob ein Merkmal für die Authentifizierung geeignet ist. Entscheidend ist wie stark die einzelnen Versuche einer Person voneinander variieren im Verhältnis zu den Unterschieden zwischen verschiedenen Personen (Vergleich zwischen Intra- und Inter-Personen-Unterschiede). Der Intra-Personen-Unterschied sagt aus, wie weit sich die einzelnen Werte eines Merkmals vom Mittelpunkt für eine Person unterscheiden. Wogegen die Inter-Personen Variable die Entfernung zwischen verschiedenen Mittelpunkten darstellt. Beide Kennzahlen werden in Tabelle 5.2 dargestellt. In Tabelle 5.2 ist zu erkennen, dass für die Standardmerkmale und die des Touchscreens größere Inter-Personen-Unterschiede vorhanden sind als Intra-Personen-Unterschiede. Besonders deutlich ist dies bei den Merkmalen Verweildauer, Digraph und Druckstärke zu erkennen. Diese Merkmale sind laut Tabelle 5.1 die mit der besten Erkennungsrate. Je kleiner die Schwankungen einer Person im Vergleich zu den Schwankungen zwischen mehreren Personen sind, desto größer ist die Erkennungsrate. Die Grenzen für die Person können daher größer werden (Benutzerfreundlichkeit), ohne dass andere Benutzer als diese Person erkannt werden (Sicherheit). Für die Analyse wurden die Eingaben der einzelnen Buchstaben direkt verglichen und danach über alle Buchstaben des Passwortes gemittelt.

Tabelle 5.2: Unterscheidungen der Intra-Personen- und Inter-Personen-Unterschiede (in %)

Merkmal	Intra-Personen		Inter-Personen
	$\varnothing x$	s	$\varnothing x$
Verweildauer	12,751	5,024	37,171
Digraph	86,977	64,470	229,803
Trigraph	154,717	122,926	447,460
Druckstärke	0,037	0,013	0,104
Druckstärke2	0,071	0,025	0,078
Auflagefläche	0,024	0,003	0,039
Auflagefläche2	0,022	0,004	0,036
x-Koordinate	9,059	4,648	15,074
x2-Koordinate	7,848	1,382	13,795
y-Koordinate	8,261	1,690	11,440
y2-Koordinate	7,770	1,386	11,280
Pitch	23,704	17,014	26,620
Roll	47,442	33,780	63,309
Inclination	34,234	19,679	41,857
GyroX	0,454	0,130	0,330
GyroY	0,541	0,148	0,321
GyroZ	0,245	0,100	0,174
Delta0	0,101	0,062	0,067
Delta1	0,125	0,076	0,089
Delta2	0,047	0,039	0,034
Delta3	0,108	0,134	0,05

Für die Bewegungs- und Lagesensoren sind die Inter-Personen-Unterschiede kleiner als die Intra-Personen-Unterschiede, was dazu führt, dass die Grenzen einer Person für das eine Merkmal von anderen Personen überschritten werden.

S6_Geräte – Auswertung der statistischen Kenngrößen der Merkmale

Eingabedaten:

- Passwort: *sommer*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Je Untersuchung ein Merkmal des kapazitiven Sensors, Bewegungs- und Lagesensors

Ergebnis:

- Die Güte hängt nicht nur von den verschiedenen Ausprägungen eines Merkmals ab, sondern von der Differenz von Intra-Personen- und Inter-Personen-Unterschieden.

Fusionierung von Gruppen von Merkmalen

Damit die Fehlerraten für das Authentifizierungssystem geringer werden, müssen die Merkmale fusioniert werden (siehe Abschnitt 2.5.3). Die Fusion der Gruppen wurde dabei auf dem Score Level durchgeführt. Die Gruppen wurden im ersten Schritt anhand ihrer Herkunft aufgestellt (Standardmerkmale beziehungsweise Merkmale von den Sensoren, kapazitives Display, Orientierung, Gyroskop und Delta). Eine spezielle Gewichtung der einzelnen Merkmale erfolgt bei der Fusionierung nicht. Die Ergebnisse sind in Tabelle 5.3 abgebildet.

Eine Fusion von Merkmalen, die eine hohe Erkennungsrate aufweisen, ergibt geringere Fehlerraten als bei den anderen Merkmalen

Tabelle 5.3: Fehlerraten für fusionierte Merkmale (in %)

Name der Gruppe	Kalkulierte EER	FAR		FRR		Merkmale
		$\varnothing x$	s	$\varnothing x$	s	
Standard-merkmale	11,6	14,1	3,4	9,3	17,0	Verweildauer, Digraph, Trigraph
Kapazitives Display	7,2	6,7	1,5	7,7	11,9	Druckstärke, Druckstärke2, Auflagefläche, Auflage-fläche2, x-Koordinaten, x2-Koordinaten, y-Koordinaten, y2-Koordinaten
Orientierung	35,7	34,4	1,4	37,4	25,8	Pitch, Roll, Inclination
Gyroskop	37,4	31,9	1,5	43,0	25,5	GyroX, GyroY, GyroZ
Delta	40,4	19,2	1,2	62,2	27,6	Delta0, Delta1, Delta2, Delta3

mit niedrigen Erkennungsraten. Das ist deutlich zu erkennen, wenn die Gruppen der Standardmerkmale und Merkmale des kapazitiven Displays mit den verbliebenen Gruppen verglichen werden. Die Fehlerraten belaufen sich für die ersten zwei Gruppen auf ca. 10 %. Die anderen Merkmale weisen Fehlerraten auf, die größer als das Dreifache sind. Die Fehlerraten für die Merkmale des kapazitiven Displays sind zudem kleiner, basierend auf dem Durchschnitt aller Anmeldeversuche, als die Standardmerkmale. Das ist durch die größere Anzahl an Merkmalen des kapazitiven Displays zu begründen. Nach der Fusionierung zu Gruppen ist zu betrachten, wie sich die Fehlerraten bei der Fusion aller Merkmale verändern. Diese Fusion wird in Tabelle 5.4 gezeigt.

Es konnte bei der Fusion aller Werte die EER um mindestens 2,2 % verbessert werden (im Vergleich zu Tabelle 5.3). Ein Unterschied der Fehlerraten mit mehr als 5,0 % ist zu den Standardmerkmalen vorhanden. Das zeigt, dass die Hinzunahme von weiteren Merkmalen bei Verwendung von Smartphones mit kapazitivem Display die Feh-

Tabelle 5.4: Ungewichtete Fusion aller Merkmale (in %)

Kalkulierte EER	FAR		FRR		Merkmale
	$\varnothing x$	s	$\varnothing x$	s	
5,00	3,30	0,31	6,70	24,35	alle

lerraten verbessert. Im nächsten Schritt kann eine Gewichtung der Merkmale benutzt werden, um die Fehlerraten weiter zu minimieren.

S6_Geräte – Auswertung der Fusion einzelner Merkmale

Eingabedaten:

- Passwort: *sommer*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: kNN

Ergebnis:

- Fusion verbessert die Fehlerraten des Systems.
- Durch die unterschiedliche Güte der einzelnen Merkmale ist es sinnvoll eine Gewichtung vorzunehmen.

Gewichtung von Merkmalen

In Tabelle 5.1 wurde gezeigt, dass jedes Merkmal unterschiedliche Fehlerraten aufweist, weswegen eine Gewichtung dieser zu berücksichtigen ist, um die Gesamtfehlerrate zu verringern. Zum einen kann dafür eine

Brute-Force-Methode der Gewichtungen verwendet werden, um die geeignetste Konfiguration zu finden. Je größer der Bereich der Gewichtungen wird, desto länger dauert die Kalkulation der Fehlerraten. Im Folgenden wurde daher der Bereich zwischen einer Gewichtung von 0 bis 8 gewählt. Zum anderen kann der Ansatz aus Abschnitt 5.2.4 verwendet werden, der bessere Fehlerraten für die einzelnen Merkmale exponentiell höher gewichtet. Die Fehlerraten für alle Verfahren sind Tabelle 5.5 zu entnehmen.

Tabelle 5.5: Fehlerraten für einzelne Gewichtungsmodelle (in %)

Gewichtung	Kalkulierte EER	FAR		FRR	
		$\varnothing x$	s	$\varnothing x$	s
keine Gewichtung	5,00	3,30	0,31	6,7	24,35
0-8 Gewichtung	3,43	3,70	0,14	3,16	24,25
Exponent 1,25	3,61	4,55	1,68	2,68	11,53
Exponent 1,5	3,53	3,24	1,46	3,81	12,99
Exponent 1,75	3,30	3,95	1,65	2,68	10,88
Exponent 2	3,12	3,97	1,60	2,30	10,06
Exponent 2,25	3,04	4,00	1,59	2,11	8,69
Exponent 2,5	2,97	2,90	1,34	3,06	9,35
Exponent 2,75	3,01	3,36	1,48	2,68	9,21
Exponent 3	3,16	3,86	1,54	2,46	9,10
Exponent 3,25	3,21	4,34	1,62	2,08	7,78

Es wird deutlich, dass eine Gewichtung der Merkmale zu einer Verringerung der Fehlerraten führt. Die Fusion mittels der Brute-Force-Methode zeigt bereits Werte unter 5 %, ist aber aufgrund der langen Berechnungszeit der einzelnen Gewichtungen für den praktischen Gebrauch eher ungeeignet. Dagegen zeigt die in Abschnitt 5.2.4 vorgestellte Formel mithilfe von Exponenten bessere Ergebnisse als die Brute-Force-Methode unter Berücksichtigung einer korrekten Auswahl des Exponenten. Ein zu kleiner Wert gewichtet die Merkmale

mit schlechter Erkennung zu hoch. Bei einem zu hohen Exponenten werden viele Werte nicht berücksichtigt. Bei den hier aufgelisteten Werten wird bei einem Exponenten von 2,5 die beste kalkulierte EER von 2,97 % erreicht, was im Vergleich zu den anderen vorgestellten Publikationen in Abschnitt 3.1.1 eine deutliche Verbesserung darstellt.

Zu der Betrachtung der einzelnen Merkmale wurde zusätzlich eine Analyse verschiedener Klassifikatoren durchgeführt, um die Güte von unterschiedlichen Klassifikationsalgorithmen nachzuweisen. Diese Betrachtung erfolgt im folgenden Abschnitt.

S6_Geräte – Auswertung der gewichteten Fusion einzelner Merkmale

Eingabedaten:

- Passwort: *sommer*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: kNN

Ergebnis:

- Gewichtung der Merkmale verringert die Fehlerraten.
- Die in Abschnitt 5.2.4 vorgeschlagene Gewichtungsformel erzeugt im Vergleich die besten Werte.

5.3.2 Vergleich von Klassifikatoren

Für die Auswertung der Studien wurde in den vorherigen Abschnitten nur ein Klassifikator verwendet. Verschiedene Klassifikatoren wurden nicht verglichen. Dieser Abschnitt zeigt daher die Eignung der

einzelnen Klassifikatoren für die Authentifizierung mittels des Tippverhaltens.

Die ersten Ergebnisse bezüglich der Analyse von Klassifikatoren wurden mithilfe der Studie **S1_Merkmale** erreicht. Die Eingaben der 18 Testpersonen wurden mittels der bestehenden Klassifikatoren aus dem Weka-Framework analysiert. Zur Klassifikation erfolgte die Auswahl von fünf verschiedenen Klassifikatoren, die bereits in anderen Studien über das Tippverhalten Verwendung fanden. Dazu zählen neuronales Netz [CF06, CHHK00], Radial Basis Function Network (RBFN) [HB97, SWS09], Naives Bayes [GLRSGC02, BPRP11], SVM [GR12, ACCF07] und Instance-Based learner for k (IBk) als Vertreter für einen statistischen bzw. Instanz-basierten Klassifikator [AKA91]. Als Konfigurationen wurden die Standardwerte aus dem Weka-Framework verwendet (die Werte sind in Abschnitt A.6 nachzulesen). Für die Auswertung wurden nur korrekte Eingaben der 10 Versuche angenommen (Korrekturen waren möglich), das zu einer geringeren Anzahl an zu vergleichenden Daten führte. Für die Klassifikation wurde aus diesem Grund die Cross-Validierung verwendet. Dabei werden die Daten in x gleichgroße und disjunkte Datenbestände (standardmäßig entspricht x gleich 10) aufgeteilt, die zusammen die Datengesamtheit ergeben. Für das Training fanden $x-1$ Datenbestände Verwendung und für die Validierung der letzte Datensatz. Es folgte eine x-malige Wiederholung, sodass alle Datenbestände einmal zur Validierung verwendet wurden. Merkmale waren Di-, Trigraph und Verweildauer sowie Druckstärke und Auflagefläche. Die Ergebnisse der Klassifikatoren präsentiert Tabelle 5.6 in Form der unterschiedlichen FAR's und FRR's.

Für die 18 Testpersonen wird in Tabelle 5.6 ein Vergleich zwischen den Klassifikatoren gezeigt. Die vorletzte Zeile repräsentiert den Durchschnitt für den jeweiligen Klassifikator. Allgemein ist zu erkennen, dass die FRR für eine reale Authentifizierung zu hoch ist. Jeder zweite Versuch muss von einer validen Person wiederholt werden. Mit ca. 3 % für die FAR ist nur jeder 33. Angriff auf das System erfolgreich. Bei einer Anpassung des Schwellenwertes aufgrund der hohen FRR wird gleichzeitig die FAR verschlechtert. Ein großes Pro-

Tabelle 5.6: Fehlerraten (Durchschnitt und Standardabweichung) für verschiedene Testpersonen (in %)

Person	Neuronales Netz		NaiveBayes		RBFN		SVM		IBk	
	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR	FAR	FRR
1	0,7	0	2,8	60	1,4	40	2,1	60	0,7	100
2	1,5	18,2	3,6	18,2	5,1	18,2	1,5	27,3	2,2	27,3
3	0,7	75	0,7	75	1,4	75	2,1	25	2,1	25
4	0,7	0	0	60	0	60	2,1	20	2,1	0
5	0,7	0	0,7	25	2,1	25	0,7	50	0,7	25
6	0,7	25	1,4	25	0,7	37,5	0	37,5	0,7	50
7	0,7	42,9	5	85,7	2,8	71,4	2,1	71,4	2,8	28,6
8	5,8	81,8	5,1	54,5	6,6	63,6	4,4	54,5	8	54,5
9	4,4	18,2	1,5	18,2	1,5	27,3	5,1	36,4	1,5	27,3
10	1,4	25	1,4	50	0,7	75	2,1	75	2,1	75
11	4,3	70	6,5	40	7,2	50	7,2	70	5,8	40
12	4,9	100	2,8	100	2,8	100	2,8	100	4,9	100
13	8	45,5	2,9	0	4,4	0	2,2	18,2	3,6	54,5
14	0,7	33,3	2,2	77,8	2,2	55,6	2,2	66,7	2,9	22,2
15	2,9	20	0	40	0,7	30	3,6	40	0,7	10
16	0	100	5	75	6,4	75	4,3	75	3,6	87,5
17	5,1	20	2,2	60	2,2	70	5,8	60	1,4	40
18	4,3	100	7,2	60	5,8	80	5,8	70	5,1	100
$\varnothing x$	3,1	44,6	3,1	48	3,3	50,7	3,4	52,7	3	48
s	2,2	34,6	2,1	25,9	2,2	25,3	1,8	22,1	1,9	31,0

blem für jeden Klassifikator stellen die Personen dar, die sich nicht authentifizieren können (FRR gleich 100 %). Dieses tritt bei jedem der fünf Klassifikatoren auf, muss aber vermieden werden, da sonst das Verfahren nicht nutzbar ist. Besonders trifft das für Person 12 zu, die sich selber nie verifizieren konnte. Das lag daran, dass sich die Person sehr oft an unterschiedlichen Stellen verschrieben hat und somit kein Schreibfluss zustande kam. Das Schreiben eines Passwortes auf dem Gerät muss daher, entsprechend der Erfahrung mit dem Gerät, geübt werden. Das kann anhand der Intra-Personen-Unterschiede erkannt werden und zu einem längeren Enrolment führen.

Zu erkennen ist, dass die Standardabweichung der FRR im Vergleich zur FAR größer ist. Dieser Unterschied liegt an der Konfiguration und der geringen Anzahl an positiven Versuchen der zu verifizierenden Person.

Nachteile bei dieser ersten Studie sind u. a. die geringe Anzahl an Testpersonen und deren Versuche. Gleichzeitig ist es bei der Testeinstellung möglich, Fehler im Passwort zu machen. Diese Versuche wurden im Nachhinein herausgefiltert und verringern die Versuchsanzahl zusätzlich. Bei verstärktem Trainieren des Passwortes erfolgen weniger Tippfehler und ein Muster einer Person wird deutlicher. Deswegen wurde eine erweiterte Studie durchgeführt, die die Kriterien für eine bessere Auswertung erfüllt. Am Ergebnis in Tabelle 5.6 wird deutlich, dass die Standard Weka-Einstellung für eine Authentifizierung nicht geeignet ist, sodass zusätzliche Modifizierungen erfolgen müssen (durch Tests zu analysieren). Die Tests für die Anpassungen werden mit dem in Abschnitt 4.3 und Abschnitt 5.2.4 beschriebenen Klassifikationsframework durchgeführt. Mit diesem wird für den Authentifizierungsfall eines Smartphones zusätzlich zu der Identifikation eine Verifikation in das Konzept aufgenommen, welches geringere Fehlerraten ermöglicht. Es ist dazu erforderlich verschiedene Klassifikatoren mit diesem Framework zu testen.

In der im Rahmen dieses Forschungsvorhabens betreuten wissenschaftlichen Arbeit von B. Behrendt [Beh13b] zeigte der statistische Klassifikator niedrigere Fehlerraten im Vergleich zu einem neuronalen Netz und einer SVM – basierend auf Mittelwerten. Die Fehlerraten für die drei Klassifikationen im Zusammenhang mit der Berechnungszeit (kalkuliert mit einem Intel i7, Quadcore mit 3,2 GHz mittels 8 Threads) werden in Tabelle 5.7 gezeigt.

Wie in Tabelle 5.7 zu erkennen, sind die Bearbeitungszeiten für den kNN im Vergleich zu den anderen beiden Klassifikatoren in der Summe am geringsten. Lediglich das neuronale Netz zeigte bei der Evaluation einen geringeren Wert. Dafür ist die Trainingszeit des Modells einer Person sehr zeitaufwendig und kann nur auf einem Server stattfinden, da die Kalkulation auf einem Smartphone ein Vielfaches dauert. Zudem müsste das Modell immer wieder neu trainiert werden. Sowohl für

Tabelle 5.7: Bearbeitungszeit und durchschnittliche Fehlerraten der einzelnen Klassifikatoren im Test pro Benutzer

	∅Bearbeitungszeit (in ms)		∅Fehlerraten (in %)	
	Enrolment	Verifikation	FAR	FRR
kNN	0,17	2,65	2,83	2,85
Neuronales Netz	2538,23	1,77	0,1	8,27
SVM	10,91	10,12	5,58	19,46

die Fehlerraten als auch die Bearbeitungszeit zeigt der statistische Klassifikator die geringsten Werte, um auf einem Gerät autonom zu funktionieren. Daher wird im Folgenden für die Analysen der kNN verwendet.

S1_Merkmale – Auswertung von existierenden Klassifikatoren

Eingabedaten:

- Passwort: *hello world*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Kombinationen aus Merkmal des kapazitiven Sensors und des Gyroskops
- Klassifikator: Neuronales Netz, NaiveBayes, RBFN, SVM, IBk, kNN

Ergebnis:

- Keine großen Unterschiede zwischen den Klassifikatoren bei kleiner Probandenanzahl.
- Bearbeitungsdauer limitiert die Vielfalt an Klassifikatoren.

5.3.3 Vergleich zwischen 12-Tasten- und QWERT-Layout

In Abschnitt 5.3.1 wurde auf die neuen Merkmale, die beim kapazitiven Display extrahiert werden, eingegangen. Basierend auf der Publikation [TO12] soll gezeigt werden, welchen Einfluss das QWERT-Tastenlayout im Gegensatz zum 12-Tastenlayout auf das Tippverhalten mit diesen Merkmalen hat. Dazu werden jeweils zwei Eingaben miteinander verglichen, wozu der Datensatz **S2_PINPasswort**, bei dem sowohl Zahlen als auch Buchstaben eingegeben wurden, dient.

Klassifikation der numerischen Eingabe

Von dem Datensatz wurden von jeder Person sieben Versuche für das Training des Modells verwendet. Bevor das Modell für jeden Benutzer generiert werden konnte, wurden mit dem in Abschnitt 5.2.4 beschriebenen Algorithmus die Ausreißer für jedes Merkmal extrahiert. Die Evaluation basierte auf den verbleibenden Versuchen.

Tabelle 5.8 zeigt die ermittelten Fehlerraten der beiden Layouts. Dabei findet der statistische Klassifikator (Schwellenwertbereich um den Mittelwert) Anwendung.

Tabelle 5.8: FAR und FRR für beide Tastaturenlayouts (in %) bei der numerischen Eingabe

Layout	Kalkulierte EER	FAR		FRR	
		$\varnothing x$	s	$\varnothing x$	s
12-Tasten	7,01	8,12	7,49	6,90	20,30
QWERT	11,59	17,05	10,46	6,14	16,85

Zu erkennen ist, dass die Fehlerraten für das 12-Tastenlayout im Durchschnitt geringer sind als beim QWERT-Layout, jedoch die Standardabweichung für beide Fehlerraten ähnlich groß ist. Bei annähernd gleicher FRR ist die FAR beim QWERT-Layout doppelt so hoch. Das Tastaturenlayout beeinflusst daher die einzelnen Merkmale während des Tippens.

Klassifikation der alphabetischen Eingabe

Zur Auswertung für die Eingabe von Buchstaben diente der identische Ansatz wie in Abschnitt 5.3.3 beschrieben. Beim 12-Tastenlayout werden verschiedene Buchstaben eingegeben, indem mehrfach in einer kurzen Abfolge auf die gleiche Taste gedrückt wurde. Die dafür entstehenden FAR und FRR zeigen zwischen den beiden Tastaturlayouts Unterschiede, die in Tabelle 5.9 dargestellt sind.

Tabelle 5.9: FAR und FRR für beide Tastaturenlayouts (in %) bei der alphabetischen Eingabe

Layout	Kalkulierte EER	FAR		FRR	
		$\varnothing x$	s	$\varnothing x$	s
12-Tasten	7,84	8,80	7,50	6,89	13,50
QWERT	7,80	9,31	8,01	6,30	16,60

Die Fehlerraten dokumentieren in diesem Experiment Unterschiede zwischen den beiden Layouts, wie auch für die numerische Eingabe. Für die Eingabe mit dem 12-Tastenlayout werden im Durchschnitt gleiche Fehlerraten erzeugt (bei kleiner Standardabweichung). Im Vergleich zu der Eingabe numerischer Werte können dagegen mit alphabetischen Eingaben geringere FAR- und FRR-Werte für beide Tastaturenlayouts erzielt werden.

S2_PINPasswort – Auswertung der Tastaturenlayouts

Eingabedaten:

- Passwort: *mein telefon* und *1864559*
- Gerät: HTC Desire

Studienparameter:

- Merkmale: Kombinationen aus Merkmal des kapazitiven Sensors (nur während des Drückens einer Taste), Bewegungs- und Lagesensors
- Klassifikator: kNN

Ergebnis:

- QWERT Tastaturlayout zieht höhere Fehlerraten als das 12-Tastenlayout nach sich.
- Alphabetische Eingabe erzielte bessere Fehlerraten als die numerische Eingabe.
- Mit dem HTC Desire wurden höhere Fehlerraten ermittelt als mit den Samsung Galaxy S II.

5.3.4 Verwendung von Wischmuster – Swype

Die Adaption der Eingabemethode mittels Swype Ansatz für die Authentifizierung wurde in Abschnitt 5.2.3 beschrieben. In diesem Abschnitt soll daher analysiert werden, ob ein abgeleiteter Ansatz zur Merkmalsextraktion beim klassischen Tippverhalten geeignet ist.

In der im Rahmen dieses Forschungsvorhabens durchgeführten wissenschaftlichen Arbeit von M. Graumann [Gra12] in Zusammenarbeit mit M. Trojahn wurde die Funktionsweise in einer Testreihe gezeigt. Die Ergebnisse der Hauptstudie präsentiert Tabelle 5.10. Es wurden dabei die Merkmale analog zum Tippverhalten (siehe Abschnitt 5.2.3) extrahiert und mittels kNN klassifiziert. Dabei fanden sechs Datensätze zum Training und zwei zur Evaluierung aus der Studie **S5_Swype** Verwendung (die ersten beiden wurden aufgrund des Lernprozesses ignoriert). Die durchschnittlich extrahierten FAR's und FRR's inklusive der Standardabweichung werden für alle fünf Passwörter präsentiert.

Das Wort *monogamie* ist mit neun Buchstaben das längste Passwort in dem Test und gleichzeitig das Passwort, das die geringsten Fehlerraten (FAR and FRR) aufweist. Wenn ein Angreifer versucht

Tabelle 5.10: Resultierende Fehlerraten pro Passwort (in %)

Passwort	Kalkulierte EER	FAR		FRR	
		$\varnothing x$	s	$\varnothing x$	s
monogamie	11,60	17,10	8,63	6,10	19,74
passwort	11,97	15,40	7,09	8,54	21,82
test	17,77	25,79	10,91	9,76	22,68
wert	23,37	22,34	10,38	24,39	31,49
qwertz	18,01	30,57	12,41	15,44	26,64

sich an dem System mit bekanntem Passwort zu authentifizieren, ist er nur in einem von sieben Versuchen erfolgreich. Gleichzeitig wird ein bekannter Benutzer, der sein Passwort schreibt, in einem von 17 Fällen abgelehnt. Aber nicht nur das Wort *monogamie* zeigte die niedrigsten Fehlerraten, auch das Passwort *passwort* weist eine Verbesserung gegenüber der Authentifizierung mit PIN auf. Darüber hinaus zeigen die anderen drei Passwörter (*test*, *wert* und *qwertz*) erhöhte Fehlerraten, da sie zu kurz (vier Buchstaben) oder zu einfach zu zeichnen (eine einfache Linie) sind.

Es ist weit verbreitet, dass ein Passwort so lang wie möglich sein sollte, damit eine Brute-Force-Methode länger dauert, um das Passwort herauszufinden [Bun11a]. Das kann gleichzeitig auf die Fehlerraten bezogen werden. Mehr Merkmale der gleichen Güte verbessern die Erkennungsrate, was auch in dieser Studie bestätigt wurde. Zudem ist die Lage der einzelnen Buchstaben von Bedeutung. Je komplexer das resultierende Muster ist, desto niedriger sind die Fehlerraten. Dazu gehört u. a. auch ein Richtungswechsel.

Ein weiterer Aspekt ist, Passwörter mit Dopplungen zu nutzen. Der Grund sind die unterschiedlichen Wege, durch die die Dopplungen bei Swype erkannt werden können. Möglichkeiten stellen zum einen das längere Berühren einer Taste dar (warten mit dem Finger an einer Stelle) und zum anderen einen Kreis auf dem entsprechenden Buchstaben zu zeichnen. Besonders im zweiten Fall spielen die Richtung und die Größe des Kreises eine Rolle. Ein weiterer Vorteil bei dem

Wischmuster ist, dass sich dieses leichter einprägen lässt als bei einer 3x3 Matrix, die in Abschnitt 3.1.1 beschrieben wurde.

Zusammenfassend zeigt die Studie, dass der Benutzer hauptsächlich für die Fehlerraten verantwortlich ist, da ein gut gewähltes Passwort die Intra-Personen Unterschiede unter Verwendung längerer Passwörter verringern kann. Dennoch existieren durch die Verwendung der reinen Adaption vom Tippverhalten einige Nachteile. Die Fehlerraten sind größer als in der Vorstudie von M. Graumann [Gra12] (kalkulierte EER bei ca. 10 %), was mit der geringeren Anzahl an Probanden zu begründen ist. Die Einmaligkeit der verwendeten Merkmale wird durch die steigende Anzahl von Personen verringert.

S5_Swype – Auswertung der Authentifizierung mittels Wischmuster

Eingabedaten:

- Passwort: *monogamie*, *passwort*, *test*, *wert* und *qwertz*
- Gerät: Samsung Galaxy S II

Studienparameter:

- Merkmale: Minimum, Maximum, Durchschnitt sowie Varianz von Daten des kapazitiven Sensors
- Klassifikator: kNN

Ergebnis:

- Mit den vorgestellten Methode sind die Fehlerraten stark abhängig von der Form des Wischmusters.
- Existierende Fehlerraten sind nicht ausreichend für eine Authentifizierung.
- Weitere Merkmale müssen gefunden werden.

5.3.5 Veränderung des Tippverhaltens durch das Lernverhalten

Die Auswertungen dieses Abschnittes beruhen auf der Studie **S4_Lernen** (siehe Abschnitt 4.1). Ziel der Studie ist es, zu analysieren, wie stark sich das Tippverhalten über einen längeren Zeitabschnitt mit einer Vielzahl von wiederholten Eingaben verändert, um herauszufinden, ob eine Anpassung des Merkmalmodells erfolgen muss. Dazu wird in Tabelle 5.11 gezeigt, wie sich die Erkennungsraten zwischen der ersten und letzten Versuchsreihe unterscheiden.

Tabelle 5.11: Vergleich der Fehlerraten zwischen dem ersten und letzten Tag (in %)

Datensätze		Kalkulierte	FAR		FRR	
Enrolment	Verifikation	EER	$\varnothing x$	s	$\varnothing x$	s
1. Tag	1. Tag	2,36	2,73	1,75	2,00	7,14
10. Tag	10. Tag	1,42	2,19	1,20	0,65	4,59
1. Tag	10. Tag	14,51	10,65	3,30	18,36	25,84

Es ist zu erkennen, dass bei den 40 Versuchen am ersten Tag die Fehlerraten höher waren, als bei den letzten 40 Versuchen. Das ist dadurch zu erklären, dass eine immer größere Routine beim Tippen erreicht wird. Daher werden die einzelnen Versuche immer ähnlicher, was gleichzeitig bedeutet, dass es nicht so viele Überschneidungen zwischen unterschiedlichen Personen gibt, weswegen die FAR niedriger ist (basierend auf Mittelwert und Standardabweichungen). Das Modell aus dem Enrolment der ersten 40 Versuche weist erhöhte Fehlerraten auf, wenn es mit den Daten aus den letzten 40 Versuchen verifiziert wird. Die FRR liegt bei über 18 %, was bedeutet, dass fast jeder fünfte Versuch wiederholt werden muss. Das zeigt, dass das Modell kontinuierlich aktualisiert werden muss, damit sich eine Person dauerhaft verifiziert und Angreifer abgelehnt werden.

Diese Unterschiede sind nicht nur in den Fehlerraten, sondern auch in den statistischen Kenngrößen der einzelnen Merkmale zu sehen. Der prozentuale Unterschied zwischen dem letzten und dem ersten Versuch wird in Abbildung 5.9 dargestellt.

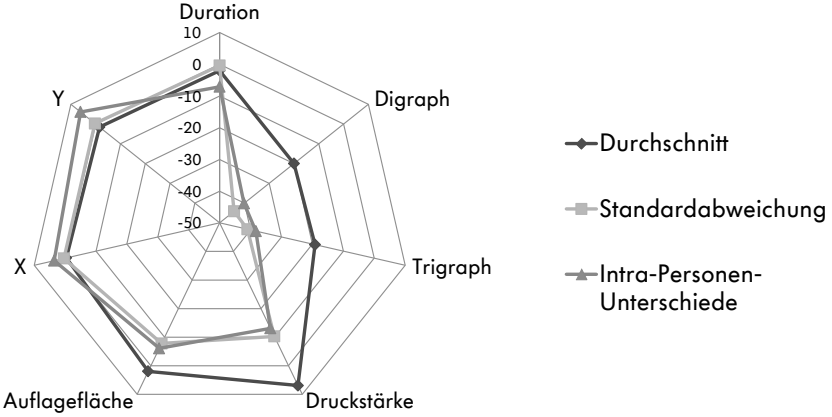


Abbildung 5.9: Prozentualer Unterschied der Werte der einzelnen Merkmale von den letzten zu den ersten Versuchen

Es ist zu erkennen, dass sich besonders die Di- und Trigraphen verringern. Das bedeutet, dass sich die Zeiten um 20 % verringern und gleichzeitig die Unterschiede zwischen den einzelnen Versuchen deutlich kleiner werden. Die durchschnittliche Druckstärke und Auflagefläche steigen hingegen (Standardabweichung sinkt dennoch). Bei den x/y-Koordinaten ist die Standardabweichung bei fast gleichbleibendem Mittelwert erhöht.

S4_Lernen – Auswertung des Lernverhaltens

Eingabedaten:

- Passwort: *donnerwetter*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: kNN

Ergebnis:

- Das Tippverhalten verändert sich im Laufe der Zeit.
- Das Modell einer Person muss dauerhaft angepasst werden.

5.4 Ergebnisse und Bewertung des entworfenen Systems

Es wird im Folgenden das Erreichen der einzelnen Unterziele, die in diesem Kapitel vorgestellt wurden, bewertet:

Wahl der Merkmale: Das Ergebnis kann durch die Fusion mit weiteren Merkmalen verbessert werden (siehe Abschnitt 5.3.1), wenn die Erkennung nur mit diesen Merkmalen besser ist als 50 %. Doch je mehr Merkmale zur Klassifizierung herangezogen werden, desto länger dauert die Klassifikation. Bei verschiedenen Klassifikationsalgorithmen, wie z. B. das neuronale Netz, ist die Entscheidung wichtig, ob zusätzliche Merkmale verwendet werden sollen. In diesem Fall muss eine Merkmalsreduktion erfolgen. Dabei sollten die Merkmale reduziert werden, die für sich eine schlechtere Erkennungsrate aufweisen.

Diese Entscheidung kann somit von der Gewichtung der einzelnen Merkmale abgeleitet werden. Durch das Weglassen wird Zeit für die Klassifikation eingespart.

In Abschnitt 5.3.1 wurde gezeigt, dass die neuen Merkmale einzeln betrachtet, insbesondere die Druckstärke, sehr geringe Fehlerraten aufweisen. In der einfachen Fusion aller Merkmale eines Sensors haben die neuen Merkmale, die aus den Daten des kapazitiven Displays extrahiert werden, die kleinsten Fehlerraten (dabei wurden mehr Merkmale verwendet als die klassischen Zeitmerkmale). Dennoch kann davon abgeleitet werden, dass die Fusion mit den neuen Merkmalen eine Verbesserung der Fehlerraten bedeutet, was auch durch die schon angesprochenen geringen Gesamtfehlerraten bestätigt wird. Für diese Authentifizierung wurde der kNN verwendet, da der Klassifikator in der Studie sowohl bei den Fehlerraten als auch bei der Bearbeitungsdauer die geringsten Resultate im Vergleich zu den anderen getesteten Klassifikatoren erzeugte.

Ein weiterer zu prüfender Punkt ist, ob die Merkmale möglichst disjunkt (voneinander unabhängig) sind. Anhand der Abbildung 6.2 in Abschnitt 6.1 konnte eine Verknüpfung der Werte für die Druckstärke und Auflagefläche verdeutlicht werden. Mittels Pearson Korrelationsanalyse [Bro98, S. 501ff] wurde der Korrelationskoeffizient berechnet, um zu analysieren, wie stark Druckstärke und Auflagefläche voneinander abhängig sind. Dazu wurde der Datensatz, der im Stehen aufgenommen wurde, mit dem Wort *anna* aus der Studie **S7_Szenarien** verwendet. Mittels der Anwendung der Open-Source Version von SPSS (PSPP) wurde die Korrelationsanalyse mit den Ergebnissen aus Tabelle 5.12 durchgeführt.

Mit dem Ergebnis eines positiven Wertes von 0,66 (Werteskala von -1 bis 1) kann eine starke Korrelation zwischen Druckstärke und Auflagefläche in positiver Richtung erkannt werden (laut Brosius [Bro98, S. 503]). Das bedeutet, dass diese voneinander abhängig sind und wenn sich die Druckstärke erhöht, sich sehr wahrscheinlich auch die Auflagefläche erhöht (umgekehrt ist die gleiche Aussage möglich). Dennoch korrelieren die beiden Werte nicht perfekt (Wert von 1,00).

Tabelle 5.12: Korrelationsanalyse mittels PSPP

		Druckstärke	Auflagefläche
Druckstärke	Pearson Korrelation	1,00	0,66
	Sig. (2-seitig)		0,00
	N	13352	13345
Auflagefläche	Pearson Korrelation	0,66	1,00
	Sig. (2-seitig)	0,00	
	N	13345	13345

Einfluss der Tastengröße: Durch die Einführung einer QWERT-Touchscreen Tastatur sind die einzelnen Tasten auf der Tastatur kleiner als bei dem 12-Tastenlayout. Daher wurde analysiert, wie der Einfluss auf die Fehlerraten ist. In der Studie zeigte das QWERT-Layout höhere Fehlerraten als das 12-Tastenlayout für numerische als auch alphabetische Eingaben. Es muss genauer fokussiert werden, wo sich die Taste befindet und es wird öfter daneben getippt. Grundsätzlich wäre für die Authentifizierung eher das 12-Tastenlayout bei numerischer Eingabe geeignet. Für alphabetische Eingaben sind beide Tastaturlayouts basierend auf den Fehlerraten geeignet. Dadurch, dass standardmäßig mit dem QWERT-Layout getippt wird, muss dieses Layout genauer betrachtet werden. Es weist höhere Fehlerraten auf, was durch die erweiterten Merkmale erfolgreich aufgefangen wird, sodass dieses Layout verwendet werden kann.

Reduzierung der Fehlerraten: Es wurde in diesem Kapitel gezeigt (siehe Abschnitt 5.3.1), dass die Fehlerraten unter den bisherigen Fehlerraten liegen. Mit einer kalkulierten EER von 2,97 % ist dieses Ergebnis fast ein Prozentpunkt besser als bei dem verwendeten Softwareprodukt in einer skandinavischen Bank. Für die geringen Fehlerraten ist vor allem die Fusion der Merkmale entscheidend. Dieses

Ergebnis kann noch weiter reduziert werden mit einer EER von unter 1 %, was in Kapitel 7 gezeigt wird.

Lernverhalten: Es wurde mittels statistischer Kenngrößen und Fehlerraten nachgewiesen, dass sich das Tippverhalten nach mehreren Eingaben verändert. Die Fehlerraten zeigten zudem, dass ein Anpassen des Merkmalmodells zwingend notwendig ist, um die Fehlerraten ausreichend klein zu halten (die in Abschnitt 1.2 angesprochenen 3,9 %).

6 Gerätespezifische und geräteübergreifende Authentifizierung

Verschiedene gerätespezifische Sensoren bedingen unterschiedliche Daten und Datenqualität. In diesem Kapitel wird analysiert, wie gerätespezifisch das Authentifizierungsverfahren ist und ob es eine geräteübergreifende Authentifizierung, d. h. die Erkennung auf verschiedenen Geräten, ermöglicht.

6.1 Zielstellung für die Authentifizierung mit mehreren Geräten

Eine gerätespezifische Authentifizierung benötigt eine Analyse unterschiedlicher Geräte. Ein Experiment mit 65 verschiedenen Geräten im Vorfeld zu den Studien hat gezeigt, dass eine Reihe von unterschiedlichen Sensoren je Sensortyp existiert. In den Gerätetypen sind z. B. unterschiedliche kapazitive Displays verbaut und insbesondere bei diesem Sensortyp kommt es zu großen Schwankungen der Werte. In Abbildung 6.1 wird gezeigt, wie sich die Geräte anhand der Anzahl der Werte für den Druck und die Auflagefläche unterteilen lassen.

Wie in Abbildung 6.1 zu erkennen, existiert eine Reihe von Smartphones, die keine der beiden Werte aufzeichnen. Darüber hinaus gibt es Geräte, die nur einen der beiden Werte aufzeichnen bzw. bei denen beide Werte identisch sind. Eine andere Gruppe, bei der die meisten Informationen (beide Werte) für die Authentifizierung entnommen werden können, stellen die Geräte dar, bei denen es eine unterschiedliche Anzahl an Druck- und Auflagefläche-Werten gibt.

Werden sowohl die Werte der Druckstärke als auch der Größe des Fingerabdrucks in einer Grafik betrachtet, sind mehrere Aspekte

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_6

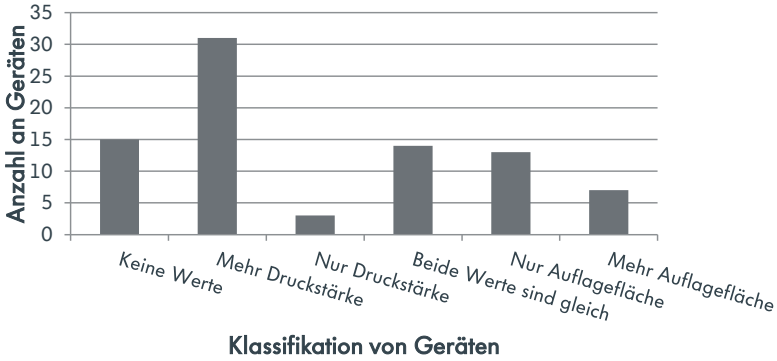
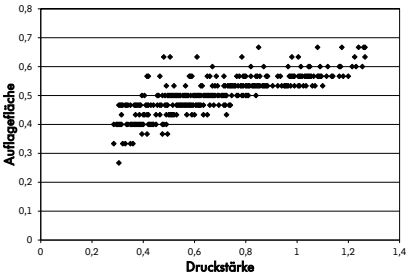


Abbildung 6.1: Unterschiedliche Verhältnisse zwischen der Anzahl an Werten der Druckstärke und der Auflagefläche

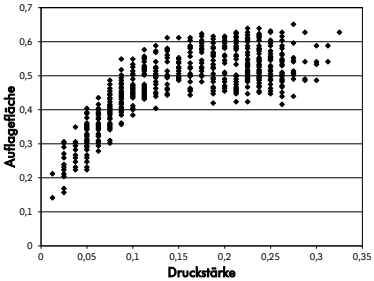
sichtbar (siehe Abbildung 6.2). Der Inhalt der Studie ist die Eingabe eines längeren Textes auf verschiedenen Geräten von unterschiedlichen Personen zu untersuchen.

Sichtbar ist u. a., dass eine unterschiedliche Anzahl an Werten für die Druckstärke und Auflagefläche (abhängig vom Gerät) existiert. Einerseits gibt es Geräte, die mehr Werte für die Druckstärke als für die Auflagefläche besitzen (Variante A). Ein Beispiel dafür ist das Galaxy Nexus. Andererseits existieren Geräte, wie das Samsung Galaxy S II, bei dem es mehr Werte für die Auflagefläche als für die Druckstärke gibt (Variante B). Der dritte Fall entspricht einer eindeutigen Zuordnung von einem Wert der Druckstärke zu einem Wert der Auflagefläche (Variante C – z. B. Sony Ericsson Xperia Neo V). Gleichzeitig gibt es Geräte, bei denen der Wert für die Druckstärke dauerhaft 1,0 entspricht (bspw. Samsung Galaxy S III). Dieser Fall kann aber mit Variante C gleichgesetzt werden, da hier kein Mehrwert existiert, wenn beide Daten aufgenommen werden. Die Druckstärke ist für die Auswertung bei dieser Geräteart unbrauchbar.

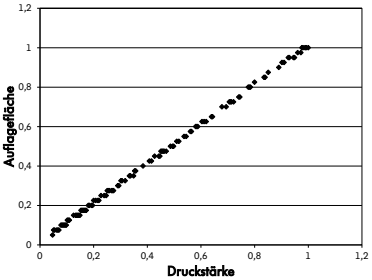
Ebenso wird deutlich, dass beide Daten in einer bestimmten Weise voneinander abhängig sind. Bei Variante A und B ist erkennbar, dass mit höherem Druck auch eine höhere Auflagefläche vorherrscht.



Variante A (mehr auswertbare Werte für die Druckstärke)



Variante B (mehr auswertbare Werte für die Auflagefläche)



Variante C (gleiche Werte)

Abbildung 6.2: Darstellung unterschiedlicher Verhältnisse zwischen Druckstärke und Auflagefläche

Gleiches gilt ebenso umgekehrt. Das ist dadurch zu erklären, dass sich der Finger beim Druck auf die Platte je nach Druckstärke der Oberfläche anpasst.

Darüber hinaus wurde für die Werte erkannt, dass die verschiedenen Geräte unterschiedlich für die Druckstärke und Auflagefläche normiert sind (siehe Abbildung 6.3).

Hierbei ist ein Vergleich der Werte der Auflagefläche und der Druckstärke von drei verschiedenen Geräten durchgeführt worden, bei denen eine Person das Wort *module* eingegeben hat (Mittelwerte über mehrere Versuche). Zum einen wird bei dem Samsung Galaxy S III ein viel niedriger Wertebereich verwendet als bei den anderen beiden

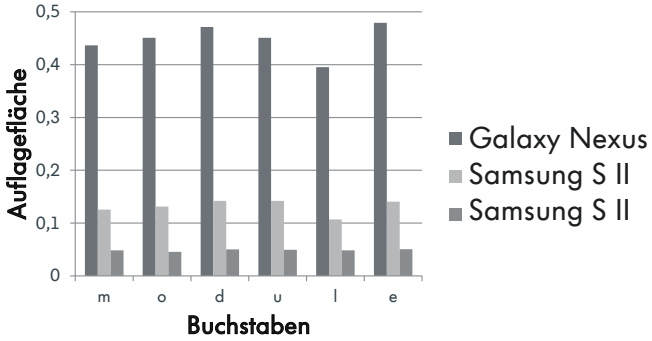


Abbildung 6.3: Unterschiedliche Normierungen der Auflagefläche für verschiedene Geräte, die schon in der Veröffentlichung [TSO13] vorgestellt wurden

verwendeten Geräten. Zum anderen existieren unterschiedlich viele Stufen, die durch die Gesamtanzahl an verschiedenen Werten für ein Merkmal bestimmt werden.

Bei den Zeitmerkmalen, vor allem Di- und Trigraph, gibt es Unterschiede, die durch die verschiedenen Displaygrößen bedingt sind. Die Größe des Displays im Zusammenhang mit der Auflösung führt für eine x/y-Koordinate zu einer unterschiedlichen Taste auf der Tastatur.

Damit ist zu erkennen, dass ohne eine Transformation der Daten u. a. die Auflagefläche und Druckstärke nicht geräteübergreifend verwendet werden können. Daraus resultieren folgende Ziele, die bezüglich der Geräte erreicht werden müssen:

- Für eine Authentifizierung des Tippverhaltens muss eine Erkennung auf unterschiedlichen Gerätemodellen möglich sein. Die Fehlerraten dürfen nicht über den in Abschnitt 1.2 beschriebenen 3,9 % liegen.

- Gleichzeitig sollte es möglich sein, ein Enrolment nur auf einem Gerät durchzuführen und durch eine Transformation dieses Merkmalmodell auf andere Geräte zu übertragen, unter der Bedingung, dass die Fehlerraten ebenfalls unter 3,9 % liegen.

6.2 Konzept für die Transformation des Merkmalmodells

Die Struktur für die geräteübergreifende Authentifizierung zeigt Abbildung 6.4. Dabei wird explizit auf die geräteübergreifende Merkmalsextraktion eingegangen, die eine Erkennung des Gerätes und eine Transformation der Daten benötigt.

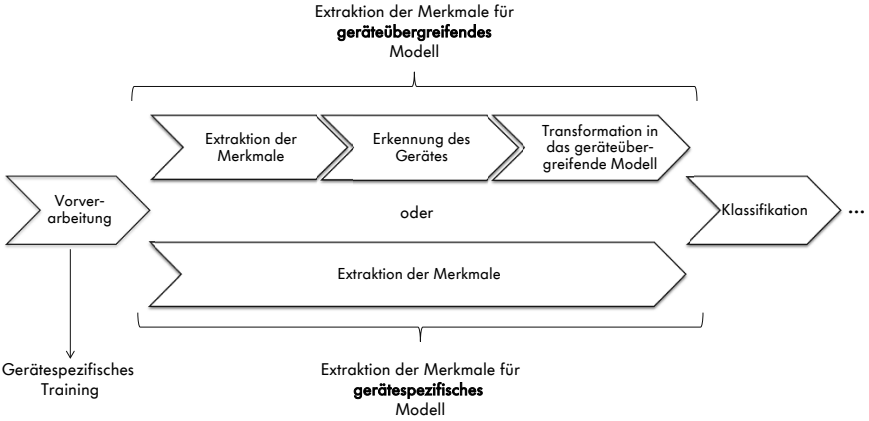


Abbildung 6.4: Unterscheidung zwischen gerätespezifischer und geräteübergreifender Verarbeitung

Die Daten der Sensoren eines Gerätes werden von der Datenerfassung aufgenommen und mittels der Vorverarbeitung gesäubert. Nach den generellen Merkmalsextraktionsschritten aus Abschnitt 5.2.3 existieren gerätespezifische Merkmale. Ohne eine Transformation entsteht aus diesem Vorgang ein gerätespezifisches Modell. Die Klassifikation kann damit nur auf diesem Gerät durchgeführt werden. Das bietet keine Möglichkeit eine Authentifizierung auf einem weiteren Gerät ohne Enrolment durchzuführen. Wird jedoch eine Gerätetransformation in ein geräteübergreifendes Modell durchgeführt, kann eine Authentifizierung ohne weiteres Enrolment auf einem anderen Gerät vorgenommen werden. Dieser Vorgang kann jedoch nur durchgeführt werden, wenn

eine Gerätetransformation in ein geräteübergreifendes Modell erfolgt. Der erste Schritt dafür ist eine Erkennung des Gerätes. Das kann mittels der API aus den Geräteinformationen extrahiert werden.

Mittels einer Auswertung der einzelnen Merkmale soll zusätzlich nachgewiesen werden, wie gerätespezifisch die Merkmale sind (siehe Tabelle 6.2). Diese Informationen werden für die geräteübergreifende Authentifizierung genutzt. Anhand der Fehlerraten und der statistischen Kenngrößen kann des Weiteren herausgefunden werden, wie die Transformation erfolgen kann. Um diese zu erreichen, müssen die verschiedenen Merkmale (z. B. Auflagefläche oder Druckstärke) für alle Geräte normiert werden. Dennoch ist zu beachten, dass durch die Anzahl von unterschiedlich vielen Abstufungen Informationen verloren gehen, wenn die Daten von einem Gerät mit kleinen Abstufungen entnommen werden.

Anhand der in Abbildung 6.3 dargestellten Gerätetypen (Galaxy Nexus, Samsung Galaxy S II und Samsung Galaxy S III) wurden die schon in Abschnitt 5.2.1 vorgestellten Daten extrahiert und gefiltert, bevor die Transformationen durchgeführt wurden. Die Präsentation dieser Transformation für die Merkmale war bereits Inhalt einer Publikation [TSO13]. Bei der Definition ist zu beachten, dass eine Transformation in ein geräteübergreifendes Modell erfolgte, das von allen Geräten akzeptiert wird. Dabei müssen die genauen Werte (Stellschrauben) für die einzelnen Merkmale definiert werden. Mit einer Voranalyse, ein Versuch mit 10 Testkandidaten, wurden die Stellschrauben festgelegt. Mittels einer Studie wird im nächsten Abschnitt gezeigt, wie gut diese Transformation geeignet ist.

Druckstärke und Auflagefläche: Wie bereits in Abschnitt 6.1 vorgestellt, existieren Unterschiede zwischen den jeweiligen Werten auf verschiedenen Geräten. Für jedes Gerät muss es einen Normierungsfaktor n geben (es handelt sich hierbei um einen Skalierungsfaktor), der für jeden Wert anwendbar ist. Aus den Testdaten der Vorstudie kann geschlossen werden, dass für die Merkmale Druckstärke und Auflagefläche der Normierungsfaktor ohne Offset multipliziert werden kann (siehe Formel 5.3).

$$Feature_{model}(x) = n_{deviceY} * Feature_{deviceY}(x) \qquad (6.1)$$

Darüber hinaus müssen Informationen über die Qualität des Merkmals gespeichert werden (u. a. wie viel unterschiedliche Ausprägungen der Werte), da sich die Anzahl der Werte bei den Geräten unterscheidet.

Zeitunterschiede: Alle Merkmale, die sich auf die Zeit (Verweildauer, Di- oder Trigraph) beziehen, zeigen Unterschiede zwischen den Geräten in dem Test mit den 65 Geräten auf. Das kann durch die abweichende Größe der Displays bedingt sein (z. B. Galaxy Nexus: 6,0 cm x 5,4 cm, Samsung Galaxy S II: 5,6 cm x 3,5 cm oder Samsung Galaxy S III: 5,8 cm x 3,2 cm). Bei einem größeren Bildschirm muss eine größere Strecke mit dem Finger zurückgelegt werden als bei kleinen Displays. Dies bedingt demnach mehr Zeit. Die Zeitverlängerung betrifft den Di- und Trigraphen. Für die Verweildauern muss anhand einer Voruntersuchung (mittels 10 Testpersonen) analysiert werden, wie groß die Veränderungen sind und mit welcher Normierung sie transformiert werden können (Berechnung analog zur Druckstärke).

Genaue Koordinaten: Sowohl die x- als auch die y-Koordinate der Berührung auf dem Display sind abhängig von der Auflösung und Größe des Gerätes. Bei einem größeren Display sind die Tasten in einem unterschiedlichen Koordinatenraum. Daher müssen die Größe und Lage der einzelnen Tasten für jedes einzelne Gerät ermittelt und transformiert werden.

Lage- und Bewegungssensoren: Das Gyroskop und das Accelerometer zeigten bei 10 Testkandidaten keine Charakteristiken, die ineinander transformiert werden konnten. In den Studien muss mit einer großen Personenanzahl untersucht werden, ob ohne Transformation ein Mehrwert für die Authentifizierung existiert, ob eine Transformation notwendig ist und wie die Normierungsfaktoren gewählt werden oder ob keine Informationen geräteübergreifend genutzt werden können.

Diese Transformationen der einzelnen Merkmale sollen mittels der Auswertung zeigen, wie eine Transformation von einem zu einem anderen Gerät funktioniert. Wenn diese Transformation eine Verringerung der Fehlerraten bewirkt, die vergleichbar zu den Fehlerraten auf einem Gerät ist, kann ein geräteübergreifendes Modell erzeugt werden, indem alle Merkmale beim Training und der Evaluation umgewandelt werden.

Gleichzeitig muss für die verschiedenen Geräte eine spezifische Gewichtung der Merkmale erfolgen. Mit den unterschiedlichen Fehlerraten für die einzelnen Merkmale können die Gewichte für eine bessere Klassifikation mit geringeren Fehlerraten bestimmt werden. Die Formel für die Berechnung der Gewichtungen wurde in Abschnitt 5.2.4 beschrieben. Für alle Berechnungen wurde der in Abschnitt 5.3.1 beste Exponent von 2,5 verwendet.

6.3 Evaluierung des Konzeptes

Im ersten Schritt wird analysiert, wie gerätespezifisch das Tippverhalten ist. Bereits in Abschnitt 6.1 wurde die Problematik der Verwendung von verschiedenen Geräten und den damit gekoppelten Sensoren angesprochen. Dafür stellte Abschnitt 6.2 eine Transformation vor, bei der die Merkmale in ein geräteübergreifendes Modell übertragen werden. Ein Erfolg dieser Methode hängt von der Analyse ab, wie stark der Einfluss unterschiedlicher Geräte auf die Erkennungsraten ist. In diesem Abschnitt werden die Ergebnisse der Studie **S6_Geräte** präsentiert, die zu Teilen in einer Publikation vorgestellt wurden [TSO13] und auf den Konzepten aus Abschnitt 6.2 basieren.

6.3.1 Gerätespezifische Authentifizierung

Für die Analyse der gerätespezifischen Authentifizierung müssen die Merkmale der Geräte verglichen werden. Tabelle 6.1 zeigt die unterschiedlichen Eigenschaften der Geräte (extrahiert aus der Vorstudie). Dazu zählen die Unterschiede zwischen Abstufungen der Werte für

Druckstärke und Auflagefläche, aber auch die unterschiedliche Anzahl für x- und y-Koordinaten.

Tabelle 6.1: Vergleich der Anzahl unterschiedlicher Merkmale

Gerät	Druckstärke	Auflagefläche	x/y-Koordinaten
Galaxy Nexus	159	12	574/397
Samsung Galaxy S II	10	93	384/296
Samsung Galaxy S III	1	50	542/381

Tabelle 6.1 verdeutlicht, dass es bezüglich des Verhältnisses von Druckstärke und Auflagefläche drei Kategorien bzgl. des Verhältnisses der Merkmale Druckstärke und Auflagefläche gibt. Das Galaxy Nexus bietet eine höhere Anzahl für die Werte der Druckstärke. Bei dem Samsung Galaxy S II ist es hingegen der umgekehrte Fall. Die dritte Kategorie wird durch das Samsung Galaxy S III repräsentiert, das nur einen Wert für die Druckstärke extrahiert, welches keine Klassifikation dieses Merkmals ermöglicht (in Tabelle 6.2 durch ein „-“ gekennzeichnet). Bei der Anzahl der genauen Koordinaten sind das Galaxy Nexus und das Samsung Galaxy S III sehr ähnlich. Im Gegensatz dazu bietet das Samsung Galaxy S II weniger unterschiedliche Ausprägungen der Merkmale.

Die drei Geräte spiegeln unterschiedliche Kategorien von Geräteklassen wider, auf denen jeweils drei Passwörter eingegeben wurden. Es wurden mehrere Passwörter verwendet, um passwortspezifische Eigenschaften zu minimieren. Im Gegensatz zu Abschnitt 5.3.1 werden die Ergebnisse für die einzelnen Merkmale für alle drei Passwörter und Geräte in Tabelle 6.2 einzeln aufgelistet.

Tabelle 6.2: Unterschiedliche FAR und FRR (in %) ausgewählter Merkmale (EER maximal 20 %) in Relation zu dem verwendeten Passwort und Gerät (Auszug, komplette Liste in Abschnitt A.7)

		Galaxy Nexus		Samsung Galaxy S II		Samsung Galaxy S III	
Merkmal	Aktivitäten	FAR	FRR	FAR	FRR	FAR	FRR
Verweildauer	*treter*	17,2	15,8	14,3	16,7	18,6	11,8
	module	15,6	14,8	18,9	11,8	15,6	12,8
	sommer	14,1	14,2	12,8	17,5	14,1	15,7
Digraph	*treter*	21,9	25,0	16,0	26,6	20,3	16,3
	module	15,7	21,1	17,4	12,7	18,6	8,5
	sommer	14,1	14,3	17,4	14,8	17,1	11,9
Trigraph	*treter*	17,5	35,0	25,3	21,1	17,3	24,3
	module	32,5	11,1	23,7	14,1	23,2	10,9
	sommer	15,7	18,6	26,7	11,0	17,2	16,5
Druckstärke	*treter*	15,6	14,8	33,0	15,1	-	-
	module	12,5	10,9	22,1	15,5	-	-
	sommer	12,4	9,0	23,6	11,8	-	-
Auflagefläche	*treter*	26,4	17,6	14,3	15,1	20,3	16,4
	module	18,7	17,3	11,2	14,1	21,7	11,9
	sommer	23,3	11,7	9,6	14,7	20,2	11,6
Auflagefläche2	*treter*	29,5	17,1	31,6	20,6	31,1	19,9
	module	20,3	18,6	36,2	18,9	25,0	24,0
	sommer	21,7	13,2	30,0	20,0	20,4	26,3
x-Koordinaten	*treter*	23,3	15,9	25,2	15,1	24,8	14,2
	module	17,2	19,0	16,0	25,7	17,2	20,8
	sommer	17,2	19,9	22,2	19,9	20,4	25,8
x2-Koordinaten	*treter*	20,3	17,2	25,2	12,3	18,7	18,3
	module	20,2	11,9	22,1	15,9	20,2	10,7
	sommer	20,2	14,7	22,1	13,9	18,8	18,8

Fortsetzung auf der nächsten Seite

Tabelle 6.2: Fortsetzung der vorherigen Seite

		Galaxy Nexus		Samsung Galaxy S II		Samsung Galaxy S III	
Merkmal	Aktivitäten	FAR	FRR	FAR	FRR	FAR	FRR
	treter	23,4	22,0	22,2	19,3	27,9	13,0
y-Koordinaten	*module*	17,3	24,2	17,5	21,4	18,8	23,4
	sommer	23,4	19,1	22,3	25,7	23,4	21,1
	treter	20,4	24,8	26,8	16,6	23,3	16,1
y2-Koordinaten	*module*	24,8	15,0	20,6	16,0	15,7	19,2
	sommer	21,8	18,6	26,9	18,4	20,3	20,3

Anhand der Ergebnisse aller Testkonfigurationen ist zu erkennen, dass, basierend auf den Mittelwerten, die Fehlerraten (siehe Abschnitt 5.3.1) für die einzelnen Merkmale von dem Gerät, mit dem die Authentifizierung durchgeführt wurde, abhängen. Die vollständige Liste mit allen durchschnittlichen Fehlerraten und deren Standardabweichungen ist in Abschnitt A.7 zu finden. Für das Samsung Galaxy S III konnten keine Wert für die Druckstärke ermittelt werden, da es nur einen Wert gibt, der somit nicht zur Unterscheidung genutzt werden kann. Somit kann die Druckstärke für die Verifikation mit einem Samsung Galaxy S III nicht verwendet werden. Andere Geräte wie z. B. das Galaxy Nexus weisen mehr als 159 verschiedene Werte auf (maximaler Wert aller drei verwendeten Geräte). Bei der Merkmalsgruppe Auflagefläche existieren die meisten Werte für das Samsung Galaxy S II. Es kann allgemein festgestellt werden, dass bei vielen Werten für ein Merkmal geringere Fehlerraten für ein Gerät im Vergleich zu anderen Geräten mit weniger Werten (siehe Tabelle 6.2) extrahiert werden können. Werden nun die Fehlerraten für jedes Gerät sortiert, wird deutlich, wie unterschiedlich die Merkmale ausfallen (siehe Tabelle 6.3).

Wie zu erkennen ist, können gerätespezifisch die Unterschiede der Merkmale klassifiziert werden. Die grundlegenden Zeitmerkmale (z. B. Verweildauer, Di- und Trigraph) besitzen im Allgemeinen eine signifikant höhere Erkennungsrate (laut t-Test für unabhängige Stichproben

Tabelle 6.3: Merkmale mit den geringsten Fehlerraten (basierend auf der durchschnittlichen Fehlerrate), aufsteigend sortiert

Nummer	Galaxy Nexus	Samsung Galaxy S II	Samsung Galaxy S III
1	Druckstärke	Auflagefläche	Digraph
2	Digraph	Verweildauer	Verweildauer
3	Verweildauer	Digraph	Auflagefläche
4	Trigraph	Druckstärke	Trigraph
5	Auflagefläche	x2-Koordinaten	x2-Koordinaten
6	Auflagefläche2	Trigraph	y2-Koordinaten
7	x2-Koordinaten	x-Koordinaten	y-Koordinaten
8	x-Koordinaten	y2-Koordinaten	x-Koordinaten
9	y2-Koordinaten	y-Koordinaten	Auflagefläche2
10	y-Koordinaten	Auflagefläche2	GyroZ
11	Druckstärke2	Druckstärke2	Delta2
12	Pitch	Roll	GyroY
13	Inclination	Delta2	GyroX
14	Roll	Pitch	Pitch
15	GyroX	Delta0	Delta0
16	GyroZ	GyroZ	Delta1
17	Delta0	Delta3	Inclination
18	Delta2	Delta1	Roll
19	GyroY	GyroY	Delta3
20	Delta3	GyroX	Druckstärke
21	Delta1	Inclination	Druckstärke2

[BS10, S. 121f.] mit α=0,001, bei über 94 % der Vergleiche). Darüber hinaus zeigen spezielle Merkmale auf dem Touchscreen (Auflagefläche und x/y-Koordinaten) zudem niedrige Fehlerraten auf. Lediglich die Druckstärke und die Werte des Gyroskopes besitzen im Verhältnis zu den anderen Merkmalen schlechtere Resultate. Dabei ist zu beachten, dass das Merkmal, wie schon erwähnt, von der Auswahl des Gerätes abhängig ist.

Die Fehlerraten sind nicht nur abhängig von den ausgewählten Merkmalen, sondern auch die Wahl der Wörter hat einen großen Einfluss auf die Ergebnisse. Die Merkmale Digraph, Trigraph und Druckstärke weisen im Vergleich zu den anderen getesteten Wörtern (laut t-Test für unabhängige Stichproben [BS10, S. 121f.] mit α=0,001) signifikant höhere Fehlerraten beim Wort *treter* auf. Nur bei den x/y-Koordinaten und den Gyroskop-Werten waren für das Wort *treter* im Durchschnitt höhere Erkennungsraten erkennbar.

Anhand des in Abschnitt 6.2 vorgestellten Ansatzes der Gewichtung einzelner Merkmale, können die in Tabelle 6.4 gezeigten Fehlerraten erzeugt werden.

Tabelle 6.4: Fehlerraten für die einzelnen Passwörter und Geräte (in %)

Passwort	Gerät	Kalkulierte EER	FAR		FRR	
			$\varnothing x$	s	$\varnothing x$	s
treter	Galaxy Nexus	4,43	3,61	1,50	5,26	12,26
	Samsung Galaxy S II	3,33	3,05	1,42	3,60	7,83
	Samsung Galaxy S III	3,89	4,44	1,80	3,35	8,18
module	Galaxy Nexus	2,67	2,37	1,33	2,97	7,00
	Samsung Galaxy S II	2,88	2,17	1,18	3,59	7,55
	Samsung Galaxy S III	2,06	2,92	1,41	1,19	4,39
sommer	Galaxy Nexus	2,96	2,80	1,29	3,12	8,35
	Samsung Galaxy S II	2,83	2,33	0,92	3,32	7,50
	Samsung Galaxy S III	3,05	4,13	1,42	1,98	5,34

Die Tendenzen der Ergebnisse sind analog zu den in Tabelle 6.2 dargestellten Werten. In dem Vergleich zeichnet sich das Wort *module* mit einer höheren Akzeptanzrate für alle drei Geräte aus. Die Unterschiede zum Wort *sommer* jedoch sind nicht signifikant verschieden. Beide Worte haben niedrigere Fehlerraten als das Wort *treter*. Darüber hinaus ist zu erkennen, dass die Wahl des Gerätes die Fehlerraten beeinflusst, da eine Abhängigkeit von dem Gerät bzw. den Sensoren besteht. Mit dem Galaxy Nexus wurden die niedrigsten Fehlerraten von allen drei Geräten erreicht. Die höchsten Fehlerraten entstanden bei der Verwendung des Samsung Galaxy S III, was aus den verbauten

Sensoren des Gerätes resultiert (z. B. konnte die Druckstärke nicht verwendet werden). Das Galaxy Nexus und Samsung Galaxy S II hingegen zeigten durchgehende Fehlerraten unter 3,9 % und erfüllen somit das Ziel.

S6_Geräte – Auswertung der gerätespezifische Authentifizierung

Eingabedaten:

- Passwort: *treter*, *module* und *sommer*
- Gerät: Galaxy Nexus, Samsung Galaxy S II und Samsung Galaxy S III

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: kNN

Ergebnis:

- Fehlerraten für die einzelnen Merkmale der Sensoren sind gerätespezifisch.
- Die Gewichtung der Merkmale muss je nach Gerät angepasst werden.
- Ein von der Struktur komplexeres Passwort erzeugt geringere Fehlerraten auf allen getesteten Geräten.
- Mit dem Samsung Galaxy S II und dem Galaxy Nexus wurden kleinere Fehlerraten extrahiert als mit dem Samsung Galaxy S III.

6.3.2 Geräteübergreifende Authentifizierung

Bei einem Wechsel des Gerätes oder paralleler Nutzung von mehreren Geräten muss eine geräteübergreifende Authentifizierung durchgeführt werden. Ohne die Verwendung von einem speziellen Algorithmus und Vergleich mit dem Modell, das durch ein Enrolment auf dem ersten und Verifikation auf einem zweiten Gerät genutzt wurde, werden die Fehlerraten erhöht. Die EER liegt dabei bei einem Wert zwischen 15 % und 40 % (siehe Abschnitt A.8). Dies ist nicht ausreichend, um eine Person zuverlässig zu authentifizieren.

Eine Transformation, die die Fehlerraten verringert, ist dafür notwendig. Diese wurde in Abschnitt 6.2 vorgestellt, basierend auf einer Transformation der Merkmale. Dabei wurden alle Daten von einem Gerät für das Enrolment verwendet und die Daten des zweiten Gerätes gegen das Modell jeder Person vom ersten Gerät verifiziert. Unter Verwendung dieses Ansatzes entstehen niedrige Fehlerraten (siehe Tabelle 6.5).

Tabelle 6.5: Fehlerraten, bei nur einem Enrolment für unterschiedliche Geräte (in %)

Gerät		*treter*				*module*				*sommer*			
Enrol.	Verifi.	FAR		FRR		FAR		FRR		FAR		FRR	
		$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s
Nexus	S II	14,0	1,1	16,7	18,6	14,1	1,1	12,5	16,6	12,5	1,2	9,2	10,9
	S III	7,8	1,2	6,4	9,9	7,2	1,2	5,9	9,1	7,2	1,1	4,0	6,1
S II	Nexus	13,8	1,2	13,4	16,3	13,5	1,5	10,3	13,1	10,6	1,1	10,2	12,4
	S III	12,8	1,2	13,8	16,5	14,5	1,4	11,0	14,9	13,0	1,6	9,4	12,5
S	Nexus	5,9	0,9	6,4	7,9	4,1	1,0	4,7	6,6	5,5	1,0	4,2	7,1
III	S II	15,2	1,2	9,0	12,7	9,5	1,1	11,4	13,5	10,1	1,3	8,3	11,5

In allen Fällen sind die Fehlerraten erhöht, wenn ein anderes Gerät verwendet wird. Diese sind jedoch kleiner im Vergleich zu der Analyse, bei der keine Transformation durchgeführt wurde. Darüber hinaus ist erkennbar, dass die Transformation von oder zu einem Samsung Galaxy S II die höchsten Fehlerraten im Test erzeugte. Im Durchschnitt sind

die Fehlerraten höher als 10 %. Das Samsung Galaxy S III und das Galaxy Nexus besitzen eine ähnliche Größe des Displays und ähnliche Dots Per Inch (DPI) Werte (308 and 315). Dabei signalisieren die Benutzer bei beiden Geräten ein gleiches Benutzergefühl, was ein ähnliches Tippverhalten begünstigt.

Die Fehlerraten auf unterschiedlichen Geräten hängen gleichzeitig vom Passwort ab. Die Worte *module* und *sommer* zeigen geringere Fehlerraten als das Wort *treter*.

S6_Geräte – Auswertung der geräteübergreifende Authentifizierung

Eingabedaten:

- Passwort: *treter*, *module* und *sommer*
- Gerät: Galaxy Nexus, Samsung Galaxy S II und Samsung Galaxy S III

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors (Transformation nach Abschnitt 6.2)
- Klassifikator: kNN

Ergebnis:

- Ohne Transformation kann das Modell einer Person nicht verwendet werden, da die Fehlerraten zu hoch sind.
- Die Fehlerraten sind abhängig davon, wie ähnlich die Geräte von Sensorik und Haptik sind.

6.4 Bewertung der Geräteunabhängigkeit

Anhand drei verschiedener Geräte wurde gezeigt, dass durch die verbauten Sensoren die Daten nicht identisch aufgenommen werden und dadurch die Werte unterschiedliche Qualität aufweisen. Dennoch ist zu erkennen, dass in acht von neun Untersuchungen eine kalkulierte EER von unter 3,9 % erreicht wurde. Lediglich beim Galaxy Nexus zeigte das erste Passwort (*treter*) eine EER von 4,4 % auf. In Bezug darauf, dass sich bei längeren Passwörtern die Fehlerraten verringern (siehe Kapitel 7), kann eine Authentifizierung mittels des Tippverhaltens von unter 3,9 % auf allen Geräten erreicht werden. Geräteübergreifend ohne eine Transformation ist das mit Fehlerraten von 15 % bis 40 % nicht der Fall. Nur die vorgestellte Transformation führt zu einer Verringerung der Fehlerraten. Aber insbesondere durch die Transformation sind EER's von mindestens 4,4 % erreichbar. Die geringsten Fehlerraten wurden dabei von den Geräten Galaxy Nexus und Samsung Galaxy S III erreicht. Nach der Übertragung des Merkmalmodells auf ein anderes Gerät sollte deswegen eine verstärkte Anpassung des Modells erfolgen, damit die Fehlerraten im weiteren Authentifizierungsverlauf noch verringert werden. Für sicherheitskritische Anwendungen muss daher für jedes Gerät ein neues Enrolment erfolgen.

7 Szenarienbasierte Authentifizierung

Das dritte Hauptaugenmerk stellt die szenarienbasierte Authentifizierung dar, auf die in diesem Kapitel eingegangen wird. Im Folgenden wird die Intensität des Einflusses von Störungen aufgezeigt.

7.1 Zielstellung für szenarienbasierte Authentifizierung

Karatzouni und Clark [KC07] erwähnten bereits, dass Untersuchungen fehlen, die praktische Situationen (Alltagssituationen) darstellen und nicht nur Daten verwenden, die aus klinischen Studien generiert wurden. Dabei werden z. B. das Gehen während der Eingabe oder allgemein körperliche Aspekte (z. B. Stress) angesprochen. In der Literatur wurde dieses Problem bereits adressiert. Insbesondere werden dabei die großen zeitlichen Unterschiede zwischen mehreren Authentifizierungsversuchen bei einer Person hervorgehoben [JFR08a, S. 17–18].

Die verschiedenen Bedingungen müssen bekannt sein, um ihre Auswirkungen auf das biometrische Verfahren untersuchen zu können. Tabelle 7.1 zeigt Umweltbedingungen auf, die einen Einfluss auf den Erfolg einer Authentifizierung haben können.

Für eine bessere Darstellung werden diese Bedingungen in vier Kategorien unterteilt: Der körperliche Zustand, die äußeren Einflüsse und die physikalischen Eigenschaften des Gerätes werden von der eigentlichen Eingabe unterschieden.

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_7

Tabelle 7.1: Auszug an existierenden Szenarien, die das Tippverhalten verändern

Gruppe	Szenario
Körperlicher Zustand	Bewegung (Gehen, Laufen ...) [DBB98, S. 3]
	Aufmerksamkeit/Tippen als Nebenbeschäftigung
	Stand (Sitzen, Liegen, Stehen)
	Verletzung (kurzzeitig)/Behinderung (langfristig)
	Sehhilfe (Brille, Kontaktlinsen, keine)
	Alkohol/Drogen/Medikamente/Hormone [Arb10, S. 3–4]
	Fingernagellänge
	Alter
	Müdigkeit [WSI+01, S. 915]
	Erfahrung/Gewandtheit im Umgang mit der Technik
	Stress (Zeit, Überforderung) [WSI+01, S. 915]
Äußere Einflüsse (Umwelt)	Umgebungsgeräusche/Lärm
	Licht (z. B. zu dunkel oder blendend) [Mey10]
	Unterbrechungen bei Eingabe (wie Pop-up, Anruf)
	Tageszeit
	Temperatur
	Mobile Umgebung (Zug, Bus, Auto ...)
Physikalische Eigenschaften des Gerätes	Tastaturlayout/Größe der Tasten
	Reaktion auf den Tastendruck
	Alter des Gerätes (z. B. Kratzer)
	Ausrichtung
	Gerät (Größe, Gewicht ...)
	Verschmutzte Oberfläche (z. B. Schmutz, Feuchtigkeit) [And12, Woo11]
Eingabe mit der Hand	Eine oder beide Hände
	Gewohnte/ungewohnte Hand
	Ein oder mehrere Finger
	Gerät in der Hand oder liegend (z. B. Tisch)
	Finger/Stift
	Finger/Handschuh
	Schwitzige Hände/Feuchtigkeit

Die verschiedenen Szenarien sollen zeigen, dass sich ein Benutzer mehrfach am Tag in einer anderen Situation befinden kann. Parallel zum Tippen wird eine weitere Aktion ausgeführt z. B. eine Bewegung

(Gehen, Laufen ...) oder es liegt eine Verletzung/Behinderung vor. Diese können kurzfristige oder langfristige Auswirkungen haben. Ebenso spielt die Erfahrung des Nutzers eine Rolle. Durch eine größere Erfahrung verbessert sich die Fähigkeit des Tippens und der Nutzer erreicht eine höhere Tippgeschwindigkeit. Gleichzeitig sollte sich die Lernkurve der Person, deren Adaptionsfähigkeit (z. B. durch Vorkenntnisse des QWERT-Layouts) vorhanden ist, weniger verändern.

Aber nicht nur der Benutzer selbst ist für die unterschiedlichen Szenarien verantwortlich, auch die Umwelt hat entscheidenden Einfluss. So können Lichtverhältnisse oder die Geräuschkulisse störend oder fördernd wirken. Ebenso wirkt eine mobile Umgebung, z. B. Fahren im Bus, auf das Eingabeergebnis ein, sodass Bewegungen ausgeglichen werden müssen.

Gleichzeitig ist die Art des Gerätes von Bedeutung. Bei einem zu kleinen Display kann nicht mit 10 Fingern im Hochformat geschrieben werden, was jedoch bei einem Tablet möglich ist. Vom Gewicht und Größe eines Gerätes hängt ab, ob es mit einer Hand bedient wird (halten und schreiben) oder ob beide Hände notwendig sind.

Allgemein folgen daraus unterschiedliche Eingabemöglichkeiten, die sich aber auch kurzzeitig bei einer Person ändern können, sodass sogar mit der nicht-dominanten Hand geschrieben wird.

Anhand von bisherigen Untersuchungen [HHSU08, GN11, KMB93, KSR11] wurden vier Szenarien extrahiert, die im Vergleich zum Sitzen ein unterschiedliches Tippverhalten aufweisen sollen. Dabei handelt es sich um das Tippen während des Stehens, während des Gehens, mit der nicht-dominanten Hand und unter Einfluss von Musik. Für das Stehen wird der Unterschied durch den verschiedenen Sauerstoffverbrauch begründet [HHSU08]. Die gleiche Begründung wird für das Gehen herangezogen sowie durch die zusätzlichen Bewegungen, die durchgeführt werden [GN11]. Bei der nicht-dominanten Hand ist das unterschiedliche Training, Koordinationsfähigkeit und Stärke der Hände laut Kabbash et. al [KMB93] verantwortlich. Die Veränderungen durch gleichzeitiges Musik hören wird durch rhythmische Taktfolgen verändert, somit kann durch eine schnellere Taktfolge das eigentliche Tippen schneller gemacht werden [KSR11].

Aus den beschriebenen Veränderungen verschiedener Szenarien ergeben sich folgende Ziele, die bezüglich der Szenarien analysiert werden müssen:

- Für eine Authentifizierung des Tippverhaltens muss eine Erkennung in unterschiedlichen Szenarien möglich sein. Die Fehlerraten der einzelnen Szenarien dürfen sich nicht über den in Abschnitt 1.2 beschriebenen 3,9 % befinden.
- Gleichzeitig sollte es möglich sein, dass ein Enrolment nur in einem Szenario durchgeführt wird und durch eine Transformation dieses Merkmalmodells in ein anderes Szenario die Fehlerraten auch unter der Grenze liegen. Damit wird die Benutzerfreundlichkeit erhöht, da nur einmal ein Enrolment durchgeführt werden muss.
- Falls für den vorherigen Punkt keine Fehlerraten unter 3,9 % möglich sind, muss gezeigt werden, welchen Einfluss eine Transformation der Merkmale hat und geprüft werden, ob die Fehlerraten in diesem Fall minimiert werden können.
- Ein zusätzlicher Punkt ist die Erkennung der Szenarien. Ziel ist es zu zeigen, dass die Erkennung von Szenarien möglich ist, damit eine Transformation mit einer Genauigkeit von über 90 % durchgeführt werden kann.

7.2 Konzept der szenarienübergreifenden Authentifizierung

Die Authentifizierung über mehrere Szenarien kann meist nur dann erfolgen, wenn diese erkannt werden. Eine Eingabe im Sitzen, im Gehen oder unter Verwendung der nicht-dominanten Hand etc. beeinflusst das Tippverhalten der Nutzer. Der Einfluss eines jeden Szenarios muss in einer Studie analysiert werden.

7.2.1 Prozess des Merkmalmodells

Ein Algorithmus für die Erkennung des Szenarios und eine anschließende Transformation werden im Folgenden beschrieben, um die Fehlerrate bei der Authentifizierung für die unterschiedlichen Szenarien zu verringern. Eine Erkennung erfolgt z. B. beim Gehen durch die Bewegungssensoren. Abbildung 7.1 zeigt, wie eine Extraktion der Merkmale mit und ohne Szenarientransformation durchgeführt werden kann.

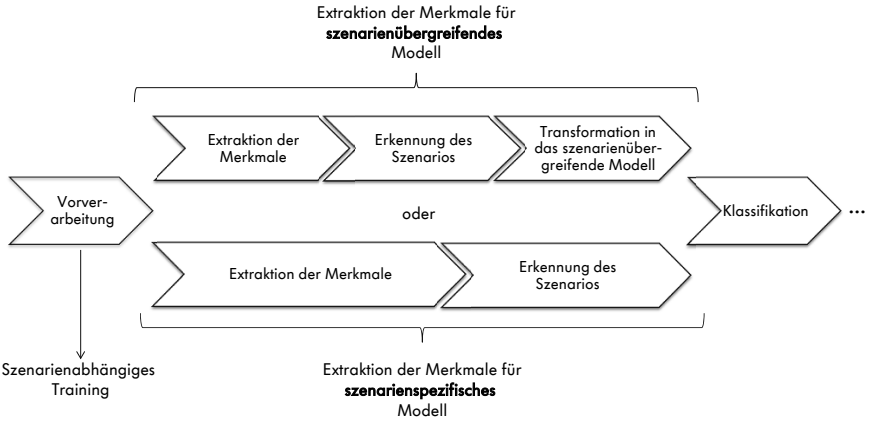


Abbildung 7.1: Unterscheidung zwischen szenarienspezifischer und szenarienübergreifender Extraktion der Merkmale

Es ist mit dem Modell nachzuweisen, dass wie bei der geräteübergreifenden Transformation die Merkmalsextraktion auch szenarienspezifisch ist. Daher muss nach der Extraktion der Merkmale eine Erkennung des Szenarios erfolgen, damit bei der weiteren Verarbeitung das richtige Referenzmodell zum Vergleich ausgewählt wird. Generell muss im Vorfeld für jedes Szenario ein Enrolment durchgeführt werden und somit existiert für jedes Szenario ein Referenzmodell.

Um die Benutzerfreundlichkeit nicht zu beeinflussen, sollte möglichst nur ein Enrolment in einer Situation stattfinden und nicht für

einzelne Szenarien jeweils ein separates Enrolment notwendig sein. Daher werden alle Authentifizierungsversuche gegen ein Modell getestet und auf Transformierbarkeit untersucht. Als Erstes werden die Erkennungsmöglichkeiten beschrieben, bevor die Transformationsalgorithmen definiert werden.

7.2.2 Erkennung der Schreibhand

Im Folgenden wird der Algorithmus zur Erkennung, mit welcher Hand bzw. mit wie vielen Händen auf dem Smartphone geschrieben wird, spezifiziert. Der Algorithmus ist dabei in zwei Teile gegliedert. Der erste Teil bezieht sich auf die Erkennung, mit wie vielen Händen getippt wird. Nach Erkennung der Anzahl der genutzten Hände erfolgt im zweiten Teil die Analyse, welche Hand benutzt wird. Die Abbildung 7.2 zeigt die vereinfachte Funktionsweise des Algorithmus. Es werden die einzelnen Entscheidungen mit einer Prozentzahl, die die Zuversicht der Entscheidung ausgibt, weitergegeben und abschließend mit einer vorher definierten Gewichtung (anhand von einer Testmenge von 10 Personen) fusioniert.

Da beim ersten Teil der Erkennung Bestandteile der Unterscheidung zwischen Rechts- und Linkshändern abgewandelt werden (Abbildung 7.2), wird der zweite Teil zuerst beschrieben.

Analyse der linken bzw. rechten Schreibhand Dieser Algorithmus beruht auf den Daten der Merkmale Druckstärke und Auflagefläche des kapazitiven Displays und dem Roll-Wert der Orientierung. Die Daten der Studie **S6_Geräte** haben gezeigt, dass sich die beiden Werte des kapazitiven Displays vergrößern, je weiter links sich die gedrückte Taste befindet. In Abbildung 7.3 wird gezeigt, dass es Unterschiede gibt, in welche Richtung die Werte vergrößert werden.

Es ist zu erkennen, dass die Werte bei Rechtshändern für die Druckstärke oben links am stärksten sind, wobei das bei der Auflagefläche unten links der Fall ist. Diese Faktoren müssen bei der Erkennung einbezogen werden. Anhand jedem dieser Werte kann der Unterschied zwischen allen vorhergehenden Zeichen überprüft werden. Bei Perso-

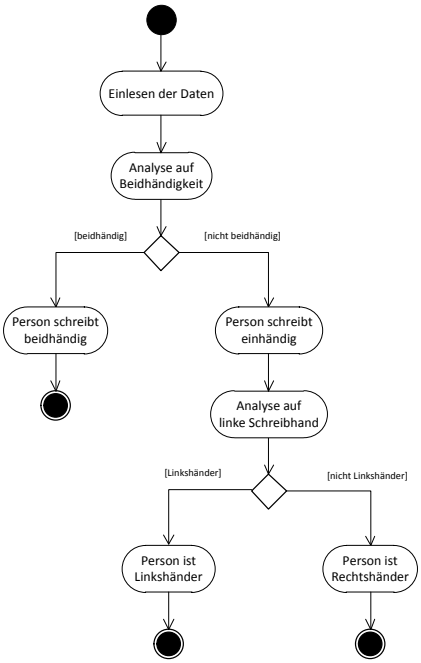


Abbildung 7.2: Vereinfachte Darstellung der Bestimmung der Händigkeit

nen, die mit der linken Hand schreiben, sind Vergrößerungen der Werte in die rechte Richtung zu erkennen. Dopplungen eines Buchstabens sollten extrahiert werden, da sich in den meisten Fällen, unabhängig von der Veränderung der Position, die Druckstärke verringert.

Zusätzlich kann, wie bereits erwähnt, der Roll-Wert der Orientierung verwendet werden. Auf Basis der Studie **S6_Geräte** wurde analysiert, dass die Roll-Werte eines Rechtshänders negativ sind, insbesondere für Buchstaben auf der linken Seite des Gerätes. Das entsteht dadurch, dass rechts das Gerät fest verankert in der Hand liegt und beim Drücken auf einen Buchstaben das Gerät auf die linke Seite kippt. Für Linkshänder gilt das analog mit positiven Werten.

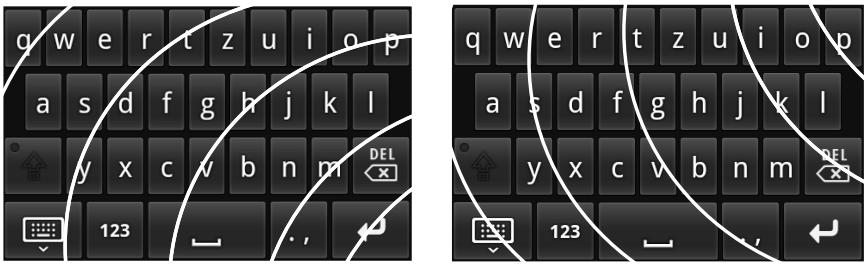


Abbildung 7.3: Links: Verlauf der Druckstärke für Rechtshänder (Maximum oben links), rechts: Verlauf der Auflagefläche (Maximum unten links)

Es wurden weitere Merkmale, wie z. B. die x- und y-Koordinaten mit ihrer Lage zum Mittelpunkt einer Taste analysiert, aber, wie auch in anderen Quellen [KWW12, HRB12] beschrieben, ist dieser Aspekt nur benutzerabhängig und unabhängig davon, mit welcher Hand geschrieben wird.

Für jedes der drei verwendeten Merkmale kann jeweils eine Entscheidung getroffen werden, um welche Hand es sich handelt. Die Zwischenergebnisse für die drei verschiedenen Merkmale können im Anschluss final fusioniert und eine endgültige Entscheidung mit welcher Hand geschrieben wird, getroffen werden.

Analyse der Beidhändigkeit Bei der Untersuchung auf Beidhändigkeit werden die Auflagefläche und Druckstärke verwendet, da in diesem Zusammenhang die größten Unterschiede zwischen dem einhändigen und beidhändigen Schreiben anhand der Daten von Studie **S6_Geräte** nachgewiesen wurden. Dabei wird das Display in zwei Hälften vertikal geteilt und nur Merkmale auf der gleichen Seite verglichen. Damit wird die Eingabe für die Beidhändigkeit gespiegelt. Somit können die Eingaben auf der linken mit der rechten Seite verglichen werden [Mei13].

Zudem kann die Flugzeit (Zeit zwischen dem Loslassen der ersten und Drücken der zweiten Taste) zwischen zwei Tasten berücksichtigt

werden. Wenn mit mehreren Fingern getippt wird, sind die Flugzeiten meist kürzer und teilweise sogar negativ. Diese Flugzeiten entstehen, indem die erste Taste noch nicht losgelassen wurde bevor die zweite gedrückt wird. Gleichzeitig können Entfernungen mit einem Finger nicht unter einer gewissen Zeitdauer (Millisekunden) zurückgelegt werden. Nach der folgenden Formel berechnet sich die Flugzeit normiert nach der zurückgelegten Strecke (s gibt dabei den euklidischen Abstand der beiden Punkte wider).

$$t_{norm} = \frac{t_{real}}{s}(normalisierte\ Zeit) \tag{7.1}$$

Durch diese Formel wird der Vergleich zwischen weit entfernten und benachbarten Tasten vereinfacht. Sowohl die negativen Zeiten als auch gewisse normierte Zeiten weisen auf das Tippen mit beiden Händen hin.

7.2.3 Erkennung von Bewegungen

Grundsätzlich ist es von Bedeutung den momentanen Zustand des Gerätes für das Re-Authentifizierungssystem (siehe Kapitel 8) und die szenarienbasierte Authentifizierung zu kennen. Bevor die Bewegungen analysiert werden können, müssen die Daten der Bewegungs- und Lagesensoren geglättet sein, da selbst bei ruhiger Lage auf einem Tisch kleine Schwankungen existieren, die die Daten verzerren. Mittels Tiefpassfilter ist das Entfernen der Schwankungen – z. B. mit dem Butterworth-Tiefpassfilter [Tön05, S. 169] – möglich.

Die gefilterten Daten können ein Modell mit Klassifikatoren trainieren oder mit diesem verglichen werden. Von den Datenströmen verschiedener Zeitboxen/Zeitbereichen (vordefinierte Zeit bzw. vordefinierte Tastenanschläge) werden bewährte Merkmale extrahiert, welche bereits getestet wurden: Durchschnitt, Minimum, Maximum, Standardabweichung, Zero-Cross (Wechsel der Daten zwischen positiven und negativen Werten) und Korrelation für die einzelnen Daten der Sensoren Accelerometer, Erdmagnet und Gyroskop (vgl. [DDK+12]).

Zusätzlich wird der Einfluss von Licht- und Annäherungssensor für Entfernungsanalysen des Gerätes berücksichtigt.

Bevor das Modell zur Erkennung der Bewegungen verwendet werden kann, muss ein Training mit fest definierten Szenarien von verschiedenen Personen durchgeführt werden, damit ein größeres Spektrum für die einzelnen Bewegungen vorhanden ist. Dieses trainierte Modell kann für die Erkennung von verschiedenen Aktivitäten mehrerer Anwender genutzt werden (siehe Abschnitt 8.3.4). Dabei erfolgt eine Unterscheidung von Zuständen (statische Lage nicht nur beim Tippen wie z. B. Gerät am Ohr oder auf einem Tisch) und Aktivitäten (Bewegungen) – siehe Abbildung 7.4.

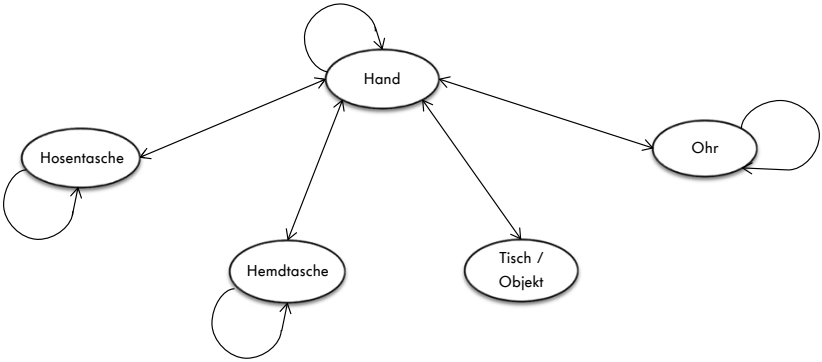


Abbildung 7.4: Zustände des Gerätes (Knoten) und Aktivitäten (Linien)

In Abbildung 7.4 sind fünf verschiedene Zustände dargestellt. Durch Aktivitäten kann sich der Zustand ändern (z. B. das Gerät für das Telefonieren zum Ohr führen oder das Gerät in die Hosentasche stecken). Die möglichen Aktivitäten müssen analysiert werden, damit eine Aussage getroffen werden kann, in welchem Szenario der Benutzer sich befindet und ob das Gerät noch vom eigentlichen Nutzer verwendet wird oder ob dazu keine Aussage getroffen werden kann. Zur Analyse

kann auch der vorherige Zustand zur besseren Erkennung dienen, ebenso wie eine Aktivität Einfluss auf den nächsten Zustand hat.

7.2.4 Transformationen

Nachdem einzelne Szenarien und Bewegungen erkannt wurden, ist es möglich mittels Transformationen die Daten in ein anderes Szenario zu überführen. Folgende Transformationen können durchgeführt werden:

Benutzung der nicht-dominanten Hand: Es ist zu beachten, dass sich das Tippverhalten bei Verwendung der nicht-dominanten Hand verändert. Jedes Merkmal, wie auch bei der Gerätetransformation, muss daher mittels einer vorher definierten Transformationsvariablen für die nicht-dominante Hand adaptiert werden. Die entsprechenden Parameter für jedes Merkmal sollen anhand einer Vorstudie mit 10 Personen festgelegt werden.

Während des Gehens: Selbst wenn alle Bewegungen erkannt werden, ist es dennoch nicht möglich, in jedem Szenario eine Transformation durchzuführen. Daher müssen dem Nutzer gewisse Restriktionen für die Authentifizierung auferlegt werden. Diese Restriktionen dienen dazu, die FAR nicht unnötig zu erhöhen.

7.3 Evaluierung des Konzeptes

Bisherige Studien über das Tippverhalten analysieren nur ein Szenario, bei dem der Nutzer ohne zusätzliche Einwirkung seiner Umwelt bzw. zusätzliche Aktionen das Passwort eingeben muss. Eine Einschränkung in der Realität, dass die Methode nur im Sitzen durchführbar ist, würde zu einer Nichtakzeptanz der Benutzer führen. In diesem Abschnitt werden unterschiedliche Szenarien verwendet und der Einfluss auf das Tippverhalten analysiert. Dabei wird die Studie **S7_Szenarien** angewendet, bei der die Personen während der Eingabe *Stehen*, *Gehen* und *Sitzen* sowie *Nutzung der nicht-dominanten Hand* und unter *Einfluss von Musik* tippen.

Die Klassifikation erfolgt mit der statistischen Klassifikation (Verifizierung), wobei alternierend zwei Eingaben für das Enrolment und eine Eingabe für die Verifikation von den 20-25 Eingaben verwendet werden. Die Gewichtungen der einzelnen Merkmale sind entsprechend der Auswertung aus Abschnitt 6.3 entnommen. Im ersten Abschnitt wird verglichen, wie der Einfluss auf jedes Szenario ist (Enrolment für jedes Szenario). Danach erfolgt die Verwendung des Modells vom Enrolment im Sitzen zur Verifikation gegenüber den anderen vier Szenarien. Um die Verschlechterung der Fehlerraten zu minimieren, wurde in Abschnitt 7.2 gezeigt, wie Szenarien erkannt werden können und welcher Einfluss existiert, wenn die Merkmale vom Sitzen für die verschiedenen Szenarien angepasst werden.

7.3.1 Neues Enrolment für jedes Szenario

Im ersten Schritt für die Analyse der Szenarien wurde für jedes einzelne Szenario ein eigenes Enrolment durchgeführt. Die Daten für die Authentifizierung sind dem gleichen Szenario entnommen. Die Ergebnisse für die einzelnen Passwörter zeigt Tabelle 7.2.

Tabelle 7.2: Fehlerraten für die verwendeten Passwörter bei der Extraktion der Daten für Enrolment und Verifizierung des gleichen Szenarios (in %)

Szenario	*anna*				*sommer*				*donnerwetter*			
	FAR		FRR		FAR		FRR		FAR		FRR	
	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s
Stehen	3,7	1,4	3,4	8,2	1,2	0,8	1,1	4,1	1,2	1,2	1,4	4,9
Gehen	2,9	1,4	6,1	9,8	2,0	1,0	3,1	9,0	0,8	0,6	1,3	5,4
Sitzen	3,5	1,3	1,7	5,5	2,8	1,2	0,3	2,0	0,5	0,5	1,3	5,5
Handwechsel	5,0	1,4	4,8	8,6	3,0	1,1	3,3	7,3	2,7	1,0	1,7	5,4
Musik	2,5	1,4	4,2	8,1	1,4	0,8	1,1	3,6	1,0	0,9	0,5	4,0

Die durchschnittlichen Fehlerraten für die einzelnen Szenarien werden im Test kleiner, je länger das gewählte Passwort ist. Das vierstellige Wort *anna* zeigt über alle Szenarien gesehen eine FAR von 3,5 % und

eine FRR von 4,0 % auf. Bei dem sechsstelligen Wort *sommer* liegen die durchschnittlichen Fehlerraten bei 2,1 % für die FAR und bei 1,8 % für die FRR. Das beste Resultat wurde mit dem Wort *donnerwetter* (zwölf Buchstaben und das längste Wort im Test) mit einer FAR und FRR von 1,2 % erreicht.

Gleichzeitig ist zu erkennen, dass für die Szenarien *Sitzen* und *Musik* die besten kalkulierten EER's berechnet werden können (1,7 % für das Sitzen und 1,8 % für die Musik). Danach folgen das Szenario Stehen (2,0 %) und mit großem Abstand das Szenario Gehen (2,7 %) und die nicht-dominante Hand (3,4 %). Je flexibler (Gehen) bzw. je ungewohnter (nicht-dominante Hand) das Szenario ist, desto höher ist die Fehleranfälligkeit. Die Bewegungen des Smartphones sind verschieden, je nachdem, ob mit dem rechten oder linken Fuß zum Zeitpunkt der Eingabe der Buchstaben des Passwortes aufgetreten wird. Auch das Nutzen der nicht-dominanten Hand erhöht die Intra-Personen-Unterschiede aller Probanden. Dadurch kommt es vermehrt zu falschen Zurückweisungen bzw. falscher Akzeptanz.

Im Detail wurden die geringsten Fehlerraten im Szenario *Musik* mit einer FAR von 1,0 % und einer FRR von 0,5 % mit dem Passwort *donnerwetter* erreicht. Das kann damit begründet werden, dass es das letzte Szenario im Test war und die Benutzer die Eingabe dieser Passwörter im Laufe der Studie übten. Dadurch sind die Intra-Personen-Unterschiede sehr gering, was die Fehlerraten verringert. Die höchsten Fehlerraten wurden bei dem Wort *anna* unter Verwendung der nicht-dominanten Hand berechnet. Mit einer FAR von 5,0 % und einer FRR von 4,8 % ist die kalkulierte EER fast sieben Mal so hoch wie bei der besten Konfiguration.

Wie schon bei der geräteübergreifenden Authentifizierung ist die Standardabweichung für die FRR höher als bei der FAR. Das liegt an der größeren Anzahl an Vergleichen (siehe Abschnitt 5.3.1). Der Durchschnitt war am geringsten für das Wort *donnerwetter*, folgend das Wort *sommer* und der schlechteste wurde beim Wort *anna* erreicht. Die Fehlerraten (bei den Wörtern *sommer* und *donnerwetter*) sind für die FAR signifikant kleiner als 3,0 % und für die FRR signifikant kleiner als 2,0 % (laut linksseitigen t-Test [BS10, S. 102f.] mit α=0,05).

Bis auf das Szenario mit der nicht-dominanten Hand sind für das Wort *donnerwetter* die Fehlerraten kleiner als 1,0 %.

Ziel eines Authentifizierungssystems ist es, in verschiedenen Szenarien nutzbar zu sein und nicht mehrere Enrolments durchzuführen, da diese für jedes neue Passwort Zeit benötigen. Im nächsten Schritt wird daher analysiert, wie das Modell einer Person im Sitzen für andere Szenarien genutzt werden kann.

S7_Szenarien – Auswertung der Authentifizierung in diversen Szenarien

Eingabedaten:

- Passwort: *anna*, *donnerwetter* und *sommer*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: kNN

Ergebnis:

- Die Fehlerraten sind abhängig vom gewählten Szenario.
- Ein längeres Passwort erzeugt geringere Fehlerraten.

7.3.2 Enrolment nur im Sitzen

Damit nur ein Enrolment für mehrere Szenarien benötigt wird, analysiert dieser Abschnitt wie die Fehlerraten sind, wenn nur ein Enrolment im Sitzen durchgeführt wird. In diesem Experiment wird geprüft, wie sich die Erkennungsraten durch das Verwenden von Daten aus unterschiedlichen Szenarien für Enrolment und Verifikation verändern, unter Anwendung der gleichen Gewichtungen (vgl. Abschnitt 7.3.1).

Die Schwellenwerte für die Merkmale wurden leicht verringert, da die Mittelwerte und Standardabweichung der Daten für die einzelnen Merkmale zwischen den Szenarien voneinander abweichen. Mit diesem Evaluationsaufbau konnten folgende, in Tabelle 7.3 abgebildete, Fehlerraten bestimmt werden.

Tabelle 7.3: Vergleich der Fehlerraten für ein Enrolment nur im Sitzen (in %).

Verifizierung	*anna*				*sommer*				*donnerwetter*			
	FAR		FRR		FAR		FRR		FAR		FRR	
Szenario	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s
Stehen	9,3	2,1	16,7	27,1	5,3	1,5	10,4	23,4	6,5	2,0	8,0	18,4
Gehen	14,7	2,3	12,4	21,6	9,6	1,9	8,2	16,4	8,2	2,1	7,0	15,2
Handwechsel	38,0	1,7	35,3	37,2	32,6	1,8	35,7	35,9	27,5	2,1	38,8	39,7
Musik	8,8	2,0	16,0	28,4	6,1	1,7	7,4	19,3	3,5	1,4	8,6	21,2

Die Ergebnisse sind deutlich schlechter als die in Tabelle 7.2, bei der für jede Authentifizierung ein szenarienabhängiges Enrolment durchgeführt wurde. Die geringsten Fehlerraten werden im Stehen und im Szenario Musik erreicht. Doch liegt die kalkulierte EER für das Wort *anna* bei über 10 % und nur für die längeren Wörter bei unter 10 % und knapp über 5 %. Wie auch bei dem Enrolment für jedes Szenario werden die Fehlerraten mit zunehmender Passwortlänge geringer. Beide Szenarien wurden zu einem unterschiedlichen Zeitpunkt des Lernprozesses durchgeführt, wodurch Veränderungen des Tippverhaltens möglich sind. Bei der Beeinflussung durch Musik wurde zudem von vielen Probanden berichtet, dass es mit Musik für die Probanden einfacher ist zu tippen. Die Fehlerraten (bei den Wörtern *sommer* und *donnerwetter*) sind für die FAR signifikant kleiner als 10 % und für die FRR signifikant kleiner als 6,5 %, außer bei dem Szenario der nicht-dominanten Hand (laut linksseitigen t-Test [BS10, S. 102f.] mit α=0,05). Die Fehlerraten sind gleichzeitig nicht signifikant kleiner als die geforderten 3,9 %.

Die mit Abstand schlechteste Erkennungsrate ergab sich bei der Verwendung der nicht-dominanten Hand. Mit dieser Hand existiert ein großer Unterschied im Tippverhalten. Nicht nur, dass das Tippen des Passwortes längere Zeit in Anspruch nimmt, es wird auch das Gerät vom Winkel her unterschiedlich gehalten. Ohne eine Transformation kann die nicht-dominante Hand somit nicht verwendet werden, da die kalkulierte EER von ca. 35 % nur eine leichte Verbesserung zum Raten ist (50 %). Die Fehlerraten beim Gehen zeigten hingegen bei der Verifikation eine geringere Erhöhung als für die anderen Szenarien, verglichen zu den Fehlerraten aus Tabelle 7.2. Das liegt unter anderem daran, dass die Szenarien direkt nacheinander aufgenommen wurden. Somit war der Lerneffekt (siehe Auswertung in Abschnitt 5.3.5) mit der dominanten Hand nicht so hoch wie für die anderen Szenarien.

Allgemein muss in einem realen System analysiert werden, ob eine andere Gewichtung für die Merkmale gewählt werden sollte, damit es bei Verwendung unterschiedlicher Szenarien nicht fehleranfällig ist. Dadurch wird das Minimum an Fehlerraten erhöht, jedoch ist das Verfahren szenarienübergreifend benutzerfreundlicher und sicherer.

Bei einem ausreichend langem Passwort und unter Betrachtung des Lernprozesses sind die Fehlerraten von ca. 5 % für das Szenario Stehen und Musik angemessen, wenn der Hauptfokus nicht auf der Sicherheit, sondern auf Benutzerfreundlichkeit liegt. In anderen Fällen darf entweder die Authentifizierung nur für limitierte Szenarien durchgeführt werden oder es muss für jedes Szenario ein extra Enrolment geben, was im Besonderen für die nicht-dominante Hand und der Authentifizierung im Gehen gilt. Damit das korrekte Modell, in dem sich der Benutzer befindet, verwendet werden kann, muss eine Erkennung der Szenarien erfolgen, was im folgenden Abschnitt beschrieben wird.

S7_Szenarien – Auswertung der Authentifizierung in diversen Szenarien (Enrolment im Sitzen)

Eingabedaten:

- Passwort: *anna*, *donnerwetter* und *sommer*

- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: kNN (Enrolment im Sitzen)

Ergebnis:

- Modell einer Person kann nicht für jedes Szenario genutzt werden.
- Eine Transformation für die Szenarien Gehen und nicht-dominante Hand muss angewendet werden.

7.3.3 Erkennung von Szenarien

Als zusätzliches Merkmal kann die Erkennung der Hand oder ob sich die Person in Bewegung befindet, genutzt werden. Gleichzeitig dienen, wie in Abschnitt 7.2 erläutert, diese Szenarien dazu, eine Transformation des Modells für das entsprechende Szenario durchzuführen. Die Ergebnisse für die beiden Erkennungsalgorithmen werden in diesem Abschnitt präsentiert.

Handerkennung

Um zu erkennen, mit welcher Hand die Eingabe erfolgt, wurde in Abschnitt 7.2 ein Algorithmus zur Erkennung beschrieben. Die Konfiguration wurde anhand des Wortes *anna* trainiert und mit den anderen beiden Wörtern verifiziert. Die Erkennungsgenauigkeit für den ersten Schritt, einhändige oder beidhändige Eingaben, wird für die einzelnen Szenarien in Tabelle 7.4 dargestellt. Da bekannt ist, mit welcher Hand ein Nutzer vorrangig tippt, muss nur diese überprüft werden. Um im letzten Schritt die Gesamtgenauigkeit zu betrachten, wird dieses Szenario im Folgenden vernachlässigt.

Tabelle 7.4: Erkennungsraten Einhändigkeit vs. Beidhändigkeit (in %)

Wort	Szenario					Gesamt
	Stehen	Gehen	Sitzen	Handwechsel	Musik	
sommer	91,14	91,14	96,20	95,38	92,41	93,25
donnerwetter	96,20	96,20	97,47	96,20	96,20	96,44
						94,85

Die durchschnittliche Erkennungsrate steigt mit zunehmender Buchstabenzahl. Im Vergleich zum Wort *anna* (Erkennungsrate 89,87 %), mit dem der Algorithmus trainiert wurde, liegt die Genauigkeit für die längeren Wörter bei über 90 % und beim Wort *donnerwetter* sogar bei über 95 %. Eine Eingabe im Sitzen erzeugt für alle Wörter eine geringfügig bessere Erkennungsrate als für die weiteren Szenarien. Wenn nur die beiden zur Validierung verwendeten Wörter (*sommer* und *donnerwetter*) betrachtet werden, hat die Handerkennung eine Genauigkeit von fast 95 %.

Nach Erkennung der einhändigen oder beidhändigen Eingabe kann im zweiten Schritt analysiert werden, ob für die einhändigen Eingaben mit links oder rechts getippt wurde. Die Auswertung dafür ist Tabelle 7.5 zu entnehmen. Der Algorithmus für diesen Schritt wurde mit dem Wort *anna* konfiguriert. Für diesen Schritt fanden nur die Versuche Verwendung, bei denen der Benutzer mit einer Hand geschrieben hat.

Tabelle 7.5: Erkennungsrate von Links- und Rechtshändern (in %)

Wort	Szenario					Gesamt
	Stehen	Gehen	Sitzen	Handwechsel	Musik	
sommer	93,75	93,75	93,75	93,75	93,75	93,75
donnerwetter	96,25	93,75	98,75	98,73	98,75	97,25
						95,5

Sowohl die Konfiguration für das Wort *anna* (Genauigkeit 91,17 %) als auch für die Validierungswörter zeigen eine höhere Genauigkeit, sodass die Gesamterkennung bei über 95 % liegt. Zudem war auch in diesem Schritt eine bessere Erkennung für längere Wörter gegeben, wobei mit einer Wahrscheinlichkeit von 97,25 % die Schreibhand anhand des Wortes *donnerwetter* erkannt wurde.

Werden beide Prozessschritte gemeinsam betrachtet, ergeben sich folgende Erkennungsraten (siehe Tabelle 7.6) für die Erkennung der Schreibhand/Schreibhände.

Tabelle 7.6: Gesamterkennungsrate mit welcher Hand bzw. ob mit beiden Händen getippt wurde (in %)

Wort	Szenario					Gesamt
	Stehen	Gehen	Sitzen	Handwechsel	Musik	
sommer	89,87	91,14	92,41	91,14	89,87	90,89
donnerwetter	94,94	92,41	97,47	97,47	96,20	95,70
						93,29

Durch die einzelnen Fehler der beiden Schritte verringert sich die Gesamtgenauigkeit im Vergleich zu den einzelnen Schritten. Dennoch liegt die Gesamtgenauigkeit bei 93 % (im Vergleich zum Wort *anna* konnte durch die beste Konfiguration ein Wert von 87,52 % erreicht werden). Mit über 95 % war bei dem Wort *donnerwetter* die genaueste Erkennung der Hand möglich.

Damit besteht die Möglichkeit, die Hand, mit der geschrieben wird, zu erkennen und eine Transformation kann durchgeführt bzw. das entsprechende Modell zur Verifikation verwendet werden, falls die Fehlerraten durch eine Transformation nicht ausreichend sind.

Erkennung des Gehens

Die Erkennung einer Person kann zum einen über Events während der Berührungen des Touchscreens (d. h. Bewegungsdaten werden nur beim Tippen extrahiert) oder zum anderen als Stream kontinuierlich

vom ersten bis zum letzten Event (Daten werden zyklisch, unabhängig vom Tippen extrahiert) erfolgen. Der zweite Fall wird als Teil der Bewegungserkennung in Abschnitt 8.3.4 adressiert.

Die Bewegungsdaten (Daten der Sensoren: Orientierung, Gyroskop und Delta) wurden mittels neuronalem Netz getestet unter Verwendung einer Cross-Validierung, siehe Abschnitt 5.3.2. Alle 3.292 Datensätze aus den Szenarien Gehen und Sitzen wurden für das Wort *donnerwetter* korrekt klassifiziert. Somit kann exakt zwischen diesen beiden Szenarien unterschieden werden. Eine Transformation der Daten bzw. das Verwenden eines Enrolments im Gehen ist damit möglich.

7.3.4 Nachweis der Verbesserung durch eine Szenarientransformation

In Tabelle 7.7 werden die Transformationen aus Abschnitt 7.2 angewendet, um die Fehlerraten bei Verwendung von nur einem Enrolment im Sitzen zu verringern. Ohne diese Transformationen sind die Fehlerraten für das Gehen und die nicht-dominante Hand zu hoch, wie in Tabelle 7.3 zu sehen. Nur Fehlerraten der Szenarien Musik und Stehen sind ausreichend gering, sodass sie in diesem Abschnitt nicht betrachtet werden.

Tabelle 7.7: Fehlerraten bei einer Transformation zum Szenario Sitzen (in %)

Konvertierung von Szenario	Gehen		Handwechsel	
	FAR	FRR	FAR	FRR
sommer	7,34	8,78	30,97	28,51
donnerwetter	6,24	6,72	29,08	24,6

Tabelle 7.7 zeigt, dass die Fehlerraten im Vergleich zu Tabelle 7.3, bei der keine Transformation durchgeführt wurde, sinken. Die kalkulierte EER liegt nicht mehr über 30 %. Aber sie zeigen vor allem

bei der nicht-dominanten Hand mit 26,83 % (beim Wort *donnerwetter*) noch sehr hohe Werte für ein nutzbares System auf. Die Transformation zeigt nur bedingt Auswirkung auf die Durchschnitte der Fehlerraten. Es müssten für jede einzelne Person eigene Transformationsvariablen berechnet werden, da die Geübtheit einer Person mit der nicht-dominanten Hand im Vergleich zur dominanten Hand nicht konstant ist.

Es existieren Personen, die mit beiden Händen ähnlich tippen, andere haben große Schwierigkeiten mit der nicht-dominanten Hand zu schreiben. Zudem ist es sinnvoll eine Unterscheidung von Rechts- und Linkshändern einfließen zu lassen, da der Winkel, in dem das Gerät gehalten wird, von der genutzten Hand abhängig ist. Aber auch in dem Szenario Gehen werden die Fehlerraten nicht ausreichend verringert. Durch das Gehen wird das Schreibmuster beeinflusst, sodass es sich nicht linear verändert. Die Einflüsse bei diesem Szenario zeigen Forschungsbedarf auf, um eine angepasste Transformationsformel zu generieren.

Allgemein sind diese Fehlerraten im Vergleich zu den Szenarien Musik und Stehen für eine sichere und benutzerfreundliche Authentifizierung zu hoch. Es muss daher in der Realität überlegt werden, den Schwellenwert anzupassen, damit die FAR bzw. FRR geringer ist, um den Fokus auf die Sicherheit oder Benutzerfreundlichkeit zu legen. Auf der anderen Seite kann das System bei Erkennung von den zwei in Tabelle 7.7 gezeigten Szenarien den Versuch ablehnen, um damit bessere Gesamtfehlerraten erzeugen zu können. Dafür existieren jedoch verschiedene Einschränkungen der Benutzerfreundlichkeit. Eine weitere Möglichkeit besteht darin, direkt ein Enrolment für die unterschiedlichen Szenarien durchzuführen. Bei der Erkennung eines Szenarios kann das dafür entsprechende Modell verwendet werden.

S7_Szenarien – Auswertung der Transformation der Szenarien (Enrolment im Sitzen)

Eingabedaten:

- Passwort: *anna*, *donnerwetter* und *sommer*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors (Transformation nach Abschnitt 7.2)
- Klassifikator: kNN (Enrolment im Sitzen)

Ergebnis:

- Fehlerraten werden verringert.
- Enrolment für die nicht-dominante Hand ist erforderlich.

7.4 Bewertung der Szenarienabhängigkeit

Es werden im Folgenden die einzelnen Unterziele dieses Kapitels, die in Abschnitt 7.1 aufgestellt wurden, bewertet:

Szenarienspezifisches Enrolment: Im Test zeigen alle Versuche mit einem Passwort der Länge sechs oder mehr Zeichen, dass die Fehlerraten im Durchschnitt unter 3,9 % lagen und nur bei Verwendung der nicht-dominanten Hand bei dem Passwort *anna* bei mehr als 3,9 %. Das gilt, wenn für jedes Szenario ein eigenes Enrolment existiert. Im Allgemeinen sind bei einem längeren Passwort die Fehlerraten szenarienunabhängig kleiner als bei kürzeren Passwörtern.

Enrolment nur in einem Szenario: Wird das Enrolment nur im Sitzen verwendet, vergrößern sich die Fehlerraten besonders für die Szenarien Gehen und Handwechsel. Mit Fehlerraten von über 30 % ist das Verfahren nicht einsetzbar. Auch im Stehen und bei dem Szenario, bei dem der Nutzer Musik hörte, existieren höhere Fehlerraten um 7 %. Eine Erhöhung ist durch den unterschiedlichen Zeitpunkt des Szenarios zu erklären. Mit zunehmender Zeit kamen die Benutzer immer besser mit dem Tippen zurecht. Dabei lagen zwischen der Eingabe für das Enrolment und der Verifizierung mehr als 240 Eingaben (drei Szenarien mit 40 Wiederholungen von drei Passwörtern inkl. den Versuchen, die nicht korrekt eingegeben wurden).

Erkennung von Szenarien: Die Szenarien Gehen und Handwechsel wurden aufgrund der hohen Fehlerraten genauer betrachtet. Das Ziel bestand in der Erkennung der Szenarien und der Transformation des Merkmalmodells. Die Erkennung vom Gehen und anderen Bewegungen wird in Abschnitt 8.3.4 genauer betrachtet. Dabei wird ersichtlich, dass Bewegungen mit dem Gerät mit einer Genauigkeit von 99 % erkannt werden können. Bei der Handerkennung wurde mittels eines kNN und der vorher analysierten Merkmale eine Erkennungsrate von über 93 % erreicht.

Szenarientransformation: Mit den Erkennungsraten der Szenarien ist es möglich, die Szenarien herauszufinden und eine Transformation durchzuführen. Im Szenario Gehen war eine leichte Verbesserung der Fehlerraten sichtbar. Zusätzlich kann die Authentifizierung mit einer Erkennung der Person fusioniert werden, um das Ergebnis zu verbessern. Dennoch muss zur Verbesserung der Fehlerraten überlegt werden, ob ein zusätzliches Enrolment in dem Szenario verwendet werden sollte, damit die Fehlerraten kleiner als 3,9 % erreicht werden. Das gilt insbesondere für das Tippen mit der nicht-dominanten Hand. Trotz einer Transformation liegen die Fehlerraten noch über 20 %. Das Tippverhalten der Hände weist zu große Unterschiede auf.

8 Nutzung der Bewegungserkennung, textabhängigen und textunabhängigen Authentifizierung zur Re-Authentifizierung

Mit dem Re-Authentifizierungssystem wird die Möglichkeit vorgestellt, kontinuierlich eine Identitätsüberprüfung durchzuführen, wodurch durchgehend eine Erkennung der Person erfolgt. Dazu müssen neben der textabhängigen Authentifizierung eine textunabhängige Authentifizierung sowie eine Bewegungserkennung erfolgen, um kontinuierlich eine Aussage über die Person treffen zu können.

Darüber hinaus befasst sich dieses Kapitel mit der allgemeinen Nutzbarkeit des Verfahrens. Dafür werden verschiedene Passwörter verwendet und diese mit generierten Negativbeispielen trainiert, bevor letztlich basierend auf den bestehenden Gewichtungen und Schwellenwerten geprüft wird, wie die FAR und FRR ausfallen.

8.1 Zielstellung des kontinuierlichen Authentifizierungssystems

Damit das Tippverhalten in einer realen Situation zur Authentifizierung genutzt werden kann, muss eine Methode existieren, die die negativen Beispiele generiert, damit eine Klassifikation erfolgen kann. Dazu wird in diesem Kapitel eine Methode basierend auf der textunabhängigen Authentifizierung vorgestellt. Im Vergleich zu vorhandenen

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_8

Lösungen sollen dabei Fehlerraten von unter 7,0 % (Studie mit der geringsten Fehlerrate, siehe Abschnitt 3.1.1) erzeugt werden.

Zusätzlich muss analysiert werden, mit welchen Fehlerraten die textabhängige Authentifizierung basierend auf generierten Negativbeispielen arbeitet. Dafür dürfen die Fehlerraten nicht über die angesprochenen 3,9 % für die textabhängige Authentifizierung steigen.

Darüber hinaus kann mittels der textunabhängigen Authentifizierung und einer Bewegungserkennung eine kontinuierliche Authentifizierung erreicht werden. Damit das theoretische Konzept praxistauglich wird, müssen die Fehlerraten unter den bisher definierten Werten liegen (textabhängig 3,9 % und textunabhängig 7,0 %). Entsprechend muss die Bewegungserkennung in dem gleichen Bereich der Erkennungsrate (ähnlich groß) liegen.

8.2 Konzept der kontinuierliche Authentifizierung

Dieser Abschnitt beschreibt wie eine kontinuierliche Authentifizierung erfolgen kann. Diese Authentifizierung beruht auf dem Konzept der Nutzung der textunabhängigen Authentifizierung zur Generierung der negativen Merkmale für die Klassifikation und der Generierung eines Re-Authentifizierungsprozesses. Dazu wird nach der Notwendigkeit dieses Verfahrens das grundsätzliche Modell mit der Fusion von unterschiedlichen Modalitäten definiert. Abschließend erfolgt eine transparente Berechnung für das Vertrauen während der Nutzung.

8.2.1 Textunabhängige Erweiterungen beim klassischen Tippen

Damit nicht nur bei der initialen Authentifizierung das Tippverhalten analysiert wird, sondern auch während der Benutzung des Gerätes, kann eine textunabhängige Authentifizierung erfolgen. Diese analysiert wie stark sich das durchschnittliche Tippverhalten einer Person verändert.

Eine Vielzahl von Daten kann nur beim Tippen eines vorher definierten Textes extrahiert werden. Es ist schwierig alle Di- bzw. Trigraphen

einer Person in einer Datenbank bereits vorhanden zu haben. Bereits bei Buchstaben (ohne Sonderzeichen), die klein geschrieben sind, gibt es allein für den Trigraphen $26^3 = 17.576$ Kombinationen. Die in der Datenbank vorhandenen Di- und Trigraphen können zur Authentifizierung verwendet werden, bei den restlichen n-Graphen fehlen die gespeicherten Werte, sodass diese bei der Authentifizierung ignoriert werden müssen. Für die anderen Daten muss der dazugehörige Buchstabe vorher bereits einmal getippt worden sein.

Daher ist es wichtig, weitere Merkmale zu finden, die auch textunabhängig sind. Diese Merkmale können dann zusätzlich zu einer textabhängigen Authentifizierung verwendet werden.

Im Folgenden werden zunächst eine Reihe von bekannten Merkmalen genannt [MR97, GPR05, Erd13], die extrahiert werden können:

- Durchschnittliche Druckdauer je Taste,
- Durchschnittlicher Digraph zweier Tasten,
- Durchschnittlicher Trigraph dreier Tasten und
- Durchschnittlicher n-Graph von n-Tasten.

Weiterhin können durch das kapazitive Display folgende Merkmale genutzt werden:

Durchschnittliche x/y-Koordinate pro Buchstabe: In Relation zum Mittelpunkt einer Taste kann extrahiert werden, in welchem Bereich diese Taste durchschnittlich gedrückt (x/y-Koordinaten) wird.

Durchschnittliche Druckstärke pro Buchstabe: Für jede Taste kann aufgenommen werden, mit welcher Kraft durchschnittlich auf diese gedrückt wird.

Durchschnittliche Auflagefläche pro Buchstabe: Neben der Druckstärke kann gleichzeitig die durchschnittliche Auflagefläche für jede Taste extrahiert werden.

Durchschnittliche Neigung des Gerätes pro Buchstabe: Die durchschnittliche Neigung des Gerätes bei einem Tastendruck kann durch den Pitch- und den Roll-Wert repräsentiert werden.

Verwendung von Sondertasten: Fehler beim Schreiben (Verschreiben) können durch versehentliches Treffen der falschen Taste oder durch Denkfehler entstehen. Diese Fehleranzahl kann als Merkmal verwendet werden, indem gezählt wird, wie oft die Löschen-Taste gedrückt wird. Gleichzeitig achten nicht alle Personen auf Smartphones auf die Groß- und Kleinschreibung, wodurch das Verwenden der Shift-Taste ebenfalls berücksichtigt werden kann.

Erkennung der Schreibhand: Ein Algorithmus zur Erkennung mit welcher Hand der Benutzer getippt bzw. ob er beide Hände verwendet hat, wurde bereits in Abschnitt 7.2 vorgestellt.

Die Gesamtheit der Daten muss – anders als bei der textabhängigen Authentifizierung – nicht in einer vordefinierten Reihenfolge aufgenommen werden. Alle vorgestellten Daten werden dann in der textunabhängigen Authentifizierung benutzt. Einige Buchstaben werden sehr oft verwendet, in diesem Fall wird über die verschiedenen Eingaben der Durchschnitt ermittelt. Andere Buchstaben werden kaum bis gar nicht verwendet und sind deshalb nicht in dem Modell für den Benutzer gespeichert. Diese Werte können bei der Authentifizierung nicht eingesetzt werden. Je mehr Daten im Modell enthalten sind, desto mehr Informationen stehen für die Authentifizierung zur Verfügung.

8.2.2 Generierung der Negativbeispiele

Zusätzlich zu den Verbesserungsschritten bei den statistischen Klassifikatoren existieren bei allen Klassifikatoren weitere Herausforderungen. Es gibt z. B. das Problem, dass insbesondere ein neuronales Netz Negativbeispiele (Authentifizierungsversuche von anderen Personen) zum Trainieren des Netzes benötigt [CTL12, S. 1159]. Ziel ist es, dass sich der Benutzer an einem Smartphone authentifizieren kann. Sein

Enrolment erfolgt durch Eingabe seines (geheimen) Passwortes. Um Negativbeispiele zu erzeugen, müssen andere Personen auch dieses Passwort eingeben. Damit wäre es aber nicht mehr geheim. Dieses Problem wird gelöst, indem Daten von einer textunabhängigen Authentifizierung verwendet werden (Auswertung siehe Abschnitt 8.3.2). Diese können speziell für das vom Nutzer gewählte Passwort Merkmale generieren, die als Negativbeispiele von anderen Personen dienen können. Somit können das neuronale Netz oder andere Klassifikatoren in der Realität trainiert werden.

Des Weiteren müssen Untersuchungen durchgeführt werden, welche Schwellenwerte für die Authentifizierung mittels des Tippverhaltens besser geeignet sind (siehe Abschnitt 8.3.1).

8.2.3 Notwendigkeit einer kontinuierlich durchgeführten Authentifizierung

Das Hauptproblem bei den existierenden Authentifizierungsansätzen ist, dass sie nur eine initiale Authentifizierung darstellen und keine kontinuierliche. Das bedeutet, dass nach der anfänglichen Authentifizierung zu keinem weiteren Zeitpunkt nachgewiesen werden kann, ob es noch die gleiche Person ist oder nicht. Ein fixer Text bzw. Passwort kann nur zu Beginn genutzt werden (sonst wird der Nutzer zu stark in seiner Arbeit gestört), danach muss eine textunabhängige Erkennung erfolgen, die noch nicht ausreichend für Mobiltelefone mit Touchscreens untersucht wurde (siehe Abschnitt 3.1).

Das Erkennen von Bewegungen mit dem Smartphone wurde bereits bei der Gangerkennung verwendet. In diesem Bereich sind die Fehlerraten aber zu hoch, um als einzige Authentifizierungsmethode zu agieren. Hierzu ist eine Fusion mit einer anderen Methode notwendig.

Damit verstanden wird, durch welche Authentifizierungsmethoden eine Fusion durchgeführt werden kann, ist in Abbildung 8.1 der Prozess während des Entsperrens und des Sperrens eines Gerätes dargestellt.

Das Sperren eines Bildschirmes bezeichnet den Prozess, der nach Reaktivierung des Gerätes die Eingabe einer Authentifizierungsmethode erfordert. Ein Bildschirmschoner führt nicht zwangsweise zum

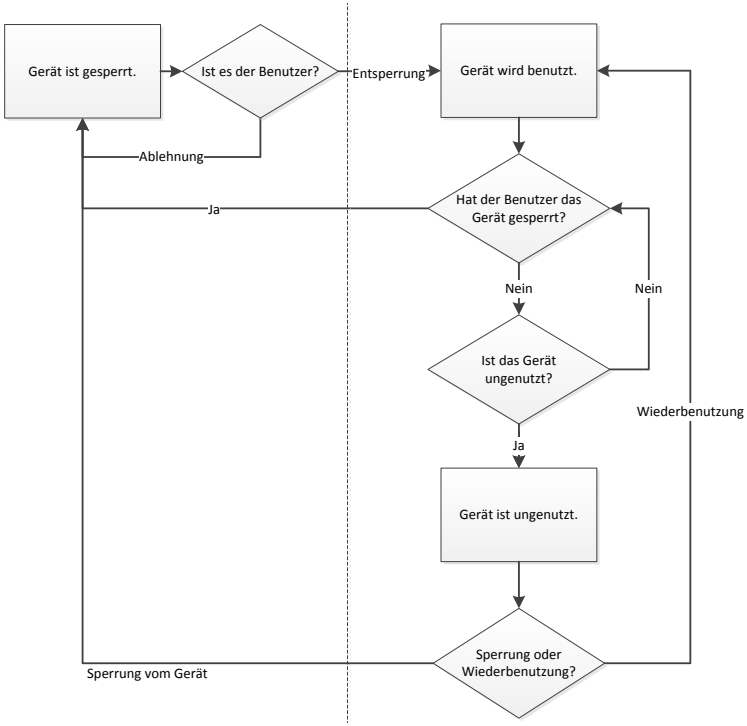


Abbildung 8.1: Ablauf der Sperrzustände eines Smartphones

Sperren des Gerätes. Wenn ein Nutzer versucht sein Smartphone zu verwenden, muss er sich gegenüber diesem authentifizieren. Wie schon in Abschnitt 8.2.1 beschrieben, kann auch hier das Tippverhalten angewendet werden. Nach der Nutzung des Gerätes können drei Fälle eintreten. Zum einen kann der Nutzer das Gerät selbst sperren oder zum anderen das Gerät sperrt sich nach einer vorher bestimmten Zeit. Darüber hinaus besteht die Möglichkeit, dass der Nutzer das Gerät wieder verwendet, bevor es gesperrt ist. In diesem Fall ist es nicht möglich, ohne eine kontinuierliche Authentifizierung, eine Aussage zu treffen, ob es sich immer noch um den gleichen Nutzer handelt oder nicht.

8.2.4 Konzept der kontinuierlichen Authentifizierung

Grundsätzlich existieren zwei Punkte, die bei dem Modell aus Abbildung 8.1 entscheidend sind und daher sowohl einzeln als auch als komplexes System betrachtet werden müssen. Zum einen ist es die initiale Authentifizierung zum Entsperren des Gerätes, zum anderen eine kontinuierliche Authentifizierung während der Benutzung und auch danach, wenn das Gerät entsperrt ist, aber nicht genutzt wird. Nur wenn alle diese Punkte für ein Authentifizierungssystem betrachtet werden, kann während der gesamten Zeit, in der das Gerät entsperrt ist, eine Aussage getroffen werden, mit welcher Sicherheit der eigentliche Nutzer das Gerät in der Hand hält.

Da dieses Konzept nur auf das kapazitive Display und die Bewegungssensoren abzielt, kann die initiale Authentifizierung an dem Gerät mittels des Tippverhaltens oder einer Gangerkennung erfolgen. Wie in Abschnitt 3.1 beschrieben, ist die Gangerkennung bisher durch ihre Fehlerraten nicht geeignet, um allein mit einer ausreichenden Sicherheit zu erkennen, ob es sich um eine spezielle Person handelt oder nicht. Darum wird eine Authentifizierung mittels eines bestimmten Passwortes vorgeschlagen, welches bereits in Abschnitt 5.2.1 beschrieben wurde.

Bereits Abschnitt 5.2.1 zeigt, dass die Daten des Gyroskop Sensors für verschiedene Aktivitäten ein Muster aufweisen. Generell kann mit dem Gyroskop analysiert werden, ob sich das Gerät bewegt oder ruht. Besonders, wenn der Nutzer das Gerät nicht in Betrieb hat oder einsetzt, ist es wichtig, diese Informationen zu erhalten, um für die Verifizierung mehr Daten zu haben. Außerdem kann eine Authentifizierung mithilfe der Gangerkennung erfolgen und damit Informationen für eine Re-Authentifizierung liefern.

Des Weiteren können bei Benutzung der Tastatur über das kapazitive Display Daten extrahiert werden, die zur textunabhängigen Authentifizierung verwendet werden können (siehe Abschnitt 3.1.1).

Für eine kontinuierliche Authentifizierung sind sowohl eine Gangerkennung als auch ein textunabhängiges Tippverhalten geeignet und werden daher beide betrachtet. Damit kann entschieden werden,

ob eine Person das Gerät weiter benutzen kann oder ob das Gerät gesperrt werden muss. Um in diesem Fall das Gerät wieder nutzen zu können, muss der Besitzer sein Passwort erneut eingeben (siehe Abbildung 8.1).

8.2.5 Vertrauensmodell

In dem vorherigen Abschnitt wurden biometrische Methoden beschrieben, die für ein Framework genutzt werden können, um herauszufinden, ob es sich noch um die gleiche Person handelt, die das Gerät nutzt. Für dieses Framework wird ein Vertrauensmodell benötigt, welches beurteilt, ob nach einer bestimmten Zeit immer noch der gleiche Benutzer das Gerät in der Hand hält oder nicht. Der Grundgedanke des Vertrauensmodells ist, dass bei initialer Authentifizierung initiales Vertrauen gesetzt wird. Dieses sinkt dann mit zunehmender Nutzungsdauer. Die Sinkgeschwindigkeit ist abhängig vom biometrisch bestimmten Vertrauen, dass der Benutzer noch dieselbe Person ist. Ist das Restvertrauen zu gering, wird das Gerät gesperrt. Entsperrt der Benutzer es, beginnt der Prozess von Neuem.

Abbildung 8.1 zeigt alle Abläufe auf, die durch das Modell beschrieben werden müssen. Wenn das Gerät gesperrt ist, muss der Benutzer sich mittels seines Passwortes und den dazugehörigen biometrischen Merkmalen authentifizieren. Der Grundwert bei dem Vertrauensmodell wird bei dieser initialen Authentifizierung gesetzt. Ein höheres Vertrauen ($auth_{initial}$) bei der initialen Authentifizierung ergibt einen höheren Grundwert zu Beginn der Nutzung (Minimum:0; Maximum:1). Darüber hinaus hat die Nutzungszeit eine wichtige Bedeutung für das Vertrauen. Je mehr Zeit nach der initialen Authentifizierung vergangen ist, desto kleiner wird das Vertrauen $trust(t)$ (wobei t den aktuellen Zeitblock beschreibt). Nur durch Re-Authentifizierungsmethoden (verschiedene Authentifizierungsmethoden während der Nutzung) kann das Vertrauenslevel konstant gehalten werden. Dieses Konzept wird durch folgende Formeln präsentiert:

$$trust(t) = auth_{initial} - \alpha \sum_{i=0}^{t} (cert(i)) \tag{8.1}$$

mit

$$cert(t) = \begin{cases} 0, & wenn(key(t) \neq null) \& (\beta\ move \\ & +\alpha\ key \geq \delta) \\ 0, & wenn(key(t) = null) \& (move \geq \delta) \\ \frac{\delta}{2} - \beta\ move(t), & wenn(key(t) = null) \\ \delta - (\beta\ move(t) + \alpha\ key(t)), & sonst \end{cases} \tag{8.2}$$

Es wird ersichtlich, dass sowohl die initiale Authentifizierung als auch die Sicherheit $cert(t)$ während eines Zeitblocks Einfluss auf das Vertrauensmodell haben. Der Wert 0 repräsentiert ein hohes Vertrauen und 100 ein niedriges bezüglich der Person. Die Länge einer Zeitbox muss in Abhängigkeit zu β und α erforscht werden. α und β stellen Variablen dar, die durch Tests bestimmt werden müssen. Während dieser Zeit wird das temporäre Vertrauen ($trust(t)$) anhand der Erkennung am Gang und von Bewegungen (siehe Abschnitt 7.2) $move(t)$ sowie der Interaktion mit dem kapazitiven Display $key(t)$ (vor allem das Tippverhalten) berechnet. Die Werte $move(t)$ und $key(t)$ basieren auf den Erkennungsraten der einzelnen Authentifizierungsmethoden. Beide Werte sagen aus, wie sicher das Gerät ist, die Person anhand des entsprechenden Sensors zu erkennen. Dabei können die Werte zwischen 0 und 100 liegen. Der Wert δ beschreibt den Schwellenwert, der erreicht werden muss, damit sich das Gesamtvertrauen nicht verändert. Der zweite Fall für $cert(t)$ repräsentiert die Situation, bei der das Gerät nicht aktiv genutzt wird. In diesem Fall werden keine Informationen über das kapazitive Display erkannt. Abbildung 8.2 zeigt, wie die Aufteilung des Vertrauenslevels aufgebaut ist.

Die Position x repräsentiert die initiale Authentifizierung. Dieser Wert wird durch die Überschreitung des Schwellenwerts bei der initialen Authentifizierung bestimmt (um wie viel der Schwellenwert überschritten wird). Mit höherer Differenz steigt die $auth_{initial}$. In

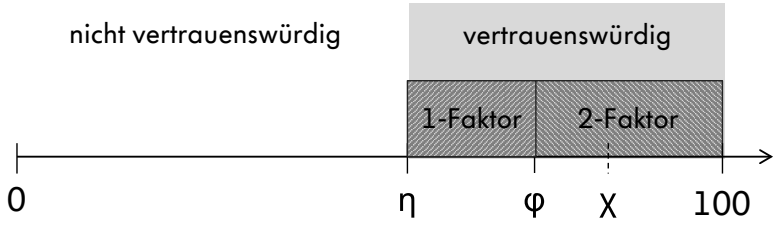


Abbildung 8.2: Skala für das Vertrauensmodell (in %)

Abbildung 8.2 werden zusätzliche Bereiche dargestellt. Der Vertrauensbereich gibt die Spanne an, in der das Gerät die Person mit einem gewissen Vertrauen erkannt hat. Wenn das Vertrauenslevel unter einen Schwellenwert η gelangt, ist das Gerät sich nicht sicher, welche Person es benutzt und wird gesperrt. Durch eine erneute initiale Authentifizierung kann der Benutzer wieder Zugriff zum System erhalten.

Eine weitere Stufe wird durch den Wert φ repräsentiert. Gerät das Vertrauen temporär unter diese Stufe, ist es nicht möglich alle Anwendungen zu benutzen. In einigen Unternehmen gibt es Richtlinien, bei denen eine Ein-Faktor-Authentifizierung (Passwort) für den Zugriff auf sicherheitskritische Systeme nicht ausreicht. Nur mit einer Zwei-Faktor-Authentifizierung (Firmenausweis mit PIN) kann der Zugriff erlangt werden. Diese Anforderung kann durch das Modell adaptiert werden. Ist das Vertrauenslevel über den Punkt φ, sind alle Anwendungen nutzbar, die auch mit einer Zwei-Faktor-Authentifizierung verwendbar sind. Zwischen φ und η wird es als eine Ein-Faktor-Authentifizierung gesehen.

8.3 Evaluierung des Konzeptes

Damit das in Abschnitt 8.2 vorgestellte System einer kontinuierlichen Authentifizierung durchgeführt werden kann, müssen nach der textabhängigen Authentifizierung weitere Authentifizierungsmethoden mit dem Smartphone durchgeführt werden. Dazu zählen die textun-

abhängige Authentifizierung und die Bewegungserkennung, die in den folgenden Abschnitten beschrieben werden. Im Anschluss werden zusätzlich Einflüsse auf das Vertrauensmodell diskutiert.

8.3.1 Textunabhängige Authentifizierung

Die textunabhängige Authentifizierung wurde, ebenso wie die textabhängige Authentifizierung, schon für die Hardwaretastaturen verwendet. Die existierenden Merkmale und die in Abschnitt 8.2.1 vorgestellten Algorithmen werden mit der gleichen Gewichtung für die Merkmale mittels der Studie **S3_Text** analysiert. Wie auch bei der textabhängigen Authentifizierung fand der statistische Klassifikator aus Abschnitt 5.2.4 für eine undefinierte Reihenfolge von Buchstaben zur Verifizierung Verwendung. Von ca. 306 Zeichen (durch Korrekturen wurden mehr Zeichen getippt) dienten die ersten 20 % (in Relation zu den gewählten Blocklängen) zum Training eines Modells einer Person. Bei Dopplungen wurde der Mittelwert gebildet. In Tabelle 8.1 wird gezeigt, wie stark der Einfluss der Blockgrößen (Anzahl an Buchstaben) auf die Fehlerraten ist.

Tabelle 8.1: Fehlerraten für eine unterschiedliche Blocklänge (in %)

Blocklänge	FAR		FRR	
	$\varnothing x$	s	$\varnothing x$	s
5	7,67	1,78	5,73	9,14
10	6,77	1,97	7,4	14,19
20	5,95	1,75	6,44	12,11
30	7,15	2,26	5,67	11,54
40	7,77	2,06	3,53	9,44
50	8,81	2,46	2,54	9,32
60	7,31	1,62	4,39	16,2
70	4,81	1,95	3,96	9,21

Für die Tests wurden die Schwellenwertkonfigurationen mit der geringsten kalkulierten EER präsentiert. Wie zu erkennen ist, werden mit größerer Blockgröße die durchschnittlichen Fehlerraten, aber auch die Standardabweichung, kleiner. Für jeden Vergleich stehen mehr Informationen zur Verfügung, als für die Entscheidung der Akzeptanz tatsächlich benötigt werden. Abweichungen der Fehler können entstehen, wenn der letzte Evaluationsblock in Relation zur Blockgröße klein ist. Bei einer Blockgröße von 60 Zeichen und einer Gesamtlänge von 306 Zeichen ist der letzte Block nur sechs Zeichen lang (sieben Blöcke, wobei der letzte nur sechs Zeichen beinhaltet und die anderen 60). Dieser kann dazu führen, dass die Verifikation nicht erfolgreich ist und sich die Standardabweichung erhöht.

Eine Herausforderung bei diesem Test ist, dass das Vorhandensein von Di- und Trigraph nicht immer gewährleistet ist. Für bessere Resultate muss ein größerer Text verwendet werden, der möglichst viele Di- und Trigraphen besitzt. Für eine weitere Verifikation sollten zusätzliche Di- und Trigraphen aufgenommen werden, da diese beiden Merkmale ebenso bei der textabhängigen Authentifizierung gut geeignet sind. Dadurch existieren von den benötigten Di- und Trigraphen alle einzelnen Merkmale, was die Fehlerraten noch weiter verringert. Einige Merkmale (Merkmale der Sensoren Gyroskop und Delta) wurden zudem in der Studie **S3_Text** nicht aufgenommen. Daher konnten diese für die textunabhängige Authentifizierung nicht verwendet werden. Wie bereits bei der textabhängigen Authentifizierung konnten sich die Fehlerraten zudem mit diesen Merkmalen verringern.

Eine Blockgröße von über 70 Zeichen wurde in diesem Test verworfen, da nicht ausreichend Evaluationsdaten vorhanden waren. In einem realen Anwendungsfall würde das bedeuten, dass über einen längeren Zeitraum eine Eingabe erfolgen muss, um eine Verifikation durchzuführen. Aber auf diesen Geräten werden meist kurze Nachrichten geschrieben. Gleichzeitig würde ein Angreifer erst nach einer sehr langen Eingabe erkannt.

S3_Text – Textunabhängige Authentifizierung

Eingabedaten:

- Gerät: Galaxy Nexus
- Passwort: vorgegebener Text (siehe Abschnitt A.1)

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: textunabhängiger kNN

Ergebnis:

- Fehlerraten sind vergleichbar mit existierenden Studien (Hardwaretastatur).
- Längere Blocklänge verringert die Fehlerraten.

8.3.2 Validierung des Frameworks mit zuvor generierten negativen Datensätzen

Die bisherigen Studien und Auswertungen dienen der Nachweisbarkeit der Funktionalität einer Authentifizierung mittels des Tippverhaltens. Wie bereits gezeigt, existieren in realen Situationen keine Datensätze von Personen mit dem gleichen Passwort. In Abschnitt 5.2.4 wurde eine Vorgehensweise beschrieben, wie ein Merkmalmodell trainiert werden kann. Dabei werden aus einer Datenbank, bei dem Personen einen längeren Text geschrieben haben, die durchschnittlichen Werte für die einzelnen Merkmale extrahiert. Der erste Teil der Studie **S3_Text** wurde hierfür verwendet. Bei den Trigraphen sind nicht alle Kombinationen vorhanden. Es existieren allein für kleine Buchstaben (ohne Umlaute) 17.576 Kombinationen. Daher wurde beim Fehlen von Werten eines Merkmals dieses nicht für die Authentifizierung

berücksichtigt. Möglichkeiten der Durchschnittsberechnung über die Entfernung sind dennoch möglich (analog Formel 7.1).

Mit dieser Vorgehensweise wurden für alle Passwörter und Personen aus der Studie **S8_EigenesPasswort** die Trainings- und Evaluationsdaten gesammelt. Aus der Studie **S3_Text** wurden dafür 50 Datensätze zum Trainieren und 100 Datensätze zum Evaluieren genutzt, wobei eine Person aus Studie **S8_EigenesPasswort** nicht mit den eigenen Daten aus Studie **S3_Text** trainiert oder evaluiert wurde. Für die Auswertung wurde die Gewichtung aus der Studie **S6_Geräte** verwendet und je nachdem, welcher Fall (Sicherheit oder Benutzerfreundlichkeit) gewünscht ist, der Schwellenwert angepasst. Mittels dieser Vorgehensweise ergaben sich für die Personen der Studie die Werte der Tabelle 8.2.

Tabelle 8.2: Fehlerraten, je nach Konfiguration (in %)

Konfiguration	FAR		FRR	
	$\varnothing x$	s	$\varnothing x$	s
FAR < 0,1 %	0,09	0,27	9,57	12,33
FAR < 0,01 %	0	0	43,98	32,39
FRR < 0,01 %	6,80	1,78	0	0
Beste Kombination	0,95	0,53	0,99	4,03

Jede Person hatte zu einem bestimmten Schwellenwert eine EER von 0 %. Daher musste analysiert werden, bei welchem Schwellenwert textunabhängig die geringsten Fehlerraten generiert werden können. In Tabelle 8.2 ist zu erkennen, dass die beste Kombination (Vergleich aller EER im Test) eine EER von kleiner als 1 % besitzt (basierend auf 10 vorher getesteten Passwörtern). Die Signifikanz dieses Ergebnisses konnte mit dem linksseitigen t-Test [BS10, S. 102f.] (α=0,05) bestätigt werden. Für ein benutzerfreundliches bzw. sicheres System wurden die Schwellenwerte angepasst. Wenn die FAR für ein sicherheitskritisches System unter 0,01 % ist, dann liegt die FRR bei 43,98 %. Bei einer

FAR unter 0,1 % wäre die FRR sogar nur 9,57 %. Wenn das System benutzerfreundlich sein soll (mit einer Fehlerrate von kleiner als 0,01 %), dann wird eine FAR von 6,8 % erreicht. Je nachdem, welches System benötigt wird, sind Einschränkungen für die FAR bzw. FRR unabdingbar.

Mit diesem System ist somit eine Möglichkeit geschaffen, die Negativbeispiele zu generieren und sie zum Training des Modells einer Person zu nutzen. Damit ist diese Problematik für Negativbeispiele bei der Verwendung des Tippverhaltens gelöst. Die Datenbank sollte für ein Produktivsystem mit mehr Daten (vor allem Di- und Trigraphen) gefüllt sein, damit die Ergebnisse noch verbessert werden können.

S8_EigenesPasswort/S3_Text – Auswertung der Generierung von Negativbeispiele

Eingabedaten:

- Gerät: Galaxy Nexus
- Passwort: beliebiges Wort mit einer Länge von 6 - 10 Zeichen

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: kNN

Ergebnis:

- Die vorgeschlagene Methode der Generierung von Negativbeispielen erzeugt niedrige Fehlerraten.
- Die Fehlerraten sind vergleichbar mit denen aus Abschnitt 7.3.1.

8.3.3 Skalierbarkeit des Tippverhaltens

Ein Verfahren sollte durch die Anzahl an Personen in einem Versuch so wenig wie möglich beeinflusst werden. Um das nachzuweisen, wurden die Daten (Szenario „Musik“, das die geringsten Fehlerraten aufwies) und die Konfiguration aus Abschnitt 7.3.1 verwendet.

Für jeden Test wurden Personen zufällig ausgewählt, sodass es eine festgelegte Personenzahl gab. Für jede Personenzahl wurden 10 verschiedene Tests mit einer zufälligen Wahl der Probanden durchgeführt. Die Ergebnisse aus dem Experiment sind in Tabelle 8.3 zusammengefasst.

Tabelle 8.3: Fehlerraten für unterschiedliche Personenzahlen im Versuch (in %)

Personenzahl	FAR		FRR	
	$\varnothing x$	s	$\varnothing x$	s
10	0,04	0,06	1,16	1,78
15	0,07	0,04	1,27	1,44
20	0,15	0,08	1,92	1,25
25	0,15	0,09	1,98	0,98
30	0,22	0,08	1,49	0,97
35	0,24	0,09	2,01	0,97
40	0,23	0,07	2,33	1,76
45	0,40	0,16	1,44	0,64
50	0,33	0,06	2,01	0,65
55	0,42	0,16	1,34	0,43
60	0,42	0,15	1,51	0,22
65	0,47	0,15	1,49	0,13
70	0,51	0,21	1,38	0,25
75	0,51	0,09	1,19	0,41
80	0,52	-	1,27	-

Auf der einen Seite ist zu erkennen, dass, je mehr Probanden sich im Test befinden, die FRR immer konstanter wird. Dabei sinkt die durchschnittliche Fehlerrate auf unter 1,50 % und die Schwankungen werden mit jeder höheren Personenzahl geringer. Auf der anderen Seite steigt die FRR leicht an.

Je mehr Personen versuchen sich zu authentifizieren, desto wahrscheinlicher ist es, dass sich zwei Versuche von unterschiedlichen Personen ähneln. Besonders bis zu der Personenzahl von 45 steigt die Fehlerrate sehr stark an, bis sie danach nur noch kleine Veränderungen erfährt.

Dieses Problem ist bereits bekannt, da es auch bei anderen biometrischen Merkmalen auftritt. In einem Bericht der NIST [Nat02] wurde gezeigt, dass die Identifizierungsgenauigkeit bei größeren Datenbeständen sinkt. Beim Fingerabdruck lag die Genauigkeit bei 93 % bei einer Datenbank von 1.000 Personen, bei der zehnfachen Anzahl waren es nur noch 90 %. Ähnliches war bei der Gesichtserkennung zu beobachten mit 83 % Genauigkeit bei der kleinen Datengröße (1.000 Personen) und 77 % bei der größeren Datenmenge (10.000 Personen). Laut der R&L AG kann dieses Problem des gewünschten Sicherheitsniveaus, speziell beim Tippverhalten, durch eine Anpassung der Textlänge gelöst werden [R&13].

S7_Szenarien – Auswertung der Skalierbarkeit

Eingabedaten:

- Passwort: *donnerwetter*
- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Kombinationen aus Merkmalen des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: kNN

Ergebnis:

- Die FRR bleibt konstant bzw. sinkt leicht bei höherer Anzahl an Personen.
- Die FAR steigt bei mehr Personen leicht an.
- Allgemein wird gezeigt, dass die Fehlerraten, die in den Tests erreicht wurden, gering sind im Vergleich zu existierenden Studien, die nur eine geringe Anzahl an Probanden hatten.

8.3.4 Bewegungserkennung des Smartphones

Die Bewegungserkennung kann genutzt werden, vor allem wenn kein anderer Authentifizierungsmechanismus möglich ist, da überprüft wird, was mit dem Gerät passiert und dadurch Rückschlüsse auf eine Person gezogen werden können. Dazu wurde die Studie **S9_Bewegungen** durchgeführt. Mit dieser Studie wurde bereits analysiert, welche Merkmale und Klassifikatoren geeignet sind (im Rahmen dieser Forschungsarbeit [Hay14]). Daraus konnten folgende Fehlerraten für die einzelnen Szenarien erreicht werden (siehe **??**). Das beste Ergebnis mit den geringsten Fehlerraten wurde mit einem neuronalen Netz und den im Abschnitt 7.2 vorgestellten Merkmalen erzeugt. Die Ergebnisse zeigen schon, dass eine Erkennung der einzelnen Aktivitäten möglich ist. Diese Informationen können für die kontinuierliche Authentifizierung verwendet werden. Für die Auswertung wurde die Teilung der Zustände „Sitzen“ und „Stehen“ vernachlässigt und zusammengefasst.

In **??** sind die einzelnen Fehlerraten zu erkennen, die für die Aktivitäten benutzerunabhängig berechnet wurden. Die FAR's liegen für alle Aktivitäten unter 0,5 % und auch die FRR's sind bei unter 2 %. Lediglich die Angriffe auf das System zeigen eine höhere FRR. Diese Versuche dienen lediglich dazu zu zeigen, welche Einflüsse Angriffe auf das System haben.

Tabelle 8.4: Fehlerraten Standardaktivitäten und Angriffsszenarien (in %)

	Aktivität	FAR	FRR
Aktivitäten	Normal-gehen-(Hand)	0,2	1,5
	Normal-gehen-(Ohr)	0,1	0,3
	Normal-gehen-(rechte-Hosentasche)	0	1,4
	Normal-gehen-(linke-Hosentasche)	0,1	1,9
	Normal-gehen-(Hemdtasche)	0,1	0,9
	Gerät-in-die-rechte-Hosentasche-stecken	0,1	2,6
	Gerät-in-Hemdtasche-stecken	0,2	1,9
	Gerät-aus-der-rechten-Hosentasche-nehmen	0,3	2,8
	Gerät-aus-der-Hemdtasche-nehmen	0,1	2,8
	Gerät-auf-den-Tisch-legen	0,2	2
	Gerät-vom-Tisch-nehmen	0,3	2,9
	Gerät-an-Person-übergeben	0,1	0,4
	Gerät-ans-Ohr-halten	0	1,1
	Gerät-vom-Ohr-entfernen	0	1,1
Angriffe	Auf-der-Stelle-gehen-(Hand)	0	5
	Auf-der-Stelle-gehen-(rechte-Hosentasche)	0	2,1
	Gerät-schütteln-(Hand)	0	10
	Gerät-schütteln-(Hemdtasche)	0	5
	Im-Kreis-drehen-(Hand)	0	0
	Gesamt	0,1	1,8

Wird bei der Klassifikation der Zustand, in dem sich das Gerät vorher befand, als Eingabeparameter mit in die Authentifizierung einbezogen, kann die Erkennung zusätzlich verbessert werden (siehe **??**).

Das Hinzufügen des Zustandes, in dem sich das Gerät vor der Aktivität befand, kann bei der Klassifikation die Fehlerraten für das ganze System verbessern. Die FRR sinkt von 1,8 % auf 1,1 % bei gleichbleibender FAR. Somit kann eine kalkulierte EER von 0,6

Tabelle 8.5: Erkennungsfehler unter Berücksichtigung des Zustandes vor der Aktivität (in %)

	Aktivität	FAR	FRR
Aktivitäten	Normal-gehen-(Hand)	0,1	0,9
	Normal-gehen-(Ohr)	0,1	0
	Normal-gehen-(rechte-Hosentasche)	0,1	1,4
	Normal-gehen-(linke-Hosentasche)	0,1	1,9
	Normal-gehen-(Hemdtasche)	0,2	0
	Gerät-in-die-rechte-Hosentasche-stecken	0,2	1,4
	Gerät-in-Hemdtasche-stecken	0,1	1,9
	Gerät-aus-der-rechten-Hosentasche-nehmen	0,1	1,2
	Gerät-aus-der-Hemdtasche-nehmen	0	0,9
	Gerät-auf-den-Tisch-legen	0	0,3
	Gerät-vom-Tisch-nehmen	0	1,2
	Gerät-an-Person-übergeben	0,1	0
	Gerät-ans-Ohr-halten	0	0,7
	Gerät-vom-Ohr-entfernen	0	1,1
Angriffe	Auf-der-Stelle-gehen-(Hand)	0,1	6,7
	Auf-der-Stelle-gehen-(rechte-Hosentasche)	0	4,2
	Gerät-schütteln-(Hand)	0	6,7
	Gerät-schütteln-(Hemdtasche)	0	6,7
	Im-Kreis-drehen-(Hand)	0	0
	Gesamt	0,1	1,1

erreicht werden. Diese Genauigkeit ermöglicht es, Bewegungen für das Re-Authentifizierungssystem zu analysieren. Für die Datenextraktion wurden nur in der Zeit der Aktivität Daten aufgenommen. In einem realen System kann es dazu kommen, dass es mehrere Aktivitäten in einem Zeitbereich gibt oder dass eine Aktivität in zwei Zeitbereichen liegt. Für diesen Fall sind noch weitere Analysen erforderlich. Das generelle Erkennen dieser Bewegungen ist, wie in **??** zu sehen, möglich.

S9_Bewegungen – Bewegungserkennung

Eingabedaten:

- Gerät: Galaxy Nexus

Studienparameter:

- Merkmale: Merkmal des kapazitiven Sensors, Bewegungs- und Lagesensors
- Klassifikator: Neuronales Netz

Ergebnis:

- Die Aktivitätserkennung erzeugt niedrige Fehlerraten.
- Die Zustandsinformationen erhöhen die Genauigkeit.

8.3.5 Einflüsse der Fehlerraten auf das Vertrauensmodell

In dem Authentifizierungsprozess existieren zwei verschiedene Angriffsszenarien. Beim ersten handelt es sich um ein gesperrtes Gerät, welches von einem Angreifer durch eine Authentifizierung mittels Passwort und dem in der Arbeit vorgestellten Tippverhalten entsperrt werden soll. Das zweite ist, dass das Gerät den Benutzer wechselt, während es entsperrt ist. In den meisten Studien handelt es sich um das erste Angriffsszenario (zur Entsperrung des Gerätes). In dieser Arbeit wurde auch das zweite Szenario der kontinuierlichen Authentifizierung angesprochen und unter Verwendung von mehreren biometrischen Methoden betrachtet. Dieser Abschnitt soll zeigen, worauf bei der Implementierung des Vertrauensmodells geachtet werden muss, damit es den gewünschten Mehrwert gegenüber keiner Re-Authentifizierung erzeugt.

Die verschiedenen biometrischen Authentifizierungen haben, wie bereits erwähnt, eine Ungenauigkeit beschrieben durch die Fehlerraten

FAR und FRR. Die unterschiedlichen Authentifizierungsmethoden besitzen folgende Fehlerraten (Tabelle 8.6):

Tabelle 8.6: Vergleich der kalkulierten EER (in %)

Methode	Kalkulierte EER	Bemerkung
Textabhängige Authentifizierung	0,75	siehe Abschnitt 7.3.1
Textunabhängige Authentifizierung	4,39	siehe Abschnitt 8.3.1
Bewegungserkennung	0,6	Der Fokus liegt direkt auf den Bereichen der Aktivität; in realen Zyklen kann eine Aktion in mehrere Zeitbereiche aufgeteilt sein bzw. mehrere Aktivitäten können gleichzeitig in einem Zeitbereich enthalten sein.
Gangerkennung	5	Bestehende Arbeiten wurden in Abschnitt 3.1.2 vorgestellt

Alle Fehlerraten sind von der zur Verfügung stehenden Datenmenge abhängig. Bei längeren Passwörtern beziehungsweise bei einer größeren Aufnahmedauer zur Erkennung von Bewegungen und Eingaben können geringere Fehlerraten in den Zeitbereichen erreicht werden. Dafür werden kurzzeitige Veränderungen nicht erkannt (Bruchteil eines Zeitbereiches), da die Überprüfung erst nach längeren Zyklen durchgeführt wird.

Für die kontinuierliche Authentifizierung sollten die Werte der Variable β (Verhältnis zwischen der Bewegungs- bzw. Gangerkennung und der textunabhängigen Authentifizierung) aus der Formel 8.2 in Abschnitt 8.2.5 anhand der aktuellen Fehlerraten der textunabhängigen Authentifizierung und Bewegungserkennung bestimmt werden, um das Gesamtsystem bezüglich der Fehlerraten zu verbessern. Die verwendete Berechnungsformel soll die grundsätzliche Funktionsweise eines Re-Authentifizierungssystems zeigen. Damit kann berechnet wer-

den, wie sicher das System in der Bestimmung ist, dass es sich um die identische Person wie bei der initialen Authentifizierung handelt. Die Ungenauigkeit der einzelnen Verfahren hat darüber hinaus entscheidenden Einfluss auf das Ergebnis und muss mit berücksichtigt werden. Abbildung 8.3 zeigt auf, welcher Einfluss auf das Vertrauensmodell durch die Fehlerraten existiert.

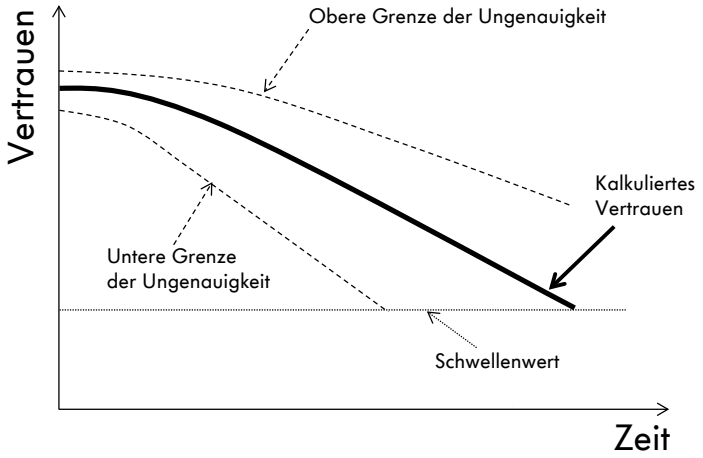


Abbildung 8.3: Beeinflussung des Vertrauens bezüglich der Ungenauigkeit der biometrischen Methoden

Bei der initialen Authentifizierung ist die Ungenauigkeit am kleinsten im Vergleich zum gesamten Authentifizierungsprozess, da die Fehlerraten geringer sind als für die anderen Methoden. Während der Benutzung des Gerätes werden die weiteren genannten biometrischen Verfahren zur Authentifizierung verwendet, die eine höhere Fehlerrate aufweisen. Die Ungenauigkeit kann dazu führen, dass eine Person fälschlicherweise als ursprünglicher Nutzer authentifiziert wird. Jedoch wird es durch die verschiedenen Methoden erschwert, den Nutzer vollständig nachzuahmen. Da teilweise nicht genügend Informationen aufgenommen werden, z. B. durch Interaktion mit dem Gerät, ohne dass die Tastatur verwendet wird und beim Lesen von E-Mails, wobei

nur gescrollt wird, muss für diese Situationen eine Lösung gefunden werden, wie die Authentifizierung durchgeführt werden soll. Sämtliche Interaktionen müssen in einem Produktivsystem zusätzlich mit betrachtet werden und dabei Informationen über die Person extrahieren. Damit das Gerät schneller bei sicherheitskritischen Anwendungen bzw. Bereichen gesperrt wird, könnte ein mehrmaliges Zurückweisen hintereinander zur sofortigen Sperrung des Gerätes führen, ohne auf das aktuelle Vertrauen zu achten.

Dieser kontinuierliche Authentifizierungsprozess bietet eine stetige Kontrolle, welche Person das Gerät zur Zeit benutzt. Dennoch müssen verschiedene Punkte verbessert bzw. betrachtet werden. Das gewollte Übergeben eines Gerätes an eine andere Person, damit diese beispielsweise eine E-Mail lesen und beantworten kann, führt in diesem Fall zur ungewollten Sperrung des Gerätes. Zudem muss betrachtet werden, wie mit der Ungenauigkeit des Systems umgegangen wird.

8.4 Bewertung der Bestandteile der kontinuierlichen Authentifizierung

Damit das Tippverhalten in einer realen Situation zur Authentifizierung genutzt werden kann, muss eine Methode entwickelt werden, die die negativen Beispiele generiert. Dieses Kapitel stellt basierend auf der textunabhängigen Authentifizierung eine entsprechende Methode vor. Im Vergleich zu existierenden Lösungen sollen dabei Fehlerraten von unter 7,0 % (siehe Abschnitt 3.1.1) erzeugt werden.

Zusätzlich muss analysiert werden, mit welchen Fehlerraten die textabhängige Authentifizierung auf der Grundlage generierter Negativbeispiele funktioniert. Dafür dürfen die Fehlerraten nicht über den 3,9 % für textabhängige Authentifizierung liegen.

Textunabhängige Authentifizierung: Die textunabhängige Authentifizierung erreichte eine kalkulierte EER von 4,38 % mit einer Blockgröße von 70 Zeichen. Aber selbst mit einer Blockgröße von mindestens 20 Zeichen wurden EER's von unter 7,0 % erreicht. Die Länge des

Blocks richtet sich danach, wie sicherheitskritisch ein System ist. Je größer die Blocklänge ist, desto kleiner sind die Fehlerraten. Dennoch sind mehr Interaktionen notwendig, was einem Angreifer ermöglicht, länger unerkannt zu bleiben.

Generierung der Negativbeispiele und allgemeine Verwendbarkeit: Die Authentifizierung mit dynamisch generierten Negativbeispielen erzeugt eine kalkulierte EER von 0,97 %. Damit wird sowohl gezeigt, dass Angreifer zurückgewiesen als auch die Personen in über 99 % der Fälle korrekt erkannt werden.

Zusätzlich wurde für die einzelnen Fehlerraten mittels Signifikanztest nachgewiesen, dass die Ergebnisse verallgemeinerbar sind. Dennoch zeigten die verschiedenen Studien unterschiedlich gute Werte bezüglich der Fehlerraten, was im Gegensatz zu anderen biometrischen Verfahren (wie z. B. dem Fingerabdruck) durch die nicht Einmaligkeit des Tippverhaltens begründet ist [TGG13].

In einem realen Szenario existieren in der Regel drei Authentifizierungsversuche, bevor das Benutzerkonto am Rechner oder die Karte bei einer Bank gesperrt werden. Der Einfluss, den die Fehlerraten bei einem Authentifizierungsversuch auf ein System mit drei Versuchen haben, wird in Tabelle 8.7 gezeigt.

Tabelle 8.7: Auswirkungen auf die Fehlerraten bei mehreren Versuchen (in %)

Konfiguration	Ein Versuch		Zwei Versuche		Drei Versuche	
	FAR	FRR	FAR	FRR	FAR	FRR
Sicherheit	0,09	9,57	0,19	0,92	0,28	0,09
FAR = 0 %	0	43,98	0	19,34	0	8,50
Beste Kombination	0,95	0,99	1,90	0,01	2,83	0,0007
Benutzerfreundlichkeit	6,80	0	13,13	0	19,04	0

Diese Fehlerraten werden anhand der folgenden Formeln berechnet. Die Variable x gibt die Anzahl der Versuche an:

$$FRR(x) = FRR^x \tag{8.3}$$

$$FAR(x) = 1 - (1 - FAR^x)^x \tag{8.4}$$

Die Wahrscheinlichkeit, dass x Mal eine Person fälschlicherweise abgelehnt wird, verringert sich mit jedem Versuch einer Person. Auf der anderen Seite können auch Personen fälschlicherweise akzeptiert werden, je mehr Versuche möglich sind. Die Auswirkungen auf die in Abschnitt 8.3.2 evaluierten Ergebnisse sind in Tabelle 8.7 zu sehen.

Es ist zu erkennen, dass die FRR sinkt, je mehr Versuche zugelassen sind. Gleichzeitig steigt die FAR, d. h. je höher die maximale Anzahl an Versuchen ist, desto kleiner muss die FAR für einen Versuch sein, damit das Verfahren weiterhin als sicher einzustufen ist. Eine FAR von 19,04 % ist zu hoch für ein sicherheitskritisches System, sie darf nicht über 1 % sein.

Damit das System für drei Versuche eine FAR von unter 0,01 % besitzt, wird eine FAR von 0,003 % bei einem Versuch benötigt. Für die FRR reicht bei gleichem Zielwert eine FAR von 4,6 % aus.

Bewegungserkennung und Konzept für die kontinuierliche Authentifizierung: Mit einer Erkennungsrate von über 99,4 % ist eine Bestimmung der Bewegungen möglich. Damit kann erkannt werden, ob das Gerät einer Person in der Tasche ist und sich bewegt oder ob das Gerät auf einem Objekt liegt. Es kann nachvollzogen werden, ob es sich noch um die gleiche Person handelt, wenn wieder mit dem Gerät interagiert wird oder ob eine neue Authentifizierung erfolgen muss. Wenn das Gerät z. B. längere Zeit auf einem Tisch liegt, kann nicht mehr vom System gesagt werden, welche Person das Gerät danach benutzt.

9 Zusammenfassung und Ausblick

In diesem Kapitel werden die wesentlichen Punkte der vorliegenden Arbeit zusammengefasst. Darüber hinaus erfolgt eine Beschreibung von noch existierenden Limitationen und dem Nutzen dieser Arbeit. Der letzte Abschnitt zeigt Möglichkeiten der Erweiterung des Authentifizierungssystems auf.

9.1 Ergebnisse

In dieser Arbeit wurde analysiert, wie das kapazitive Display und die Beschleunigungssensoren zur Authentifizierung mittels des Tippverhaltens verwendet werden können. Dafür wurden unterschiedliche Prozesse zur Verringerung der Fehlerraten der Erkennung entwickelt und mit verschiedenen Studien verifiziert. Im Folgenden sind die Hauptaspekte dieser Arbeit zusammenfassend aufgelistet:

Funktionalität des Touchscreens: Erweiterungen des biometrischen Prozesses der Authentifizierung mittels des Tippverhaltens wurden in dieser Arbeit beschrieben und durch verschiedene Studien nachgewiesen. Es konnte gezeigt werden, dass das Tippverhalten auch bei Nutzung einer anderen Technologie – eines Smartphones mit kapazitiven Display – durchgeführt werden kann. Bei den verwendeten Geräten wurde ausschließlich eine Softwaretastatur mit kapazitivem Display genutzt. Zudem wurden weitere Sensoren hinzugefügt, die bei der Authentifizierung verwendet werden konnten (das Accelerometer und das Gyroskop, siehe Abschnitt 5.2.1).

Die Datenströme aus den Sensoren wurden aufgenommen, in der Vorverarbeitung gefiltert und die Multitouch-Events ausgewertet. Aus den Rohdaten konnten neben den Standardmerkmalen (Verweildauer,

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6_9

Di- und Trigraph) auch weitere Merkmale von den verschiedenen angesprochenen Sensoren extrahiert werden (siehe Abschnitt 5.2.3).

Initial wurden verschiedene Klassifikatoren auf ihre Nutzbarkeit getestet. Anhand von Bearbeitungszeit und entstehenden Fehlerraten wurde auf eine Erweiterung des k nächsten Nachbarn (kNN) zurückgegriffen, geclustert anhand des euklidischen Abstandes. Zusätzlich zeigt die Arbeit in Abschnitt 5.2.4 eine Gewichtung der verschiedenen Merkmale in Abhängigkeit von ihrer Fehlergenauigkeit auf. Mit Einführung eines Schwellenwertmodells verbessert sich zusätzlich das Ergebnis einer Fusion von Merkmalen.

Somit wurden die Fehlerraten (kleiner gleich 1 %) im Vergleich zu den Studien mit einer Hardwaretastatur verbessert. Aus diesem Grund stellt das Tippverhalten eine Alternativmöglichkeit zu anderen biometrischen Verfahren zur Authentifizierung dar. Das Tippverhalten kann damit als dritter Faktor, neben dem BESITZ- und WISSENS-Faktor, zur 3-Faktor-Authentifizierung verwendet oder als Alternative zu einer vertrauenswürdigen 2-Faktor-Authentifizierung (BESITZ und WISSEN) angesehen werden.

Funktionsfähiges System: Eine Klassifikation ist nur möglich, wenn positive und negative Authentifizierungsversuche existieren. Dadurch, dass ein Passwort nur dem eigentlichen Nutzer bekannt sein soll, muss eine Methode zur Generierung von Negativbeispielen, die zu einer Ablehnung der Person führen sollen, entwickelt werden. Ein solches Verfahren wurde zur Lösung dieses Problems anhand von Merkmalen von einer textunabhängigen Authentifizierung erstellt und deren Funktionsfähigkeit nachgewiesen.

Darüber hinaus muss das Modell zyklisch angepasst werden, da in dieser Arbeit in Abschnitt 5.3.5 nachgewiesen wurde, dass sich das Tippverhalten im Laufe der Verwendung durch das Lernverhalten einer Person verändert. Dadurch wird gewährleistet, dass sich die Person auch nach längerer Zeit immer noch authentifizieren kann.

Bei dem nächsten in dieser Arbeit nachgewiesenen Aspekt handelt es sich um eine Authentifizierung, die geräteunabhängig ist (siehe

Abschnitt 6.3). Durch die Qualität der eingebauten Sensoren entstehen unterschiedliche Fehlerraten, die bei allen verwendeten Geräten akzeptabel sind.

Nutzung in verschiedenen Szenarien: Bisherige Studien basieren nur auf einem Szenario (Texteingabe während des Sitzens). Einschränkungen auf dieses Szenario limitieren den Nutzungsbereich. In dieser Arbeit wurde daher der Einfluss verschiedener Szenarien (u. a. Gehen oder die Verwendung der nicht-dominanten Hand) auf das Tippverhalten analysiert. Resultat ist die Erkennung einer Veränderung des Tippverhaltens, wodurch dieses nicht mit ausreichender Qualität zur Verifizierung der Person geeignet ist. Daher wurden Szenarienerkennungs- und Transformationsalgorithmen entwickelt, die dem entgegenwirken. Teilweise ist ein separates Enrolment für die Szenarien (z. B. bei Verwendung der nicht-dominanten Hand) notwendig (siehe Abschnitt 7.3), damit die Fehlerraten unter 5 % bleiben.

Kontinuierliche Authentifizierung: Ein weiterer wichtiger Aspekt ist das Modell der kontinuierlichen Authentifizierung, das in Abschnitt 8.2 vorgestellt und in Abschnitt 8.3 analysiert wurde. Dieses Modell stellt eine Problemlösung dar, wie der Nutzer auch nach dem Entsperren des Gerätes überprüft werden kann. Es werden mehrere verschiedene biometrische Modalitäten verwendet (u. a. textunabhängige Authentifizierung oder Bewegungserkennung). Somit kann zu jedem Zeitpunkt festgestellt werden, ob es sich noch um den eigentlichen Nutzer handelt oder ob das Gerät gesperrt werden muss.

9.2 Limitation

Studien unterliegen im Allgemeinen verschiedenen Limitationen. Durch mehrere Studien wurde versucht, diese zu minimieren. Die noch existierenden Limitationen werden im Folgenden genannt und beschrieben.

Jede Studie wird für sich in einer kontrollierten Umwelt durchgeführt, weil nicht alle äußeren Einflüsse eliminiert werden können. So

kann das Experiment durchgeführt werden, bei dem die Person bereits im Vorfeld gestresst war oder beim Experiment abgelenkt ist. Das verändert das Tipperhalten, da z. B. Frustration bei Fehleingaben die Druckstärke verstärkt [GTN+99].

Mit den verschiedenen Studien wurde gezeigt, wie diese äußeren Einflüsse zu relativieren sind. Entgegen der meisten Experimente (in Abschnitt 3.1.1) sollten die einzelnen Szenarien realitätsgetreuer dargestellt werden, d. h. nicht nur klinische Studien im Sitzen. Wie in Abbildung 9.1 gezeigt, ist das ein kleiner Teil von allen möglichen Szenarien. Es kann nicht jedes Szenario evaluiert werden bzw. zu einer Authentifizierung genutzt werden.

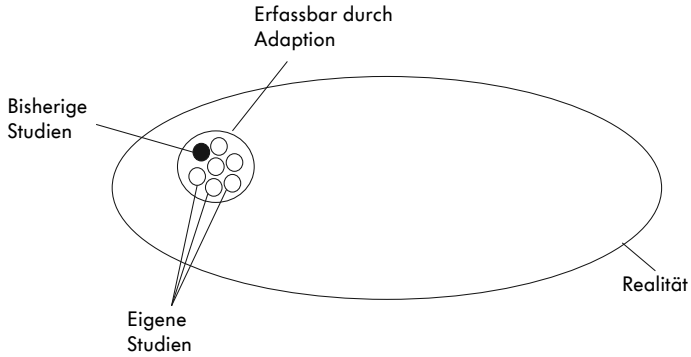


Abbildung 9.1: Übersicht der analysierten Gebiets beim Tippverhalten

Darüber hinaus existieren Einschränkungen bezüglich der Allgemeingültigkeit der zu verwendenden Geräte und Betriebssysteme. Es wurden diverse Geräte unterschiedlicher Hersteller getestet (u. a. HTC oder Samsung). Diese Geräte verwenden dennoch das gleiche Betriebssystem (Android OS). Gleichzeitig hatten Benutzer, die ein Android Smartphone besitzen, eine kürzere Anlernphase während der Studie, somit war die Veränderung durch das Lernverhalten kleiner als bei anderen Probanden. Zudem ist nicht bekannt, welchen Einfluss andere Betriebssysteme auf das Tippverhalten haben, weil z. B. nicht auf

alle Daten zugegriffen werden kann bzw. die Sensoren nicht genutzt werden können.

Zudem muss eine weitere Betrachtung erfolgen, welche Auswirkungen der geschriebene Text auf die Probanden hat. Die freie Wahl eines Passwortes wurde den Probanden nur in einer Studie eingeräumt. Ungewohntes Tippen von verschiedenen Wörtern wurde nicht berücksichtigt.

Ein weiterer Aspekt ist die Auswahl der Probanden. Durch den IT-nahen Untersuchungsbereich wurde nur eine geringe Anzahl an weiblichen Testpersonen befragt. Gleichzeitig waren Alter und Bildungsniveau nicht ausgeglichen. Andere Bereiche und Altersklassen können andere Fehlerraten erzeugen.

Die Klassifikation erfolgt auf Grundlage nur einer Verifikation, d. h. es wurden alle Datensätze gegenüber einem Modell einer Person überprüft. Das ist möglich, da sich im Bereich des Smartphones immer nur eine vorher definierte Anzahl an Nutzern anmelden darf. Die Ergebnisse sind nicht im Bereich der Identifikation verallgemeinerbar, da die Fehlerraten des Tippverhaltens bei dieser Art von Klassifikation im Vergleich zur Verifikation höher ausfallen.

Es ist zudem zu überprüfen, ob eine passwortunabhängige Authentifizierung verwendet werden sollte. Bei der Entwendung eines Datensatzes kann das Tippverhalten angelernt werden und es ist möglich, sich als eine andere Person auszugeben, da es sich um das generelle Schreibverhalten der Person handelt (unter Vernachlässigung des Lernverhaltens einer Person). Passwörter stellen dagegen nur einen kleinen Auszug des Tippverhaltens dar und können passwortspezifisch angepasst werden (z. B. bewusste Pausen zwischen verschiedenen Zeichen). Wird der Datenstrom kompromittiert, kann bei einer Passwortänderung ein neuer Rhythmus verwendet werden. Dieser kann vom alten Passwort nicht adaptiert werden.

Dieser Aspekt ist auch in dem Bereich des Datenschutzes von Bedeutung. Bevor dieses Verfahren kommerziell eingesetzt werden kann, müssen die Probleme bezüglich des Datenschutzes (u. a. das Speichern von biometrischen Daten) gelöst werden. Die momentane Implementierung entspricht zudem einem Keylogger, der alle Daten speichert.

Somit ist die Aufnahme von sensitiven Daten möglich. Der letzte Umstand betrifft lediglich die textunabhängige Authentifizierung. Sofern eine textabhängige Authentifizierung nur zum Entsperren verwendet wird, müssen nur die klassischen Datenschutzprobleme gelöst werden (z. B. Speicherung von personenbezogenen Daten).

9.3 Nutzen

Das in dieser Arbeit entwickelte Authentifizierungsverfahren bewirkt, dass die Daten auf dem Smartphone besser gesichert werden können. Insbesondere Firmen, bei denen die Mitarbeiter über das Smartphone auf sensible Daten zugreifen wollen, haben mit diesem Verfahren die Möglichkeit, dies gesichert zu tun, da die Daten nicht nur durch ein einfaches Passwort geschützt sind.

Die vorgestellte Authentifizierung mittels des Tippverhaltens kann sowohl als 1-Faktor und 2-Faktor (im Zusammenhang mit einem Passwort) als auch 3-Faktor-Authentifizierung (im Zusammenhang mit einem Passwort und einem BESITZ-Faktor) verwendet werden. In allen Fällen wird die Sicherheit durch diesen Faktor erhöht. Damit kann der gezielte Diebstahl, um an die Daten des Gerätes zu gelangen, zurückgehen. Der Berechnungsaufwand dauert zu lange im Vergleich zum Nutzen. Besonders in Bereichen, bei denen ein BESITZ-Faktor verwendet wird, kann diese Methode als Alternativmethode verwendet werden, da ein BESITZ-Faktor vergessen, verloren oder gestohlen werden kann. Gleichzeitig muss sich der Anwender nicht unbedingt ein Passwort merken. Anstatt eines festgelegten Passwortes kann jedes beliebige Wort eingegeben werden („Bitte geben Sie XXXX ein.“). In diesem Fall sind nur die biometrischen Merkmale von Bedeutung.

Der Nutzen der vorliegenden Dissertation ist nicht nur von praktischer Natur, sondern liegt auch im Bereich der Wissenschaft. In dieser Arbeit wurden neue Merkmale für das Tippverhalten auf Geräten mit kapazitivem Display vorgestellt. Diese Merkmale können für weitere Authentifizierungsverfahren (z. B. die Unterschriftenerkennung mittels Wischmuster oder eines speziellen Stiftes) verwendet werden. Das

Verfahren wurde für verschiedene Geräte und Szenarien getestet und benötigte den wissenschaftlichen Nachweis, dass das Verfahren für unterschiedliche Bereiche verwendbar ist.

Die Möglichkeit der Generierung von Negativbeispielen für eine Klassifikation kann allgemein auf alle Authentifizierungen mittels des Tippverhaltens, auch auf die mit Hardwaretasten, ausgeweitet werden. Zudem wurde mit dem Konzept der Re-Authentifizierung ein System vorgestellt, das es ermöglicht, permanent eine Person zu authentifizieren. Die Fehlerraten für das textabhängige und textunabhängige Tippverhalten wurden auf eine andere Technologie adaptiert und die Fehlerraten für diese Systeme verringern sich.

9.4 Ausblick

Neben den in dieser Arbeit gezeigten Verbesserungen sind noch weitere Verfahren bzw. Schritte möglich, die auf dem Gebiet der Authentifizierung verwendet und in Zukunft umgesetzt werden können. Zu diesen Aspekten gehören die Folgenden:

Datenschutzkonforme biometrische Authentifizierung: Wie in Abschnitt 9.2 beschrieben, sind die Punkte bezüglich des Datenschutzes (u. a. Privatsphäre) mit dieser Arbeit nicht vollständig geklärt. Eine Verschlüsselung der Daten und der Übertragung inklusive eines Hashwertes der Merkmale, sodass nicht auf die Eingabe zurück geschlossen werden kann, können für dieses Verfahren entwickelt werden. Gleichzeitig kann gezeigt werden, ob der Prozess für die Authentifizierung eines Benutzers auf einem Server durchgeführt werden kann. Einen Ansatz bietet das in der Publikation [TPS13] vorgestellte Markov Modell, das in der Lage ist, die Anzahl an virtuellen Maschinen und die Regeln für das Warten von Prozessen zu berechnen, die für eine bestimmte Anzahl an Benutzern notwendig sind.

Angriffe auf das System: Die Sicherheitsanalyse in der Arbeit beruht auf dem Vergleich von unterschiedlichen Benutzern. Gezielte Angriffe auf das System, bei denen versucht wird, das Schreibverhal-

ten nachzuahmen, könnten für eine bessere Sicherheitsbetrachtung durchgeführt werden.

Des Weiteren gibt es eine Vielzahl von Möglichkeiten, die genutzt werden können, um die geringen Fehlerraten weiter zu optimieren. Dazu zählen folgende Punkte, die noch erforscht werden könnten:

Fusionierung mit anderen Modalitäten: Smartphones haben weitere noch nicht einbezogene Sensoren, die zusätzliche Daten extrahieren und mit den bestehenden fusionieren können. Dazu gehören u. a. der in Abschnitt 2.4.2 angesprochene visuelle Sensor und der Audiosensor. Hierfür wurden bereits einige Studien durchgeführt, die die Qualität dieser Methoden beschreiben [RJ03, AM11, SYY+11].

Alternative Klassifikationsverfahren: Durch Verwendung einer Server-Client-Infrastruktur, bei denen die biometrischen Daten auf einen Server übertragen und das dort ausgewertete Ergebnis zurück auf das Smartphone transferiert werden, können weitere Klassifikatoren benutzt werden. Diese sind nur nutzbar, wenn das Smartphone mit dem Server verbunden ist. Damit minimieren sich die Fehlerraten. Zudem könnte eine Klassifikation der Klassifizierung (Ergebnis einer Klassifikation wieder klassifizieren) erfolgen, um die Ergebnisse zu verbessern.

Wischmuster: Die Nutzung eines Wischmusters wurde nur am Rande dieser Arbeit adressiert. Eine weitere Adaptierung der Unterschriftenerkennung kann verwendet werden, weil noch nicht alle Merkmale vom kapazitiven Display und der sonstigen Sensoren verwendet wurden.

Übertragung des Konzeptes für die kontinuierliche Überprüfung: Das in dieser Arbeit vorgestellte theoretische Konzept einer kontinuierlichen Überprüfung für einen Nutzer des Smartphones muss in einem realen Szenario nachgewiesen und die entsprechende Formel für das Vertrauensmodell überprüft werden. Zudem sind weitere Informationen für die Authentifizierung denkbar, wenn z. B. beim

Lesen gescrollt wird bzw. allgemeines Nutzerverhalten. Gleichzeitig können die Bewegungsdaten für die textabhängige und -unabhängige Authentifizierung nicht nur bei Berührung des Gerätes, sondern während der ganzen Eingabe als Datenfluss aufgenommen und analysiert werden.

Wortwahl & Grammatik für die textabhängige Authentifizierung: Es kann nicht nur analysiert werden, wie eine Person tippt, sondern zusätzlich kann eine Erkennung über die Wortwahl geschehen, analog zum Studiengebiet der Natural Language Processing (NLP).

Erweiterung des Konzeptes auf andere Geräte: Diese Technologie kann des Weiteren auf andere Geräte übertragen werden. Nicht nur das Smartphone oder Tablet besitzt ein Touchscreen, auch in Produktionsgeräten oder in der Smart Grid Umgebung [KHLF10, ME10] kann das Verfahren zur Authentifizierung adaptiert werden.

Zusammenfassend zeigt diese Arbeit, dass durch einen geringen, noch zu betreibenden Aufwand das Authentifizierungsverfahren mittels des Tippverhaltens auf einem Smartphone mit kapazitivem Display verwendbar ist, wobei darüber hinaus noch viel Erweiterungspotential existiert.

A Anhang

A.1 Experiment-Text

Verwendeter Text für Studie **S3_Text**:

> eine schöne legende ist mittlerweile der standort des koloss von rhodos. seit dem späten mittelalter ist man bei künstlern der festen meinung, dass dieser breitbeinig über der hafeneinfahrt von rhodos gestanden haben muss. dies ist eine reine spekulation, die sich aber sehr beeindruckend darstellen lässt. (306 Zeichen, 45 Wörter) Quelle: [Bot12]

A.2 Eigene Studien im Überblick

Studien, bei denen eine Interaktion mit dem kapazitiven Display erfolgte:

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6

Tabelle A.1: Überblick über die verschiedenen Studien

Studie	Test-personen	Wieder-holungen pro Person	Daten		Passwort	Gerät	Eingabe-art
			Kapazitives Display	Bewegungs-sensor			
S1_Merkmale	18	10	Alle	Keine	hello world	Galaxy Nexus	Tippen
S2_PIN Passwort	35	11	Alle	Keine	mein telefon, 1864559	HTC Desire	Tippen
S3_Text	152	10	Alle	Nur Gyroskop	koloss von rhodos, freier Text	Galaxy Nexus	Tippen
S4_Lernen	20	400	Alle	Alle	donnerwetter	Galaxy Nexus	Tippen
S5_Swype	16 und 42	10	Alle außer Zeitin-formationen	Nur Gyroskop	wert, test, QWERT, passwort, monogamie	Samsung Galaxy S II	Swypen
S6_Geräte	82	20	Alle	Alle	treter, sommer, module	Galaxy Nexus, Samsung Galaxy S II und Samsung Galaxy S III	Tippen
S7_Szenarien	80	20	Alle	Alle	anna, sommer, donnerwetter	Galaxy Nexus	Tippen
S8_Eigenes Passwort	40	40	Alle	Alle	Kein vordefiniertes Passwort	Galaxy Nexus	Tippen

A.3 Durchgeführte Bewegungen

Die Tabelle A.2 zeigt die durchgeführten Aktivitäten auf [Hay14]:

Tabelle A.2: Liste der aufgenommenen Aktivitäten

Aktivität	Kurzbeschreibung
Smartphone in die Hosen-/ Hemdtasche stecken	Das Smartphone wird in die jeweilige Tasche gesteckt. Sowohl im Sitzen als auch im Stehen durchgeführt.
Smartphone aus der Hosen-/Hemdtasche entfernen	Das Smartphone wird aus der jeweiligen Tasche genommen. Sowohl im Sitzen als auch im Stehen durchgeführt.
Smartphone auf den Tisch legen	Das Smartphone wird auf den Tisch gelegt. Sowohl im Sitzen als auch im Stehen durchgeführt.
Smartphone vom Tisch nehmen	Das Smartphone wird vom Tisch genommen. Sowohl im Sitzen als auch im Stehen durchgeführt.
Smartphone ans Ohr halten	Das Smartphone wird ans Ohr gehalten, um ein Telefonat zu simulieren. Sowohl im Sitzen als auch im Stehen durchgeführt.
Smartphone vom Ohr entfernen	Das Smartphone wird vom Ohr entfernt, um den Abbruch eines Telefonats zu simulieren. Sowohl im Sitzen als auch im Stehen durchgeführt.
Smartphone an Person übergeben	Das Smartphone an eine andere Person übergeben.
Smartphone von Person zurücknehmen	Das Smartphone wird von einer anderen Person zurückgenommen.
Langsam/Normal/Schnell gehen	Der Proband geht in jeweiliger Geschwindigkeit.
Treppe hoch-/ heruntergehen	Der Proband geht die Treppe hoch/runter.
Fahrstuhl hoch-/ herunterfahren	Der Proband fährt mit dem Fahrstuhl hoch/runter.
Im Kreis drehen	Der Proband dreht sich zur Simulation einer Fortbewegung um 360 Grad.
Smartphone kreisen	Der Proband kreist das Gerät zur Simulation einer Fortbewegung langsam mit der Hand.
Auf der Stelle gehen	Der Proband geht zur Simulation eines Ganges auf der Stelle.

A.4 Anonyme Identifikator

In Zusammenarbeit mit Florian Arndt [Arn12] abgeleitet von Augustin [Aug11]:

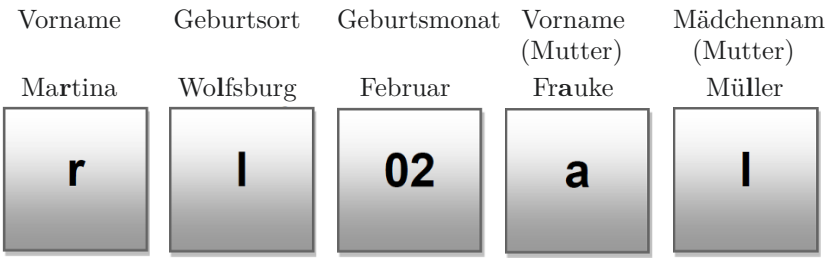
Beschreibung des anonymen Codes Um die Studie anonymisiert zu halten und Sie als Proband dennoch wiederzuerkennen, falls Sie beispielsweise an einer von unseren weiteren Studien teilnehmen, benötigen wir einen Identifier von Ihnen, mit denen wir Sie eindeutig identifizieren können.

Aus diesem Grund möchten wir Sie bitten, folgende Buchstaben und Zahlen hintereinander zu Beginn des Experiments einzugeben:

- **3. Buchstabe Ihres Vornamens**
- **3. Buchstabe Ihres Geburtsortes**
- **Ihren Geburtsmonat in Zwei-Ziffer-Schreibweise**
- **3. Buchstabe des Vornamens Ihrer Mutter**
- **3. Buchstabe des Mädchennamens Ihrer Mutter**

Beispiel: Als Beispiel nehmen wir Martina, die im Februar in Wolfsburg geboren wurde und deren Mutter Frauke heißt und den Mädchennamen Müller besitzt.

Testperson: Ma**r**tina
Geboren in: Februar (**02**) in Wo**l**fsburg
Mutter: Fr**a**uke
Mädchenname: M**ü**ller (Achtung: Umlaute werden als **ein** Zeichen gezählt!)



Resultierender Code: **rl02al**
Bei Fragen wenden Sie sich bitte an den Versuchsleiter.

A.5 Deskriptive Daten

Fragebogen für die Erfassung der deskriptiven Daten:

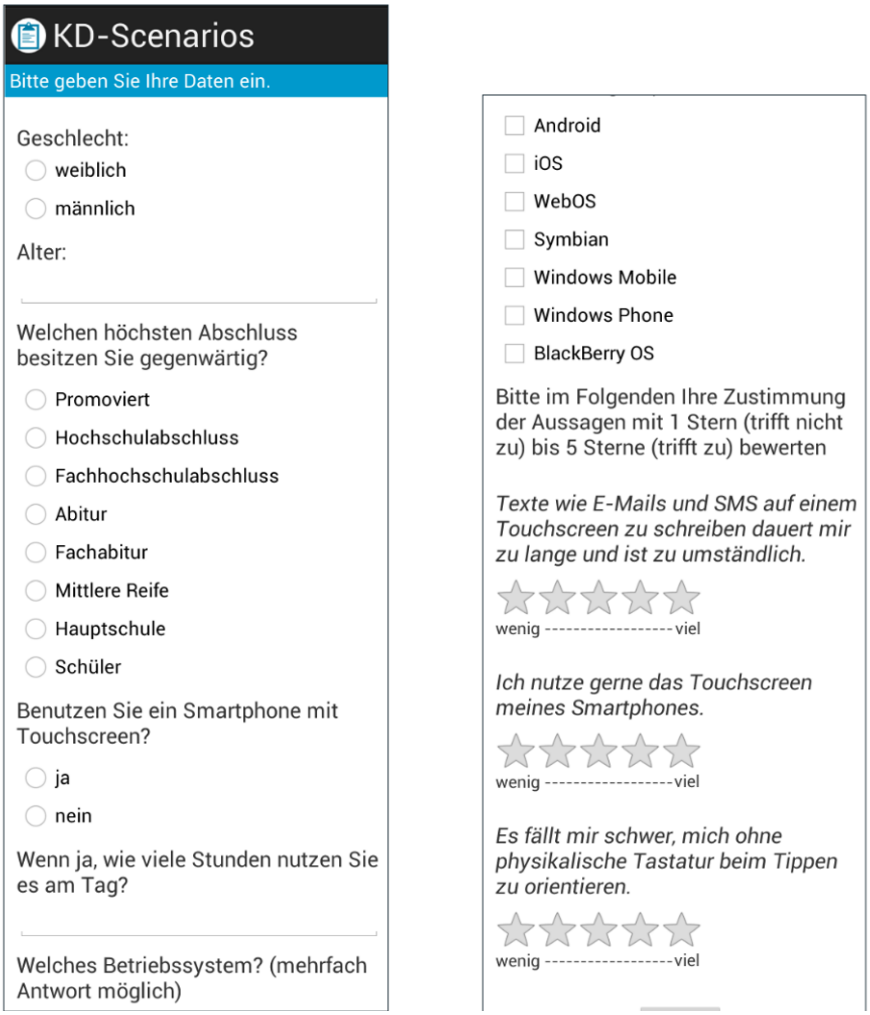


Abbildung A.1: Fragebogen

A.6 Standardkonfigurationen für Weka-Klassifikation

Im Folgenden werden die Standardkonfigurationen von den Weka-Klassifikatoren neuronales Netz, SVM, IBk und NaiveBayes, die für die Klassifikation verwendet wurden, beschrieben.

Neuronales Netz NAME:

- weka.classifiers.functions.MultilayerPerceptron

OPTIONS:

- GUI: False
- autoBuild: True
- debug: False
- decay: False
- hiddenLayers: a
- learningRate: 0.3
- momentum: 0.2
- nominalToBinaryFilter: True
- normalizeAttributes: True
- normalizeNumericClass: True
- reset: True
- seed: 0
- trainingTime: 500
- validationSetSize: 0
- validationThreshold: 20

RBFN NAME:

- weka.classifiers.functions.RBFNetwork

OPTIONS:

- clusteringSeed: 1
- debug: False
- maxIts: -1
- minStdDev: 0.1
- numClusters: 2
- ridge: 1.0E-8

SVM NAME:

- weka.classifiers.functions.LibSVM

OPTIONS:

- SVMType: C-SVC(classification)
- cacheSize: 40.0
- coef0: 0.0
- cost: 1.0
- debug: False
- degree: 3
- doNotReplaceMissingValues: False
- eps: 0.0010

- gamma: 0.0
- kernelType: radial basis function: exp(-gamma*|u-v|^2)
- loss: 0.1
- normalize: False
- nu: 0.5
- probabilityEstimates: False
- shrinking: True
- weights:

IBk NAME:

- weka.classifiers.lazy.IBk

OPTIONS:

- KNN: 1
- crossValidate: False
- debug: False
- distanceWeighting: No distance weighting
- meanSquared: False
- nearestNeighbourSearchAlgorithm: LinearNNSearch -A "weka.core.EuclideanDistance -R first last"
- windowSize: 0

NaiveBayes NAME:

- weka.classifiers.bayes.NaiveBayes

OPTIONS:

- debug: False
- displayModelInOldFormat: False
- useKernelEstimator: False
- useSupervisedDiscretization: False

A.7 Merkmale für die gerätespezifische Authentifizierung

Tabelle A.3: Unterschiedliche FAR und FRR (in %) der einzelnen Merkmale in Relation zu dem verwendeten Passwort und Geräte

Merkmale		Galaxy Nexus				Samsung Galaxy S II				Samsung Galaxy S III			
		FAR		FRR		FAR		FRR		FAR		FRR	
		$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s
Verweildauer	*treter*	17,2	0,3	15,8	22,2	14,3	0,3	16,7	19,7	18,6	0,3	11,8	17,2
	module	15,6	0,3	14,8	19,6	18,9	0,3	11,8	17,8	15,6	0,3	12,8	18,3
	sommer	14,1	0,3	14,2	19,2	12,8	0,3	17,5	21,2	14,1	0,3	15,7	18,6
Digraph	*treter*	21,9	0,4	25,0	28,1	16,0	0,5	26,6	31,1	20,3	0,3	16,3	22,5
	module	15,7	0,4	21,1	25,4	17,4	0,2	12,7	14,6	18,6	0,3	8,5	16,6
	sommer	14,1	0,3	14,3	17,3	17,4	0,3	14,8	17,3	17,1	0,2	11,9	15,8
Trigraph	*treter*	17,5	0,5	35,0	31,9	25,3	0,4	21,1	26,3	17,3	0,4	24,3	26,7
	module	32,5	0,3	11,1	17,6	23,7	0,2	14,1	15,4	23,2	0,3	10,9	18,4
	sommer	15,7	0,3	18,6	21,2	26,7	0,2	11,0	15,2	17,2	0,3	16,5	17,6
Druckstärke	*treter*	15,6	0,3	14,8	21,3	33,0	0,2	15,1	15,0	-	-	-	-
	module	12,5	0,2	10,9	15,9	22,1	0,3	15,5	17,9	-	-	-	-
	sommer	12,4	0,2	9,0	13,3	23,6	0,2	11,8	15,2	-	-	-	-
Druckstärke2	*treter*	23,5	0,3	25,3	21,3	38,0	0,3	29,1	21,6	-	-	-	-
	module	28,1	0,3	23,8	17,0	37,8	0,3	20,0	17,0	-	-	-	-
	sommer	21,9	0,3	26,0	22,7	22,4	0,4	33,6	23,5	-	-	-	-
Auflagefläche	*treter*	26,4	0,3	17,6	18,2	14,3	0,4	15,1	22,6	20,3	0,3	16,4	18,2
	module	18,7	0,3	17,3	16,7	11,2	0,3	14,1	20,9	21,7	0,2	11,9	13,4
	sommer	23,3	0,3	11,7	16,6	9,6	0,4	14,7	22,8	20,2	0,2	11,6	15,1
Auflagefläche2	*treter*	29,5	0,3	17,1	19,4	31,6	0,3	20,6	20,9	31,1	0,3	19,9	19,2
	module	20,3	0,2	18,6	15,7	36,2	0,2	18,9	15,0	25,0	0,3	24,0	19,9
	sommer	21,7	0,3	13,2	16,7	30,0	0,3	20,0	18,8	20,4	0,3	26,3	18,2
x-Koordinaten	*treter*	23,3	0,2	15,9	15,3	25,2	0,2	15,1	14,6	24,8	0,2	14,2	13,5
	module	17,2	0,4	19,0	23,0	16,0	0,4	25,7	26,0	17,2	0,3	20,8	22,3
	sommer	17,2	0,3	19,9	20,9	22,2	0,4	19,9	22,6	20,4	0,4	25,8	25,7
x2-Koordinaten	*treter*	20,3	0,2	17,2	16,1	25,2	0,2	12,3	13,9	18,7	0,2	18,3	15,2
	module	20,2	0,2	11,9	13,4	22,1	0,3	15,9	19,5	20,2	0,2	10,7	14,2
	sommer	20,2	0,3	14,7	16,5	22,1	0,3	13,9	16,4	18,8	0,3	18,8	20,5
y-Koordinaten	*treter*	23,4	0,3	22,0	22,6	22,2	0,3	19,3	17,2	27,9	0,3	13,0	16,3
	module	17,3	0,4	24,2	23,3	17,5	0,3	21,4	20,3	18,8	0,3	23,4	18,8
	sommer	23,4	0,3	19,1	18,1	22,3	0,4	25,7	23,1	23,4	0,3	21,1	20,3
y2-Koordinaten	*treter*	20,4	0,4	24,8	23,3	26,8	0,2	16,6	15,6	23,3	0,3	16,1	18,0
	module	24,8	0,2	15,0	15,9	20,6	0,2	16,0	15,0	15,7	0,3	19,2	17,1
	sommer	21,8	0,3	18,6	17,6	26,9	0,2	18,4	15,9	20,3	0,3	20,3	17,5

Merkmale		Galaxy Nexus				Samsung Galaxy S II				Samsung Galaxy S III			
		FAR		FRR		FAR		FRR		FAR		FRR	
		$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s
	treter	16,1	0,6	44,4	40,6	30,5	0,4	50,6	24,5	45,2	0,3	34,9	21,0
Pitch	*module*	26,8	0,5	39,0	33,7	39,7	0,3	41,2	21,8	42,2	0,4	40,6	25,8
	sommer	23,8	0,5	49,4	34,6	41,2	0,4	39,6	25,2	42,1	0,4	36,4	26,5
	treter	11,6	0,7	54,5	43,6	44,2	0,4	27,0	23,0	60,4	0,4	28,9	26,6
Roll	*module*	29,8	0,5	38,2	30,4	45,8	0,4	30,9	22,9	52,8	0,4	34,5	27,5
	sommer	36,1	0,5	43,4	31,2	48,8	0,3	23,3	21,0	31,6	0,4	54,1	25,4
	treter	28,2	0,5	33,4	32,6	69,1	0,3	21,8	16,7	43,7	0,3	41,5	22,5
Incli-nation	*module*	34,4	0,4	33,9	28,0	44,4	0,3	42,6	21,9	33,1	0,4	53,4	25,3
	sommer	40,5	0,4	33,4	23,7	18,3	0,3	72,3	19,6	45,2	0,3	39,8	20,3
	treter	42,1	0,3	39,2	22,6	29,0	0,4	58,8	24,4	34,5	0,3	41,5	22,4
GyroX	*module*	48,2	0,3	30,4	21,1	53,6	0,3	31,0	20,3	30,0	0,4	48,5	23,9
	sommer	40,6	0,3	38,8	22,0	53,7	0,3	34,8	21,4	22,4	0,4	53,5	24,0
	treter	34,7	0,4	53,1	24,1	36,6	0,4	44,2	23,8	23,7	0,4	42,9	25,4
GyroY	*module*	46,8	0,3	40,7	21,1	53,7	0,3	34,3	18,4	32,9	0,4	37,3	26,5
	sommer	25,6	0,4	62,4	25,5	58,3	0,3	29,5	21,7	35,9	0,3	35,5	22,3
	treter	37,6	0,4	44,8	24,8	55,2	0,3	30,0	20,0	25,3	0,3	46,8	22,2
GyroZ	*module*	37,6	0,4	46,0	27,6	30,6	0,3	57,2	22,0	29,8	0,3	37,2	21,3
	sommer	36,1	0,4	45,2	25,5	55,1	0,4	27,5	27,4	37,4	0,3	30,7	21,0
	treter	22,5	0,4	61,3	27,8	44,4	0,5	42,3	29,1	14,9	0,4	69,9	27,5
Delta0	*module*	25,5	0,4	56,8	23,3	18,2	0,4	63,1	24,9	20,9	0,5	58,9	29,4
	sommer	31,6	0,4	52,8	26,9	47,4	0,4	34,3	28,0	26,9	0,4	51,4	26,4
	treter	42,3	0,4	47,2	29,0	27,4	0,4	54,4	27,1	25,5	0,5	58,9	30,2
Delta1	*module*	37,7	0,4	49,8	28,0	35,1	0,4	48,8	25,0	19,3	0,4	57,5	27,0
	sommer	30,2	0,4	60,4	27,5	39,8	0,4	45,6	26,5	17,9	0,4	64,1	26,8
	treter	37,6	0,4	46,5	25,5	41,3	0,4	45,2	28,1	30,0	0,5	51,5	30,4
Delta2	*module*	40,6	0,4	42,2	28,6	39,8	0,4	45,9	27,4	26,9	0,5	48,6	31,8
	sommer	16,5	0,4	70,3	23,4	24,3	0,4	56,1	26,9	20,8	0,4	49,8	26,0
	treter	46,9	0,6	45,5	38,7	59,9	0,6	33,1	38,6	16,5	0,5	73,9	33,5
Delta3	*module*	28,6	0,5	58,9	34,9	42,9	0,5	44,0	33,7	31,6	0,6	54,8	40,2
	sommer	34,7	0,5	53,2	35,0	27,4	0,5	56,6	32,5	31,6	0,6	54,7	39,3

A.8 Geräteübergreifende Authentifizierung ohne Anpassung

Tabelle A.4: Fehlerraten, bei nur einem Enrolment für die unterschiedlichen Geräte, wenn keine Transformation verwendet wird (in %)

Gerät		*treter*				*module*				*sommer*			
Enrol.	Verifi.	FAR		FRR		FAR		FRR		FAR		FRR	
		$\varnothing x$	s	$\varnothing x$	s	s	$\varnothing x$	s	$\varnothing x$	s	$\varnothing x$	s	
1	2	44,8	1,8	33,6	41,2	50,8	2,2	18,7	32,8	59,9	1,7	18,4	34,9
	3	16,1	2,7	27,1	32,7	17,1	2,8	13,8	27,4	18,1	2,3	20,2	30,7
2	1	39,4	1,8	38,5	42,3	56,6	1,6	15,7	29,7	50,6	2,4	25,2	37,5
	3	42,8	1,7	20,9	29,0	39,7	2,7	15,9	26,7	40,9	2,4	22,5	35,6
3	1	27,5	1,7	19,5	28,4	22,5	2,2	17,8	28,9	24,0	2,2	20,8	29,9
	2	45,0	1,6	23,7	34,5	33,6	2,8	23,8	34,3	41,7	3,8	22,8	35,6

Literaturverzeichnis

[ACCF07] Gabriel L. F. Azevedo, George D. C. Cavalcanti und Edson C. B. Carvalho Filho. Hybrid Solution for the Feature Selection in Personal Identification Problems through Keystroke Dynamics. In *International Joint Conference on Neural Networks*, Seiten 1947–1952, 2007.

[ACS08] Fawaz A. Alsulaiman, Jongeun Cha und Abdulmotaleb Saddik. User Identification Based on Handwritten Signatures with Haptic Information. In *Proceedings of the 6th international conference on Haptics: Perception, Devices and Scenarios (EuroHaptics 2008)*, Seiten 114–121, Berlin, Heidelberg, 2008. Springer-Verlag.

[AKA91] David Aha, Dennis Kibler und Marc Albert. Instance-based learning algorithms. In John Ross Quinlan, Hrsg., *Machine Learning*, Jgg. 6, Seiten 37–66. Kluwer Academic Publishers, 1991.

[ALM+05] Heikki J. Ailisto, Mikko Lindholm, Jani Mäntyjärvi, Elena Vildjiounaite und Satu-Marja Mäkelä. Identifying people from gait pattern with accelerometers. *BiometricTechnology for Human Identification II*, 5779:7–14, 2005.

[AM11] André Anjos und Sébastien Marcel. Counter-Measures to Photo Attacks in Face Recognition: a public database and a baseline. In *International Joint Conference on Biometrics (IJCB)*, Seiten 1–7, 2011.

M. Trojahn, *Sichere Multi-Faktor-Authentifizierung an Smartphones mithilfe des Tippverhaltens*, AutoUni – Schriftenreihe 85,
DOI 10.1007/978-3-658-14049-6

[ANB+01] Kamiar Aminian, Bijan Najafi, Christophe Büla, Pierre François Leyvraz und Philippe Robert. Ambulatory Gait Analysis Using Gyroscopes. In *25th Annual meeting of the American Society of Biomechanics (ASB2001)*, Seiten 309–310, San Diego, USA, 2001. American Society of Biomechanics.

[And12] Erik Anderson. The basics of waterproofing capacitive touchscreens. `http://www.eetimes.com/design/industrial-control/4374783/The-basics-of-waterproofing-capacitive-touchscreens?pageNumber=0`. Abruf am 10.12.2013, 2012.

[Arb10] Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften e.V. (AWMF). Leitlinien der Deutschen Gesellschaft für Neurologie: Tremor, 2010. `http://www.awmf.org/uploads/tx_szleitlinien/030-011_S1_Tremor_10-2008_10-2013.pdf`. Abruf am 25.10.2013.

[Arn12] Florian Arndt. Erkennung von Emotionen anhand des Tippverhaltens auf Touchscreen-Tastaturen. Masterarbeit, TU Braunschweig, Braunschweig, 2012.

[Aug11] Dieter Augustin. *Kleine Einführung in das Data Management*. Institut für Biometrie und Klinische Epidemiologie, Charité - Universitätsmedizin Berlin, Berlin, 22. Februar 2011. `http://biometrie.charite.de/fileadmin/user_upload/microsites/m_cc04/biometrie/SPSS/Data_Management.pdf`. Abruf am 13.10.2013.

[BC08] Arnaud Buchoux und Nathan L. Clarke. Deployment of Keystroke Analysis on a Smartphone. In *Proceedings of the 6th Australian Information Security & Management Conference*, 2008.

[Bee10] Wolfgang Beer. GeoPointer: approaching tangible augmentation of the real world. In Gabriele Kotsis, David Taniar, Eric Pardede, Irfan Awan, Imad Saleh und Ismail Khalil, Hrsg., *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM2010)*, Seiten 229–233, 2010.

[Beh13a] BehavioSec Inc. *White Paper - BehavioMobile: Applying the BehavioSec technology for Multilayered Mobile Security.* Stockholm, Sweden, 2013. `http://www.behaviosec.com/wp-content/uploads/2012/01/BehavioSec-BehavioMobile.pdf`. Abruf am 29.12.2013.

[Beh13b] Benjamin Behrendt. Evaluierung von Klassifikatoren zur Authentifizierung mithilfe des Tippverhaltens. Bachelorarbeit, Otto-von-Guericke Universität, Magdeburg, 2013.

[BH97] William Lowe Bryan und Noble Harter. Studies in the physiology and psychology of the telegraphic language. *Psychological review*, 4(1):27, 1897.

[BI12] Telekommunikation und neue Medien e.V. (BITKOM) Bundesverband Informationswirtschaft. *Smartphone-Besitzer vernachlässigen Sicherheit.* Berlin, 2012. `http://www.bitkom.org/files/documents/BITKOM_Presseinfo_Sicherheit_bei_Smartphones_24_07_2012.pdf`. Abruf am 13.12.2013.

[Bic12] Scott Bicheno. *Global Smartphone Installed Base by Operating System for 88 Countries: 2007 to 2017.* Strategy Analytics Wireless Smartphone Strategies (WSS), 09.10.2012. `http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=7834`. Abruf am 23.12.2013.

[BKKN03] Christian Borgelt, Frank Klawonn, Rudolf Kruse und Detlef Nauck. *Neuro-Fuzzy-Systeme: Von den Grundlagen künstlicher Neuronaler Netze zur Kopplung mit Fuzzy-Systemen.* Vieweg + Teubner, 3. Auflage, 2003.

[Bot12] Matthias K. Bothe. Der Koloss von Rhodos, 2012. `http://www.weltwunder-online.de/antike/koloss-rhodos-griechenland.htm`. Abruf am 23.12.2013.

[BP93] Roberto Brunelli und Tomaso Poggio. Face recognition: features versus templates. In *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Jgg. 15, Seiten 1042–1052, 1993.

[BPRP11] Kiran S. Balagani, Vir V. Phoha, Asok Ray und Shashi Phoha. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication. *Pattern Recognition Letters*, 32(7):1070–1080, 2011.

[Bro98] Felix Brosius. *SPSS 8.0: professionelle Statistik unter Windows.* mitp-Verlag, 1998.

[BS10] Jürgen Bortz und Christof Schuster. *Statistik für Human- und Sozialwissenschaftler. Lehrbuch mit Online-Materialien.* Springer-Lehrbuch. Springer, 2010.

[Bun11a] Bundesamt für Sicherheit in der Informationstechnik (BSI). *BSI gibt Tipps für sichere Passwörter.* Bonn, 2011. `https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Passwortsicherheit_27012011.html`. Abruf am 10.01.2013.

[Bun11b] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Überblickspapier Smartphones.* Bonn, 2011. `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf`. Abruf am 10.01.2013.

[Bun12] Bundesministerium für Bildung und Forschung (BMBF). Organische Elektronik - Hightech aus Kunststoff, 07.05.2012. `http://www.bmbf.de/de/16267.php`. Abruf am 13.12.2013.

[BW12] Salil P. Banerjee und Damon L. Woodard. Biometric Authentication and Identification using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research*, 7:116–139, 2012.

[CAJ03] Lynne Coventry, Antonella de Angeli und Graham Johnson. Usability and biometric verification at the ATM interface. In *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI 2003)*, Seiten 153–160, New York, NY, USA, 2003. ACM.

[CBF03] Kyong I. Chang, Kevin W. Bowyer und Patrick J. Flynn. Face recognition using 2D and 3D facial data. In *ACM Workshop on Multimodal User Authentication*, Seiten 25–32, 2003.

[CBS07] CBS Interactive Inc. *Google unveils cell phone software and alliance*, 2007. `http://news.cnet.com /8301-17939_109-9810937-2/google-unveils-cell-phone-software-and-alliance`. Abruf am 13.12.2013.

[CC11] Liang Cai und Hao Chen. TouchLogger: inferring keystrokes on touch screen from smartphone motion. In *Proceedings of the 6th USENIX conference on Hot topics in security (HotSec 2011)*, Berkeley, CA, USA, 2011. USENIX Association.

[CF06] Nathan L. Clarke und Steven M. Furnell. Authenticating mobile phone users using keystroke analysis. In *International Journal of Information Security*, Jgg. 6, Seiten 1–14, Berlin, Heidelberg, 2006. Springer-Verlag.

[Che03] Kyle Cherry. Biometrics: An In Depth Examination. In *InfoSec Reading Room*, Seiten 3–23. SANS Institute, 2003.

[CHHK00] Sungzoon Cho, Chigeun Han, Dae Hee Han und Hyung-Il Kim. Web-Based Keystroke Dynamics Identity Verification Using Neural Network. *Journal of Organizational Computing and Electronic Commerce*, 10(4):295–307, 2000.

[CHI09] CHIP Digital GmbH. *HTC Desire: Datenblatt*, 2009. `http://www.chip.de/preisvergleich/137110/Datenblatt-HTC-Desire.html`. Abruf am 13.12.2013.

[Cla94] Roger Clarke. Human identification in information systems: Management challenges and public policy issues. *Information Technology & People*, 7(4):6–37, 1994.

[CM07] Michał Choraś und Piotr Mroczkowski. Keystroke Dynamics for Biometrics Identification. In *Proceedings of the 8th international conference on Adaptive and Natural Computing Algorithms, Part II (ICANNGA 2007)*, Seiten 424–431, Berlin, Heidelberg, 2007. Springer-Verlag.

[CTL12] Ting-Yi Chang, Cheng-Jung Tsai und Jyun-Hao Lin. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of Systems and Software*, 85(5):1157–1165, 2012.

[Dau02] John Daugman. How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14:21–30, 2002.

[DBB98] Günther Deuschl, Peter Bain und Mitchell Brin. Consensus statement of the Movement Disorder Society on tremor. *Movement Disorders*, 13(S3):2–23, 1998.

[DDK+12] Stefan Dernbach, Barnan Das, Narayanan Chatapuram Krishnan, Brian L. Thomas und Diane J. Cook. Simple and Complex Activity Recognition through Smart Phones. In *Intelligent Environments'12*, Seiten 214–221, 2012.

[DG04] Kresimir Delac und Mislav Grgic. A survey of biometric recognition methods. In *Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium*, Seiten 184–193, 2004.

[DK09] Homa Davoudi und Ehsanollah Kabir. A new distance measure for free text keystroke authentication. In *Computer Conference, 2009. CSICC 2009. 14th International CSI*, Seiten 570–575, 2009.

[DLHB+12] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner und Heinrich Hussmann. Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *SIGCHI Conference on Human Factors in Computing Systems (CHI'12)*, Seiten 987–996, 2012.

[DNBB10] Mohammad Omar Derawi, Claudia Nickel, Patrick Bours und Christoph Busch. Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition. In *Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2010)*, Seiten 306–311, Washington, DC, USA, 2010. IEEE Computer Society.

[DPS05] Johan Du Preez und Basie von Solms. Personal Identification and Authentication by using "The way the heart beats". In *Electronic Proceedings of Information Security South Africa (ISSA)*, Seiten 1–12, 2005.

[ELM11] Clayton Epp, Michael Lippold und Regan L. Mandryk. Identifying emotional states using keystroke dynamics. In *Proceedings of the 2011 annual conference on Human factors in computing systems (CHI 2011)*, Seiten 715–724, New York, NY, USA, 2011. ACM.

[Erd13] Sebastian Erdenreich. *Negative Identifizierung anhand des Tippverhaltens bei Verwendung fester und freier Textbestandteile.* Dissertation, Wirtschaftswissenschaftlichen Fakultät der Universität Regensburg, Wiesbaden, 2013.

[Esp12] Alfredo Esposito. Debunking some myths about biometric authentication. *CoRR*, abs/1203.0333, 2012.

[Fra11] Helen Francis. *Unsaubere Berührung - Kapazitive Touch-Sensoren für nasse und schmutzige Oberflächen*, 2011. `http://www.all-electronics.de/texte/anzeigen/42925/Kapazitive-Touch-Sensoren-fuer-nasse-und-schmutzige-Oberflaechen`. Abruf am 13.12.2013.

[Fz05] Marcos Faundez-zanuy. Study of a Committee of Neural Networks for Biometric Hand-Geometry Recognition. *Neural Networks*, Seiten 1180 – 1187, 2005.

[Gaf08] Davrondzhon Gafurov. *Performance and security analysis of gait-based user authentication.* Dissertation, University of Oslo, Oslo, 2008.

[GCML13] Anshul Gupta, Roberta Cozza, Carolina Milanesi und C. K. Lu. *Market Share Analysis: Mobile Phones, Worldwide, 4Q12 and 2012.* Gartner Inc., 12.02.2013.

[GLRSGC02] Francisco J. Gutiérrez, Margarita M. Lerma-Rascón, Luis R. Salgado-Garza und Francisco J. Cantu. Biometrics and Data Mining: Comparison of Data Mining-Based

Keystroke Dynamics Methods for Identity Verification. In *Proceedings of the Second Mexican International Conference on Artificial Intelligence: Advances in Artificial Intelligence (MICAI 2002)*, Seiten 460–469, London, UK, UK, 2002. Springer-Verlag.

[GN11] Kirsten Götz-Neumann. *Gehen verstehen: Ganganalyse in der Physiotherapie*. Thieme, Stuttgart and , New York, 3. Auflage, 2011.

[GOM02] Shaun J. Grannis, J. Marc Overhage und Clement J. McDonald. Analysis of identifier performance using a deterministic linkage algorithm. *Proceedings of the AMIA Symposium*, Seiten 305–309, 2002.

[GPR05] Daniele Gunetti, Claudia Picardi und Giancarlo Ruffo. Keystroke analysis of different languages: a case study. In *Proceedings of the 6th international conference on Advances in Intelligent Data Analysis (IDA 2005)*, Seiten 133–144, Berlin, Heidelberg, 2005. Springer-Verlag.

[GR12] Romain Giot und Christophe Rosenberger. A new soft biometric approach for keystroke dynamics based on gender recognition. *International journal of information technology and management*, 11(1/2):35–49, 2012.

[Gra12] Michael Graumann. Extracting Biometrical Features via Swype. Bachelorarbeit, Otto-von-Guericke Universität, Magdeburg, 2012.

[GTN+99] Dale N. Glaser, B. Charles Tatum, Delbert M. Nebeker, Richard C. Sorenson und John R. Aiello. Workload and social support: Effects on performance and stress. *Human Performance*, 12(2):155–176, 1999.

[Har10] Shon Harris. *CISSP Certification All-in-One Exam Guide*. McGraw-Hill Professional, 2010.

[Hay14] Naveed Hayat. Aktivitätserkennung anhand der Sensorik eines Smartphones zur Unterstützung der Authentifizierung. Bachelorarbeit, Universität Kassel, Kassel, 2014.

[HAZ00] Sajjad Haider, Ahmed Abbas und Abbas K. Zaidi. A multi-technique approach for user identification through keystroke dynamics. In *Systems, Man, and Cybernetics, 2000 IEEE International Conference on*, Jgg. 2, Seiten 1336–1341, 2000.

[HB97] Young-Sup Hwang und Sung-Yang Bang. An efficient method to construct a radial basis function neural network classifier. *Neural Networks*, 10(9):1495–1503, 1997.

[HBGM05] Michael Husken, Michael Brauckmann, Stefan Gehlen und Christoph von der Malsburg. Strategies and Benefits of Fusion of 2D and 3D Face Recognition. In *Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR 2005)*, Seite 174, Washington, DC, USA, 2005. IEEE Computer Society.

[HCHX07] Bufu Huang, Meng Chen, Panfeng Huang und Yangsheng Xu. Gait Modeling for Human Identification. In *2007 IEEE International Conference on Robotics and Automation, ICRA 2007, 10-14 April 2007, Roma, Italy*, Seiten 4833–4838. IEEE, 2007.

[HFH+09] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann und Ian H. Witten. The WEKA Data Mining Software: An Update. In *SIGKDD Explorations*, Jgg. 11, Seiten 10–18, 2009.

[HHSU08] Andreas Holzinger, Martin Holler, Martin Schedlbauer und Berndt Urlesberger. An investigation of finger

versus stylus input in medical scenarios. In *30th International Conference on Information Technology Interfaces, 2008 (ITI 2008)*, Seiten 433–438, 2008.

[Hil99] Robert Hill. Retina Identification. In Anil K. Jain, Ruud M. Bolle und Sharath Pankanti, Hrsg., *Biometrics Personal Identification Networked*. Kluwer Academic Publishers, Boston, MA, 1999.

[HKNT09] Markus Huber, Stewart Kowalski, Marcus Nohlberg und Simon Tjoa. Towards automating social engineering using social networking sites. In *Computational Science and Engineering, 2009. CSE '09. International Conference on*, Jgg. 3, Seiten 117–124, 2009.

[HRB12] Niels Henze, Enrico Rukzio und Susanne Boll. Observational and experimental investigation of typing behaviour using virtual keyboards for mobile devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2012)*, Seiten 2659–2668, New York, NY, USA, 2012. ACM.

[HYJ+12] Hwan Hwangbo, Sol Hee Yoon, Beom Suk Jin, Young Suk Han und Yong Gu Ji. A Study of Pointing Performance of Elderly Users on Smartphones. *International Journal of Human-Computer Interaction*, 2012.

[IEE10] IEEE Biometrics Certification. *IEEE Certified Biometrics Professional (CBP): Learning System*, Jgg. Module 2 of *Biometric Modalities*. 1.1. Auflage, 2010.

[II05] International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC). ISO/IEC 27001, 15.10.2005.

[II06] International Organization for Standardization (ISO) und International Electrotechnical Commission (IEC). JTC 1/SC 37 Biometrcs, 28.02.2006.

[JBP02] Anil K. Jain, Ruud M. Bolle und Sharath Pankanti. *Biometrics: personal identification in networked society*. Kluwer Academic Publishers, New York, Boston, Dordrecht, London, Moscow, 2002.

[JFR08a] Anil K. Jain, Patrick J. Flynn und Arun A. Ross. *Handbook of biometrics*. Springer, New York, N.Y, 2008.

[JFR08b] Anil K. Jain, Patrick J. Flynn und Arun A. Ross, Hrsg. *Introduction to Biometrics*. Springer US, Boston, MA, 2008.

[JG90] Rick Joyce und Gopal Gupta. Identity authentication based on keystroke latencies. In *Commun. ACM*, Jgg. 33, Seiten 168–176, New York, NY, USA, 1990. ACM.

[JHP00] Anil K. Jain, L. Hong und S. Pankanti. Biometric identification. *Communications of the ACM*, 43(2):90–98, 2000.

[JNN08] Anil K. Jain, Karthik Nandakumar und Abhishek Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008.

[KAK11] Marcus Karnan, Muthuramalingam Akila und Nishara Krishnaraj. Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*, 11(2):1565–1573, 2011.

[KC07] Sevasti Karatzouni und Nathan L. Clarke. Keystroke Analysis for Thumb-based Keyboards on Mobile Devices. In Hein S. Venter, Mariki M. Eloff, Les Labuschagne, Jan H. P. Eloff und Rossouw von Solms, Hrsg.,

New Approaches for Security, Privacy and Trust in Complex Environments, Proceedings of the IFIP TC-11 22nd International Information Security Conference (IFIP), Jgg. 232, Seiten 253–263. Springer, 2007.

[KHA+05] Seong G. Kong, Jingu Heo, Besma R. Abidi, Joonki Paik und Mongi A. Abidi. Recent advances in visual and infrared face recognition - a review. *Computer Vision and Image Understanding*, 97:103–135, 2005.

[KHLF10] Himanshu Khurana, Mark Hadley, Ning Lu und Deborah A. Frincke. Smart-grid security issues. *Security & Privacy, IEEE*, 8(1):81–85, 2010.

[KMB93] Paul Kabbash, Scott MacKenzie und William Buxton. Human performance using computer input devices in the preferred and non-preferred hands. In *Proceedings of the INTERACT'93 and CHI'93 conference on Human factors in computing systems*, Seiten 474–481, 1993.

[Kri12] David Kriesel. Ein kleiner Überblick über Neuronale Netze, 16.05.2012. `http://www.dkriesel.com/_media/science/neuronalenetze-de-zeta2-2col-dkrieselcom.pdf`. Abruf am 13.12.2013.

[KSR11] Juliane Kämpfe, Peter Sedlmeier und Frank Renkewitz. The impact of background music on adult listeners: A meta-analysis. *Psychology of Music*, 39(4):424–448, 2011.

[KWM11] Jennifer R. Kwapisz, Gary M. Weiss und Samuel A. Moore. Activity recognition using cell phone accelerometers. *ACM SIGKDD Explorations Newsletter*, 12(2):74–82, 2011.

[KWW12] Sarah Martina Kolly, Roger Wattenhofer und Samuel Welten. A personal touch: recognizing users based on

touch screen behavior. In *Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones (PhoneSense 2012)*, Seiten 1:1–1:5, New York, NY, USA, 2012. ACM.

[Lin97] Daw-Tung Lin. Computer-access authentication with neural network based keystroke identity verification. In *International Conference on Neural Networks*, Jgg. 1, Seiten 174 –178, 1997.

[LJ05] Xiaoguang Lu und Anil K. Jain. Integrating Range and Texture Information for 3D Face Recognition. In *Proceedings of the Seventh IEEE Workshops on Application of Computer Vision (WACV/MOTION'05)*, Seiten 156–163, Washington, DC, USA, 2005. IEEE Computer Society.

[LW88] John J. Leggett und Glen Williams. Verifying identity via keystroke characteristics. In *Int. J. Man-Mach. Stud*, Jgg. 28, Seiten 67–76, London, UK, UK, 1988. Academic Press Ltd.

[LWTJ04] Jiangwei Li, Yunhong Wang, Tieniu Tan und Anil K. Jain. Live face detection based on the analysis of Fourier spectra. In *In Biometric Technology for Human Identification*, Seiten 296–303, Orlando, Fla, USA„ 2004.

[MCGCN11] Emanuele Maiorana, Patrizio Campisi, Noelia González-Carballo und Alessandro Neri. Keystroke dynamics authentication for mobile phones. In *Proceedings of the 2011 ACM Symposium on Applied Computing (SAC 2011)*, Seiten 21–26, New York, NY, USA, 2011. ACM.

[ME10] Anthony R. Metke und Randy L. Ekl. Security Technology for Smart Grid Networks. *IEEE Transactions on Smart Grid*, 1(1):99–107, 2010.

[Mei13] Torsten Meier. Ubiquitäre biometrische Authentifizierung mithilfe des Tippverhaltens. Bachelorarbeit, Otto-von-Guericke Universität, Magdeburg, 2013.

[Mey10] Paul Meyer. E-Ink vs. LCD, 08.11.2010. `http://eink-vs-lcd.articles.r-tt.com/`. Abruf am 13.12.2013.

[MFM+09] Robert Moskovitch, Clint Feher, Arik Messerman, Niklas Kirschnick, Tarik Mustafic, Ahmet Camtepe, Bernhard Löhlein, Ulrich Heister, Sebastian Möller, Lior Rokach und Yuval Elovici. Identity theft, computers and behavioral biometrics. In *Proceedings of the 2009 IEEE international conference on Intelligence and security informatics (ISI 2009)*, Seiten 155–160, Piscataway, NJ, USA, 2009. IEEE Press.

[ML07] Hyeonjoon Moon und Kisung Lee. Biometric driver authentication based on 3D face recognition for telematics applications. In *Proceedings of the 4th international conference on Universal access in human computer interaction: coping with diversity (UAHCI 2007)*, Seiten 473–480, Berlin, Heidelberg, 2007. Springer-Verlag.

[MLV+05] Jani Mäntyjärvi, Mikko Lindholm, Elena Vildjiounaite, Satu-Marja Makela und Heikki J. Ailisto. Identifying users of portable devices from gait pattern with accelerometers. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2005.

[Mor04] Stacy J. Morris. *A Shoe-integrated Sensor System for Wireless Gait Analysis and Real-time Therapeutic Feedback*. Dissertation, Division of Health Sciences and Technology, Harvard University-MIT, Cambridge, Mass, USA, 2004.

[MR97] Fabian Monrose und Aviel D. Rubin. Authentication via keystroke dynamics. In *Proceedings of the 4th ACM*

Conference on Computer and Communications Security (CCS 1997), Seiten 48–56, New York, NY, USA, 1997. ACM.

[MR00] Fabian Monrose und Aviel D. Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4):351–359, 2000.

[MVBC12] Emiliano Miluzzo, Alexander Varshavsky, Suhrid Balakrishnan und Romit Roy Choudhury. Tapprints: your finger taps have fingerprints. In *Proceedings of the 10th international conference on Mobile systems, applications, and services (MobiSys 2012)*, Seiten 323–336, New York, NY, USA, 2012. ACM.

[Nat02] National Institute of Standards and Technology (NIST). Summary of NIST standards for biometric accuracy, tamper resistance, and interoperability, 13. November 2002.

[OF00] Tim Ord und Steven M. Furnell. User Authentication for Keypad-Based Devices Using Keystroke Analysis. In *2. International Network Conference (INC 2000)*, Seiten 263–272, 2000.

[Olz06] Tom Olzak. Keystroke Dynamics: Low Impact Biometric Verification. *Erudio Security, September*, 2006.

[OM93] Mohammad S. Obaidat und D.T Macchiarolo. An online neural network system for computer access security. *IEEE Transactions on Industrial Electronics*, 40(2):235–242, 1993.

[Ope08] Open Handset Alliance (OHA). Get the Android SDK, 2008. `http://developer.android.com/sdk/index.html`. Abruf am 13.12.2013.

[Ope13a] Open Handset Alliance (OHA). Licenses, 2013. `http://source.android.com/source/licenses.html`. Abruf am 13.12.2013.

[Ope13b] Open Handset Alliance (OHA). Position Sensors | Android Developers, 2013. `http://developer.android.com/guide/topics/sensors/sensors_position.html`. Abruf am 13.12.2013.

[Ope13c] Open Handset Alliance (OHA). SensorManager | Android Developers, 2013. `http://developer.android.com/reference/android/hardware/SensorManager.html`. Abruf am 13.12.2013.

[OS97] Mohammad S. Obaidat und Balqies Sadoun. Verification of computer users using keystroke dynamics. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*, 27(2):261–269, 1997.

[Ote05] Michael Otero. Application of a continuous wave radar for human gait recognition. In *Defense and Security*, Seiten 538–548, 2005.

[PPJ03] Salil Prabhakar, Sharath Pankanti und Anil K. Jain. Biometric recognition: Security and privacy concerns. *Security & Privacy, IEEE*, 1(2):33–42, 2003.

[QTKJ08] Yi Qian, David Tipper, Prashant Krishnamurthy und James Joshi. *Information Assurance: Dependability and Security in Networked Systems*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2008.

[R&13] R&L AG. Thema: Tippbiometrie: Sichere und komfortable Authentifizierung und Identifizierung durch Tippverhaltenserkennung, 2013.

[Rad07] Katrin Radestock. Bewertung der praktischen Einsetzbarkeit von multibiometrischen Verfahren. Diplomarbeit, Otto-von-Guericke Universität, Magdeburg, 2007.

[Rae01] Martin Raepple. *Sicherheitskonzepte für das Internet*. dpunkt.verlag GmbH, Heidelberg, 2. Auflage, 2001.

[RJ03] Arun Ross und Anil K. Jain. Information fusion in biometrics. In *Pattern Recognition Letters*, Jgg. 24, Seiten 2115–2125, 2003.

[RJMX07] Liu Rong, Zhou Jianzhong, Liu Ming und Hou Xiangfeng. A Wearable Acceleration Sensor System for Gait Recognition. *2nd IEEE Conference on Industrial Electronics and Applications, 2007 (ICIEA 2007)*, Seiten 2654 – 2659, 2007.

[RNJ06] Arun A. Ross, Karthik Nandakumar und Anil K. Jain. *Handbook of Multibiometrics (International Series on Biometrics)*, Jgg. 6. Springer-Verlag New York, Inc, Secaucus, NJ, USA, 2006.

[Rob06] Chris Roberts. Biometric technologies-palm and hand, 2006. `http://www.ccip.govt.nz/newsroom/information-notes/2006/biometricstechnologies-palmhand.pdf`. Abruf am 13.12.2013.

[RZJM07] Liu Rong, Duan Zhiguo, Zhou Jianzhong und Liu Ming. Identification of individual walking patterns using gait acceleration. In *The 1st International Conference on Bioinformatics and Biomedical Engineering, (ICBBE)*, Seiten 543–546, 2007.

[Sam11a] Samsung Electronics GmbH. *Technische Daten: Galaxy Nexus*, 2011. `http://www.samsung.com/uk/consumer/mobile-devices/smartphones/android/GT-I9250TSAXEU`. Abruf am 13.12.2013.

[Sam11b] Samsung Electronics GmbH. Technische Daten: GALAXY S II, 2011. http://www.samsung.com/global/business/mobile/product/smartphone/GT-I9100LKAXSP-spec. Abruf am 13.12.2013.

[Sam12] Samsung Electronics GmbH. Technische Daten: GALAXY S III, 2012. http://www.samsung.com/de/consumer/mobile-device/mobilephones/smartphones/GT-I9300MBDDBT. Abruf am 13.12.2013.

[Sas05] Angela Sasse. Usability and trust in information systems. In *Mansell, R., Collins, B. (Eds.), Trust and Crime in Information Societies.*, Seiten 319–348, Cheltenham, UK: Edward Elgar, 2005.

[SBD+09] Tobias Scheidat, Michael Biermann, Jana Dittmann, Claus Vielhauer und Karl Kümmel. Multi-biometric fusion for driver authentication on the example of speech and face. In *Proceedings of the 2009 joint COST 2101 and 2102 international conference on Biometric ID management and multimodal communication (BioID_MultiComm'09)*, Jgg. 5707, Seiten 220–227, Berlin, Heidelberg, 2009. Springer-Verlag.

[SK12] Jan Erik Solem und Fredrik Kahl. 3D Object Recognition, 2012. http://www.freepatentsonline.com/y2012/0114251.html. Abruf am 13.12.2013.

[SKBD+01] Henning Stolze, Johann P. Kuhtz-Buschbeck, H. Drücke, K. Jöhnk, Michael Illert und Günther Deuschl. Comparative analysis of the gait disorder of normal pressure hydrocephalus and Parkinson's disease. *J Neurol Neurosurg Psychiatry*, 70(3):289–297, 2001.

[Smi12] Chris Smith. How It Works: AMOLED Displays, 01. Juni 2012. http://www.androidauthority.com/

`amoled-display-how-it-works-91552/`. Abruf am 13.12.2013.

[SR05] Jürgen Schoolmann und Holger Rieger. *Praxishandbuch IT-Sicherheit. Risiken, Prozesse, Standards*. Symposion Publishing GmbH, Düsseldorf, 2005.

[Sto01] Gary Stoneburner. NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, 2001.

[STS10] Sulochana Sonkamble, Ravindra Thool und Balwant Sonkamble. Survey of Biometric Recognition Systems and Their Applications. In *Journal of Theoretical and Applied Information Technology*, 2010.

[SWS09] Abu Bakar Sulong, Martono Wahyudi und Muhammad Umar Siddiqi. Intelligent keystroke pressure-based typing biometrics authentication system using radial basis function network. In *Proceedings of 2009 5th International Colloquium on Signal Processing and Its Applications, CSPA 2009*, Seiten 151–155, 2009.

[Swy12] Swype Inc. Swype: Type Fast, Swype Faster, 2012. `http://www.swypeinc.com/`. Abruf am 13.12.2013.

[SYY+11] Weidong Shi, Jun Yang, Yifei Jiang, Feng Yang und Yingen Xiong. SenGuard: Passive user identification on smartphones using multiple sensors. In *7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Seiten 141–148, 2011.

[SZ09] Sebastijan Sprager und Damjan Zazula. A cumulant-based method for gait identification using accelerometer data with principal component analysis and support vector machine. *WSEAS Trans. Sig. Proc*, 5(11):369–378, 2009.

[TAO13] Matthias Trojahn, Florian Arndt und Frank Ortmeier. Authentication with Keystroke Dynamics on Touchscreen Keypads - Effect of different N-Graph Combinations. In *3. International Conference on Mobile Services, Resources, and Users (MOBILITY 2013)*, 2013.

[TAWO13] Matthias Trojahn, Florian Arndt, Markus Weinmann und Frank Ortmeier. Emotion Recognition Through Keystroke Dynamics on Touchscreen Keyboards. In *15th International Conference on Enterprise Information Systems (ICEIS 2013)*, Seiten 31–37, 2013.

[TGG13] Chee Meng Tey, Payas Gupta und Debin Gao. I can be You: Questioning the use of Keystroke Dynamics as Biometrics. In *20th Annual Network and Distributed System Security Symposium, NDSS 2013, San Diego, California, USA, February 24-27, 2013*. The Internet Society, 2013.

[TM12] Matthias Trojahn und Philipp Marcus. Towards coupling user and device locations using biometrical authentication on smartphones. In *7. International Conference For Internet Technology And Secured Transactions (ICITST)*, Seiten 736–741, 2012.

[TO12] Matthias Trojahn und Frank Ortmeier. Biometric Authentication Through a Virtual Keyboard for Smartphones. In Jan Zizka, Hrsg., *International Journal of Computer Science & Information Technology (IJCSIT)*, 5, Seiten 1–12, 2012.

[TO13a] Matthias Trojahn und Frank Ortmeier. KeyGait Framework for Continuously Biometric Authentication during Usage of a Smartphone. In *3. International Conference on Mobile Services, Resources, and Users (MOBILITY 2013)*, 2013.

[TO13b] Matthias Trojahn und Frank Ortmeier. Keystroke Authentication on Mobile Devices with a Capacitive Display. In *2nd International Conference on Pattern Recognition Applications and Methods (ICPRAM 2013)*, Seiten 637–640, 2013.

[TO13c] Matthias Trojahn und Frank Ortmeier. Toward mobile authentication with keystroke dynamics on mobile phones and tablets. In Leonard Barolli, Fatos Xhafa, Makoto Takizawa, Tomoya Enokido und Hui-Huang Hsu, Hrsg., *27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Seiten 697 – 702, 2013.

[Tön05] Klaus D. Tönnies. *Grundlagen der Bildverarbeitung*. Pearson Studium, 2005.

[TPS13] Matthias Trojahn, Lei Pan und Fabian Schmidt. Developing a Cloud Computing Based Approach for Forensic Analysis using OCR. In Holger Morgenstern, Ralf Ehlert, Felix Freiling, Sandra Frings, Oliver Goebel, Detlef Guenther, Stefan Kiltz, Jens Nedon und Dirk Schadt, Hrsg., *7th International Conference on IT Security Incident Management & IT Forensics (IMF 2013)*, Seiten 59 – 68, 2013.

[Tro11] Matthias Trojahn. Softwareunterstützte Entscheidungsfindung für authentisierten Zugang in IT-Infrastrukturen aus ungesicherten Medien. Masterarbeit, Otto-von-Guericke Universität, Magdeburg, 2011.

[TSO13] Matthias Trojahn, Christian Schadewald und Frank Ortmeier. Keystroke Authentication with a Capacitive Display using Different Mobile Devices. In *10th International Conference on Security and Cryptography (SECRYPT 2013)*, Seiten 580–585, 2013.

[TTS03] Filareti Tsalakanidou, Dimitrios Tzovaras und Michael G. Strintzis. Use of depth and colour eigenfaces for face recognition. *Pattern Recognition Letters*, 24(9-10):1427–1435, 2003.

[TVTC12] Hoang Minh Thang, Vo Quang Viet, Nguyen Dinh Thuc und Deokjai Choi. Gait identification using accelerometer on mobile phone. In *Control, Automation and Information Sciences (ICCAIS), 2012 International Conference on*, Seiten 344–348, 2012.

[Twe09] Jessica Twentyman. Lost smartphones pose significant corporate risk, 2009. `http://www.scmagazineuk.com/lost-smartphones-pose-significant-corporate-risk/article/12675 9/`. Abruf am 13.12.2013.

[UW85] David Umphress und Glen Williams. Identity verification through keyboard characteristics. In *International Journal of Man-Machine Studies*, Jgg. 23, Seiten 263–273, 1985.

[Vie06] Claus Vielhauer. *Biometric User Authentication for IT Security: From Fundamentals to Handwriting*. Advances in information security. Springer-Verlag, New York, NY, 2006.

[VML+06] Elena Vildjiounaite, Satu-Marja Makela, Mikko Lindholm, Reima Riihimäki, Vesa Kyllönen, Jani Mäntyjärvi und Heikki J. Ailisto. Unobtrusive Multimodal Biometrics for Ensuring Privacy and Information Security with Personal Devices. In *Pervasive Computing*, Jgg. 3968, of *Lecture Notes in Computer Science*, Seiten 187–201, 2006.

[Woo11] James T. Wood. Droid Touchscreen Tests | eHow.com, 2011. `http://www.ehow.com/info_12212814_droid-touchscreen-tests.html`. Abruf am 13.12.2013.

[WSI+01] Fadhli Wong Mohd Hasan Wong, Ainil Sufreena Mohd Supian, Ahmad Faris Ismail, Lai Weng Kin und Ong Cheng Soon. Enhanced user authentication through typing biometrics with artificial neural networks and k-nearest neighbor algorithm. In *Conference Record of Thirty-Fifth Asilomar Conference on Signals, Systems and Computers (Cat.No.01CH37256)*, Jgg. 2, Seiten 911–915. IEEE, 2001.

[ZG09] Xiaozheng Zhang und Yongsheng Gao. Face recognition across pose: A review. *Pattern Recognition*, 42(11):2876–2896, 2009.

[ZSKF09] Saira Zahid, Muhammad Shahzad, Syed Ali Khayam und Muddassar Farooq. Keystroke-Based User Identification on Smart Phones. In *Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection (RAID 2009)*, Seiten 224–243, Berlin, Heidelberg, 2009. Springer-Verlag.