ML-gestützte Authentifizierung mit QR Code und Smartphone

Markus Hertlein

XignSys GmbH
hertlein@xignsys.com

Zusammenfassung

Die Welt wird immer digitaler und vernetzter. Dies führt zu einem massiven Angebot an digitalen Diensten für Privatpersonen und Unternehmen. Alle diese digitalen Dienste beherbergen eine Fülle an sensiblen persönlichen Informationen und Unternehmensdaten. Das hat zur Folge, dass heute jede Person eine Vielzahl von digitalen Identitäten besitzt, mit der sie sich im Internet bewegt. Der Schutz und die Verwendung der digitalen Identität, der Daten und Dienste liegt einer vorherigen Authentifizierung zu Grunde. Hier besteht die Notwendigkeit nach einer digitalen Identitylösung, die ein hohen Schutzbedarf liefert, zeitgleich aber flexibel für mehrere Use Cases geeignet ist und für den Endnutzer einfach zu verwenden ist. Ein QR Code basiertes Identity und Authentifikationssystems, das als Nutzerschnittstelle das Smartphone verwendet, erfüllt diese Anforderung [HeMP17] [CHCP18]. Durch die Erweiterung des Systems, um die Authentifizierung durch Nutzerverhaltensanalyse per Smartphone-Sensoren, mit maschineller Lerneinheit, wird sowohl die Sicherheit als auch die Benutzerfreundlichkeit gesteigert. Dazu wird in der vorliegenden Arbeit ein möglicher Ansatz zur Umsetzung beschrieben und bewertet.

1 Einleitung

Die Welt wird immer digitaler und vernetzter. Dies führt zu einem massiven Angebot an digitalen Diensten für Privatpersonen und Unternehmen. All die digitalen Dienste beherbergen eine Fülle an sensiblen persönlichen Informationen und Unternehmensdaten. Das hat zur Folge, dass heute jede Person eine Vielzahl von digitalen Identitäten besitzt, mit der sie sich im Internet bewegt. Digitale Identitäten sind für die Datendiebe interessant, da sie sensible Informationen beinhalten, die missbraucht werden können, um Betrug, strafbare Geschäfte, illegale Transaktionen etc. durchzuführen [Do18]. Dabei kann eine digitale Identität sowohl privat als auch geschäftlich sein. Um die Nutzung digitaler Identitäten und die damit verbundenen Daten vor unbefugten Zugriffen zu schützen, wird eine Authentifizierung durch den Eigentümer benötigt. Dabei ist die Nutzung von unsicheren Passwörtern immer noch die am häufigsten verwendete Form der Authentifizierung. Laut einer Umfrage auf Statista aus dem Jahr 2014 besitzen die Menschen mehrere Online-Passwörter. Doch bei Identitätsdiebstählen wurden in den letzten fünf Jahre mehr als 5 Milliarden digitale Identitäten und Passwörter gestohlen [Hert17]. Dabei sind nicht nur kleine und mittelständische Firmen von Angriffen betroffen, sondern auch Internet-Unternehmen mit mehr als drei Milliarden Nutzern. Sowohl der Umstand der Benutzerunfreundlichkeit, als auch die Unsicherheit bei der Verwendung aktueller Authentifizierungsverfahren erfordert einen neuen Ansatz, der die einfache und sichere Verwendung von digitalen Identitäten ermöglicht, in einer Vielzahl von Use Cases.

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 372-382.

1.1 Ziele

Die vorliegende Arbeit stellt eine innovative Lösung der Authentifizierung für eine Vielzahl von Use Cases vor. Um ein möglichst hohes Maß an Sicherheit und Nutzerakzeptanz zu gewährleisten, soll die vorgestellte Authentifizierungslösung folgende Ziele abdecken:

1. Erhöhte Benutzerfreundlichkeit. Um den Nutzer aus der Verantwortung zunehmen, soll die Benutzerfreundlichkeit erhöht werden, indem Fehlverhalten minimiert wird und auftretendes Fehlverhalten toleriert wird und auch ungeübte und nicht technikaffine Personen ihre digitale Identität sicher nutzen können.
2. Erhöhte Sicherheit. Ein Fehlverhalten des Nutzers soll nicht zur Unsicherheit des Systems führen. Damit sollen auch Phishing und weitere aktuelle Angriffe auf Nutzer und die Authentifizierung von Informationssystemen nicht zur Unsicherheit oder den Identitätsdiebstahl führen.
3. Maximale Flexibilität. Ein Nutzer soll die Möglichkeit haben ein Authentifizierungsverfahren für eine Vielzahl und unterschiedliche Anwendungsfälle zu nutzen. Dabei sollen heute aktuelle Anwendungen, bspw. die Authentifizierung an Webseiten, aber auch zukunftsweisende Anwendungsfälle, wie z. B. die Authentifizierung im Internet der Dinge oder an elektrolade Säulen, unterstützt werden.
4. Erhöhung des Datenschutzes. Das Authentifizierungssystem soll bedarfsgerecht Nutzerdaten verarbeiten und bei der Ansammlung von personenbezogenen Daten, diese auf die für die Authentifizierung nötige Menge reduzieren. Es soll verhindert werden, dass ein Nutzer zu jedem Zeitpunkt, ggf. auch ohne Wissens des Nutzers authentifiziert und somit identifiziert werden kann.

1.2 Abgrenzung

Aktuellen Themen aus dem Bereich der ML gestützten Authentifizierung befassen sich mit der passiven kontinuierlichen Authentifizierung [SLY+16] [CeMC17] und der Analyse von Eingaben [Bart00]. Die hier vorliegende Arbeit, beschränkt sich im Vergleich zu den Arbeiten, der passiven kontinuierlichen Authentifizierung, auf die Nutzung der Smartphone-Sensoren bei der direkten Handlung des Scannens eines QR Codes [HeMP15b]. Damit soll die Belastung der Smartphone-Batterie reduziert werden und die Akzeptanz beim Nutzer erhöht werden. Der Nutzer empfindet eine kontinuierliche Erfassung und Auswertung der Daten der Smartphone-Sensoren als Überwachung, bspw. in dem die Interaktion mit dem Smartphone analysiert wird [MTSH18].

2 Verwendete Technologien

Damit die oben genannten Ziele erreicht werden können, muss ein Paradigmenwechsel bei der Authentifizierung stattfinden [HeMP15a]. Dabei sollen alten Verfahren im Ganzen, durch eine neue auf maschinelles Lernen beruhende Methode abgelöst werden. Dazu wird als Nutzerschnittstelle das Smartphone genutzt und als Schnittstelle zum Auslösen einer Authentifizierung, ein optischer Auslöser im Form eines QR Codes.

2.1 QR Codes

QR Codes sind 2D-Barcodes, die es ermöglichen bis zu 31.329 Bytes zu codieren. Die maximale Anzahl der zu codierenden Bytes hängt dabei von der Version des QR Codes (max. Version 40 mit 177 Spalten * 177 Zeilen) und weiteren Parametern abhängig. Dabei können Parameter die Stärke der Fehlerkorrektur sein und um welchen Inhalt (numerische, alphanumerisch, binär, …) es sich handelt. Fehlerkorrektur wird erzeugt, indem Teile des QR Codes redundant innerhalb der 2D-Matrix vorkommen [Hara02]. QR Codes finden im Bereich der Authentifizierung eine immer größer werdende Akzeptanz. Der Unterschied des Systems, das die Grundlage der hier vorliegenden Arbeit bildet, im Vergleich zu anderen Systemen die QR Codes für die Nutzerauthentifizierung nutzen, liegt in den im QR Code enthaltenen Daten. Es werden hier keine sensiblen Informationen gespeichert, wodurch das System auch für die Authentifizierung in Szenarien genutzt werden kann, bei dem statische und nicht dynamische QR Codes verwendet werden können [HePM15c].

2.2 Smartphone

Die Nutzung des Smartphones wird in der heutigen Zeit immer wichtiger und nimmt immer mehr Zeit im täglichen Leben eines jeden Menschen in Anspruch. Im Jahr 2016 nutzen 49 Millionen Menschen in Deutschland ihr Smartphone, wohingegen es nur rund 45,5 Millionen Menschen im Februar 2015 waren [Stat16a]. Bis 2019 wird vorausgesagt, dass 55,5 Millionen Menschen in Deutschland ein Smartphone für ihr tägliches Leben nutzen werden [Stat16a]. Zusätzlich nutzten 2014 knapp 54% der deutschen Bevölkerung mobiles Internet.

Damit hat das Smartphone den Weg in unsere Gesellschaft als technologischer Alltagsgegenstand gefunden. Neben der weiten Verbreitung ist die Interaktion mit dem Smartphone einfach zu erlernen, wodurch eine komfortable und benutzerfreundliche Nutzerschnittstelle gegeben ist [Do17].

Das Smartphone bietet neben den Anzeigekomponenten wie Bildschirm und Signal-LEDs, weitere Mitteilungskomponenten wie den Lautsprecher und Vibrationsmöglichkeiten, mit denen man dem Nutzer für unterschiedliche Ereignisse bei einer Authentifizierung, unterschiedliches Feedback geben kann.

Damit bildet das Smartphone eine einfach zu verwendende Nutzerschnittstelle. Der Nutzer muss zur Verwendung des Smartphones nicht trainiert werden, wodurch die Akzeptanz durch den Nutzer erhöht wird. Darüber hinaus bietet das Smartphone mit dem hochauflösenden Display eine sehr gute Möglichkeit, um dem Nutzer über Aktivitäten, verwendete Daten und Schritte während der Authentifizierung transparent zu Informieren. Damit kann die Sicherheit des Gesamtsystems gesteigert werden.

Das Smartphone besitzt aktive Eingabekomponenten, wie die Touchfunktionalität des Displays, mit denen der Nutzer eine bewusste und prüfbare Handlung durchführen kann. Bspw. das Bestätigen der Zustimmung der zu übertragenden Daten, um eine datenschutzkonforme und für den Nutzer transparente Handlung durchzuführen. Für die hier vorliegende Arbeit soll die Nutzerauthentifizierung anhand der verfügbaren passiven Sensoren durchgeführt werden. Passive Smartphone-Sensoren können dazu genutzt werden, Informationen, über den Kontext oder der Umgebung, in der sich ein Nutzer befindet, zu sammeln. Um die Akzeptanz durch den Nutzer weiter zu erhöhen, sollen für die passive Authentifizierung Sensoren genutzt werden, die keine weitere Berechtigung erfordern. Damit kann die passive Authentifizierung auch zu bestehenden Apps hinzugefügt werden, um auch hier die Sicherheit zu erhöhen.

In der folgenden Tabelle 1 [Do18] werden die verfügbaren Sensoren eines Smartphones aufgelistet. Nicht jedes Smartphone verfügt über alle Sensoren. Bei einem empirischen Vergleich von 10 Smartphones, waren die häufigsten vorkommenden Sensoren das Mikrofon, der Accelerometer und das Gyroskop. Die betrachteten Smartphones waren zwischen zwei und sieben Jahren alt.

Tab. 1: Verfügbare Sensoren eines Smartphones.

Sensor	Erfasste Daten	Kategorie	Zustimmung erforderlich
Accelerometer	Beschleunigung (x,y,z)	Bewegung	Nein
Gyroskop	Erfasst Richtungsänderungen (x,y,z)	Bewegung	Nein
Magnetometer	Magnetisches Feld (Erde)	Umgebung	Nein
Luxmeter	Helligkeitsinformationen	Umgebung	Nein
Mikrofon	Aufnahme von Geräuschen	Umgebung	Ja
Proximity Sensor	Erfasst ob Objekt in unmittelbarer Nähe	Umgebung	Nein
Barometer	Luftdruck	Umgebung	Nein
Hygrometer	Luftfeuchtigkeit	Umgebung	Nein
Thermometer	Temperatur	Umgebung	Nein
Fingerabdruck-sensor	Fingerabdruck	Biometrie	Ja
GPS	Positionsdaten	Bewegung	Ja

Die hier vorliegende Arbeit verwendet ausschließlich den Accelerometer und das Gyroskop, um das Verhalten des Nutzers zu erfassen. Zu einem sollen die These, dass ein Nutzer eindeutige Bewegungen während des Scannen eines QR Codes ausführt und damit eine sichere Authentifizierung durchgeführt werden kann, überprüft werden. Zum anderen, werden für diese beiden Sensoren keine zusätzlichen Berechtigungen benötigt und der Nutzer muss nicht befürchten, dass weitere Informationen aus seiner Umgebung aufgenommen werden.

2.3 Maschinelles Lernen

Die durch das Smartphone gesammelten Sensorwerte werden durch eine maschinelle Lerneinheit ausgewertet. Dabei werden unterschiedliche Algorithmen hinsichtlich der Laufzeit und Qualität der Auswertung betrachtet. Algorithmen sind die Support Vector Maschine und k-Nearest-Neighbour.

Mit dem Starten einer Smartphone App werden die beiden Sensoren dazu genutzt 7 Sensorwerte (x,y,z jeweils vom Gyroskop und Accelerometer) und die Dauer der Authentifizierung aufzunehmen. Das Intervall, in dem die Sensorwerte erfasst werden – die Dauer der Authentifizierung –, endet mit dem Scannen des QR Codes.

Die Sensorwerte der ersten Nutzerauthentifizierungen werden dazu genutzt, um ein Profil des Nutzers zu erlernen. Die Profile werden später dazu genutzt, um bei einer erneuten Authentifizierung den Nutzer automatisiert wieder zu erkennen, ohne weitere Interaktion.

2.3.1 Merkmalextraktion

Aus den erfassten Rohdaten lassen sich per Merkmalextraktion weitere Merkmale gewinnen, die zur Beschreibung der Messreihe genutzt werden. Folgende Merkmale stehen nach der Merkmalextraktion zur Verfügung, vgl. Tabelle 2.

Tab. 2: Merkmaler nach der Merkmalsextraktion

Merkmal	Erzeugte Daten	Anzahl Merkmale	Bedeutung
Rohdaten (Koordinaten)	X,Y,Z des Gyroskops und Accelerometer	6	Ausgangsdaten der verwendeten Sensoren. Koordinaten zur Beschreibung der Beschleunigung und Ausrichtung.
Rohdaten (Zeit)	Sekunden von 0 - Ende der Authentifizierung	1	Dauer der Authentifizierung. Vom Starten der App bis zum Abschluss mit der lokalen Authentifizierung.
Diskrete Fourier Transformation (DFT)	Überführung eines zeitkontinuierlichen Signals (Rohdaten) in ein diskretes periodisches	14	Fasst man die gemessenen Daten der jeweiligen Sensoren, als Signal auf, kann man mit Hilfe der DFT weitere Erkenntnisse erlangen, indem man das nicht-periodische Signal der Sensordaten in ein periodisches transformiert. Die Diskrete Fourier Transformation wird auf alle Rohdaten angewendet und liefert auf Grund ihrer imaginären Anteile, 14 weitere Merkmale, die für die Auswertung verwendet werden können.
Pearson Korrelationskoeffizient	Koeffizient über die Rohdaten und den realen Anteil des DFT	2	Der Koeffizient wird für jede Datenreihe der Messung über die x, y und z Werte des Accelerometers und des Gyroskops, bzw. die realen Ergebnisse des DFT der jeweiligen Achse berechnet. Mittels des Korrelationskoeffizienten lässt sich der lose Zusammenhang, der durch den Verlust der Zeit entstanden ist, der einzelnen Messwerte pro Achse in Verbindung bringen.
Minima und Maxima	Max und Min für eine gesamte Messreihe pro Achse pro Sensor	12	Die Minima und Maxima sollen dazu dienen charakteristische Züge eines Nutzers zu manifestieren. Es wird davon ausgegangen, dass dies eindeutige Verhaltensweisen darstellen.
Werte-bereiche	Wertebereich für die jeweilige Achse eines Sensors	6	Aus den Minima und Maxima lässt sich anschließend der Wertebereich für die jeweilige Achse und den jeweiligen Sensor bestimmen. Auf diese Weise erhält man 6 weitere Features.
Arithmetisches Mittel	Arithmetisches Mittel für jede Achse des Sensors	6	Mit dem arithmetischen Mittelwert soll eine Verschiebung der Messwerte erfolgen. Es wird davon ausgegangen, dass der Nutzer zwar ein ähnliches Verhalten hat, die Umgebung, in der der Nutzer sein Smartphone benutzt sich aber ändern kann. Sollte sich also der Wert einer Achse verschieben, wird davon ausgegangen, dass sich dieser Wert im weiteren Verlauf der Bewegung wieder aufhebt. Wird bspw. eine stärke Auslenkung auf der X-Achse des Gyroskops bei der Bewegung in die positive Richtung ausgeführt, da z. B. die Position des Nutzers beim Authentifizierungsvorgang anders ist als üblich, wird mit einer ebenso starken Reaktion in die negative Richtung beim weiteren Verlauf der Bewegung gerechnet.

2.3.2 k-Nearest-Neighbour

Der k-Nearest-Neighbour (k-NN) Algorithmus ist ein instanzenbasiertes Verfahren und gehört zu den Lazy Learning Verfahren. Für die Verwendung muss ein Abstandsmaß für die zu klassifizierenden Daten existieren. In der hier vorliegenden Arbeit wird die Manhattan-Distanz verwendet:

$$d(a,b) = \sum_{i=1}^{n} |a_n - b_n|$$

Häufig wird beim k-NN die Euklidische Distanz verwendet:

$$d(a,b) = \sqrt{\sum_{i=1}^{n} (a_n - b_n)^2}$$

Es wurde sich aufgrund der quadratischen Komplexität der euklidischen Distanz für die Manhattan-Distanz entschieden.

Der k-NN ist ein simpler Algorithmus der auf reinem Zählen, ohne vorherige Berechnung eines Profils beruht. Der Parameter k gibt dabei die Anzahl der Nachbarn, Punkte der vorherigen Messungen, an, die benötigt werden um einen Testpunkt einer Klasse zu zuordnen [GWB+03]. Abbildung 1 zeigt beispielhaft, wie entschieden wird in welche Klasse ω der Punkt x_j fällt.

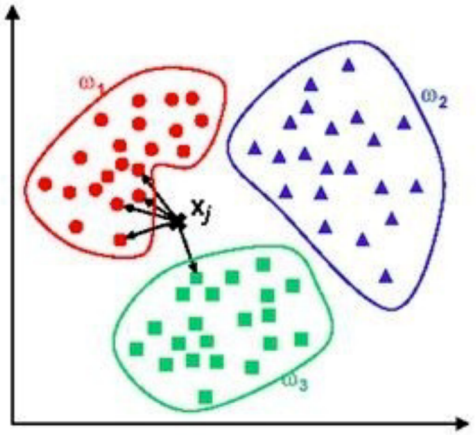

Abb. 1: Zuordnung der Testdaten zu einer Klasse mit k-NN[1]

2.3.3 Support-Vector-Machine

Support-Vector-Machine (SVM) ist ein universelles mathematisches Verfahren zur Mustererkennung. Im Wesentlichen wird SVM zur Klassifizierung von Objekten und Bildung der Klassengrenzen verwendet. SVM klassifiziert die Objekte nach bestimmten Merkmalen um sie anschließend den entsprechenden Klassen zuordnen zu können. Die dabei gebildeten Klassengrenzen haben einen möglichst weiten Abstand von allen anderen Objekten und sorgen dafür, dass auch Objekte, die nicht genau den Trainingsobjekten entsprechen, möglichst zuverlässig

[1] Mahmoud Afifi: https://www.mathworks.com/matlabcentral/fileexchange/63621-knn-classifier

klassifiziert werden. Die Punkte, die der Trennlinie am nächsten liegen, bestimmen die Lage der Trennlinie und werden als Support Vectors bezeichnet (vgl. Abbildung 2) .

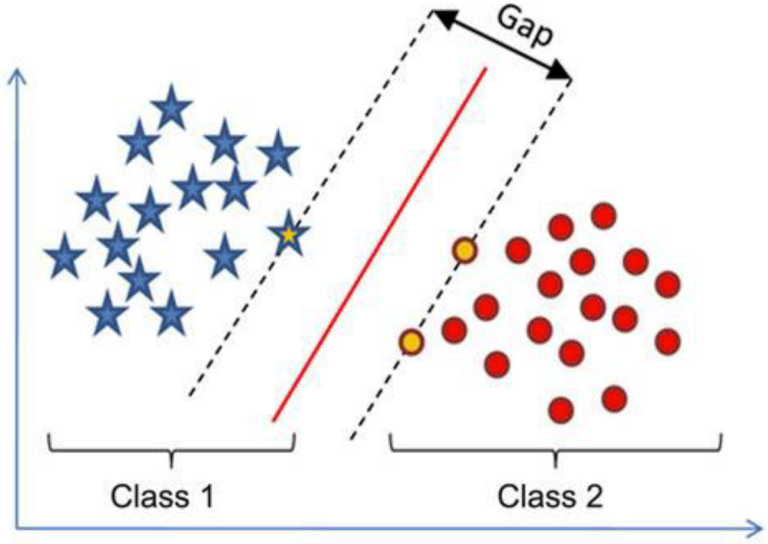

Abb. 2: Zuordnung der Testdaten zu einer Klasse mit k-NN

Befindet sich der Raum nicht im 2-dimensionalen, sondern in höheren Dimensionen, wird aus der Linie eine Hyperplane. In SVM werden Daten mit niedriger Dimension auf ein Modell mit höherer Dimension abgebildet, welches von dem SVM-Algorithmus zu lernen benutzt wird. Für die anschließende Klassifikation wendet man lineare Schätzer oder Näherungsfunktionen auf das neue Modell an. Da die linearen Schätzer bzw. die Näherungsfunktionen einfache mathematische Formeln zur Berechnung der optimalen Trennung sind, werden Fehler bei der Datenklassifizierung minimiert [Fisch7].

Eine Besonderheit des SVM ist die one-class-classifier SVM. Dabei gibt es nur eine Trainingsklasse. Der Abstand des zu testenden Punktes wird dann zwischen der aufgespannten Ebene der Lerndaten und des Nullpunktes bestimmt. Hierbei liegt der Vorteil der Anwendung des Verfahren auf nur einen Nutzerdatensatz. Damit kann die Rechenzeit verringert werden und das System kann ein Ergebnis ausgeben, auch wenn nur ein Nutzer im System enthalten ist [JeWe17].

3 Versuchsaufbau und Versuchsdurchführung

Der hier vorliegenden Arbeit liegt ein Versuchsaufbau mit einem im Einsatz befindlichen Authentifizierungssystem zu Grunde, das den zuvor beschriebenen Ablauf erfüllt [HeMP17] [HeMP15a].

Für den Versuch wurden 30 Nutzer gewählt, die jeweils 40 Authentifizierungen durchgeführt haben. Eine Authentifizierung begann mit dem Öffnen der App, gefolgt vom Scannen des QR Codes und dem Abschluss mit der Authentifizierung per Fingerprint. In der Zeit wurden auf dem Smartphone die Sensordaten vom Accelerometer und Gyroskop, mit einer Abtastrate von 25 Hz, gesammelt und mit dem Abschluss der Authentifizierung, zur Auswertung, an das Backend des Authentifizierungssystems, geschickt. Das Backend hat die Rohdaten an die Auswertungseinheit weitergeleitet, woraufhin die Merkmalsextraktion durchgeführt wurde (vgl. Abbildung 3).

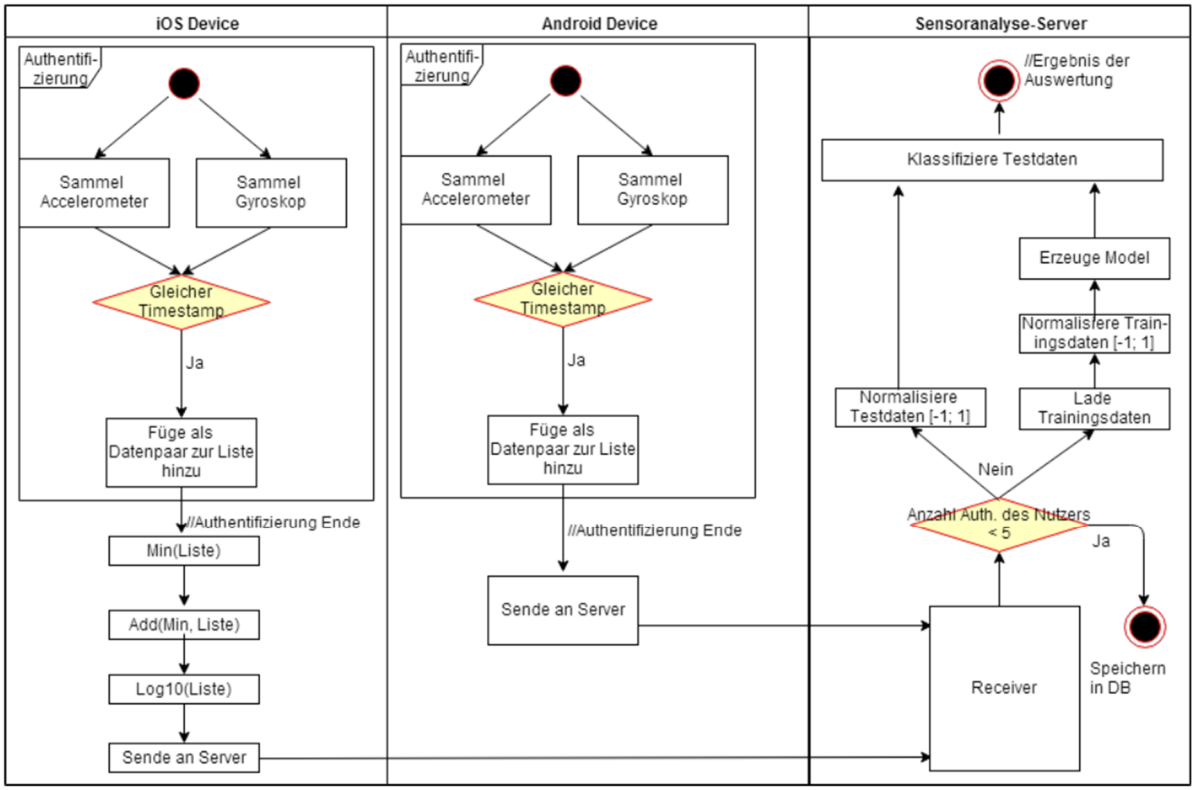

Abb. 3: Darstellung der Sensordatenverarbeitung

Das Ergebnis wurde bei erfolgreicher aktiver Authentifizierung in das Trainingsset aufgenommen.

Erste Ergebnisse wurden bei beiden Algorithmen am der 5. Authentifizierung ausgegeben. Die besten Ergebnisse wurden ab der 35. Authentifizierung erzielt. Diese Art der Durchführung ist eine Methode des Retrainings. Grundsätzlich werden vier Retrainingsverfahren unterschieden:

1. Growing Window
2. Moving Window
3. Intelligent Window
4. Adaptiv Threshold

Das eingesetzte Verfahren beschreibt das Intelligent Window. Dabei handelt es sich um eine Kombination aus Growing- und Moving Window. Bei dem Growing Window wird jede erfolgreiche Authentifizierung zum Trainingsset, bis zu einer bestimmten Größe, hinzugefügt. Während beim Moving Window, aber der erreichten Größe alte Trainingsdaten entfernt werden und die neuen genutzt werden.

Für die Durchführung mit dem k-NN wurden 46 Features verwendet (vgl. Tabelle 2). Ausgenommen wurde die Zeit, da diese stark von der Qualität des Netzwerkes beeinflusst wird. Bei dem Test mit der occ-SVM wurden nur die 6 Rohdaten der Achsen jedes Sensors zur Beschreibung des Punktes verwendet.

3.1 Ergebnis

Im Folgenden werden die Ergebnisse der jeweiligen Auswertung mit den Vor- und Nachteilen der Algorithmen beschrieben. Zu Bewertung des Algorithmus wir die Fault Acceptance Rate (FAR) und die Fault Recognition Rate (FRR) herangezogen.

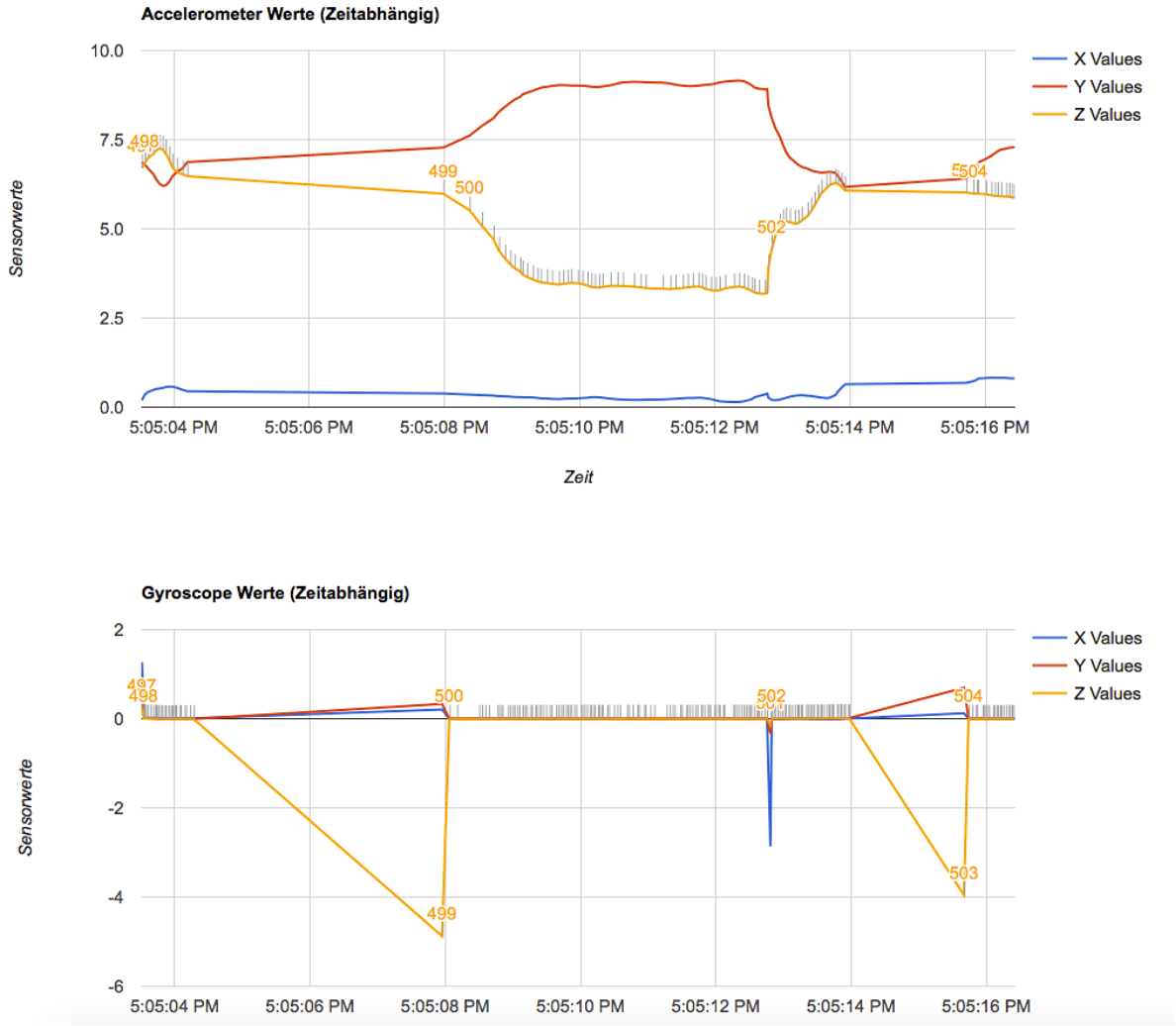

Abb. 4: Visualisierung der Accelerometer- und Gyroskopwerte einer Nutzerauthentifizierung

FAR beschreibt die fehlerhafte Anerkennung eines Angreifers als legitimen Nutzer. Die FRR beschreibt das Zurückweisen eines legitimen Nutzers, obwohl dieser Zugriffsberechtigt ist.

Daraus ergibt sich für den k-NN:

- FAR: 10%
- FRR: 0%

Für den occ-SVM resultiert:

- FAR: 20%
- FRR: 5%

Der k-NN erzielte deutliche bessere Ergebnisse als der occ-SVM. Jedoch stieg beim k-NN mit jeder Authentifizierung die Rechenzeit proportional zur Anzahl der vorhandenen Authentifizierungen. Die Laufzeit des occ-SVM war konstant und liefert erfolgreiche Ergebnisse mit einem Nutzer. Im aktuellen Versuchsaufbau lagen jedoch beide Verfahren nicht im Bereich von etablierten biometrischen Verfahren, wie beispielweise dem Fingerprint.

Aufgrund der Vorteile des occ-SVM, wurde sich für den occ-SVM entschieden, da dieser auch mit wenig Ressourcen akzeptable Ergebnisse liefert. Zum aktuellen Zeitpunkt wurde sich dazu entschieden, die Authentifizierung per Smartphone-Sensor für die Fraud-Detection zu verwenden. In der Kombination mit anderen Kontextinformationen lässt sich ein effektives Scoring zur Erkennung von Fraud errechnen. Anschließend können bei Verdacht, adaptiv, weitere Faktoren aus den Kategorien Wissen, Besitz oder Biometrie verlangt werden.

3.2 Ausblick

Der SVM Algorithmus ist stark abhängig von der Parametrisierung. Auf Basis der Daten, die weiterhin bei der Authentifizierung gesammelt werden, werden Algorithmen zum Ableiten und Optimierung der Parameter angewandt.

Eine weitere Möglichkeit ist die Verwendung von Deep Learning und Neuronal Netzen [GüWe11].

Literatur

[BaRa16] P. Baraki, V. Ramaswamy: Bio-Metric Authentication of an User using Hand Gesture Recognition. IN: International Journal of Applied Engineering Research Volume 11, Number 6 (2016) 4118-4123.

[Bart00] D. Bartmann: Benutzerauthentisierung durch Analyse des Tippverhaltens mit Hilfe einer Kombination aus statistischen und neuronalen Verfahren, München: Utz, Wiss. (2000).

[CeMC17] M. P. Centeno, A. van Moorsel, S. Castruccio: Smartphone Continuous Authentication Using Deep Learning Autoencoders (2017).

[CHCP18] M. Cagnazzo, M. Hertlein, T. Holz, N. Pohlmann: Threat Modeling for Mobile Health Systems. IN Proceedings of the Conference IoT-Health 2018: IRACON Workshop on IoT Enabling Technologies in Healthcare (IEEE WCNCW IoT-Health 2018), Barcelona (2018).

[ClLä14] J. Cleve, Jürgen, U. Lämmel: Data Mining. München: De Gruyter (2014).

[CLX+13] B. Cheng, Z. Lan, L. Xiang-Yang, H. Qiuyuan, W. Yu: SilentSense: Silent User Identification Via Touch and Movement Behavioral. IN: Biometrics. MobiCom'13 (2013).

[Do18] M. T. Do: Konzeption eines Fraud-Detection-Systems zur Aufdeck von Identitätsdiebstahl unter Verwendung von Big Data-Analysemethoden, Master Thesis, Westfälische Hochschule (2017).

[Fisch7] J. Fischer: Support Vector Machines (SVM). Ulm, Universität Ulm, Seminararbeit (2007).

[GWB+03] G. Guo, H. Wand, D. Bell, Y. Bi, K. Greer: KNN Model-Based Approach in Classification. IN: OTM 2003: On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE (2003) 986-996.

[GüWe11] D. R. Günter, K. F. Wender: Neuronale Netze. Eine Einführung in die Grundlagen, Anwendungen und Datenauswertung. 2. Aufl., Verlag Hans Huber (2011)

[Hara02] M. Hara: Method for displaying and reading information code for commercial transaction, Patent (2002).

[HeMP15a] M. Hertlein, P. Manaras, N. Pohlmann: Bring Your Own Device For Authentication (BYOD4A) – The Xign–System. IN: N. Pohlmann, H. Reimer, W. Schneider (Eds.): Proceedings of the ISSE 2015 – Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 2015, Springer Vieweg (2015).

[HeMP15b] M. Hertlein, P. Manaras, N. Pohlmann: Abschied vom Passwort – Authentifikation für ein gereiftes Internet, IN: IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag (2015).

[HeMP17] M. Hertlein, P. Manaras, N. Pohlmann: Smart Authentication, Identification and Digital Signatures as Foundation for the Next Generation of Eco Systems, IN: C. Linnhoff-Popien, R. Schneider, M. Zaddach (Eds.): Digital Marketplaces Unleashed, Springer (2017).

[Hert17] M. Hertlein: Yahoo Hack ist größer als gedacht! IN: XignSys Blog, https://blog.xignsys.com/yahoo-hack-ist-groesser-als-gedacht/ Abruf: 23.04.2018.

[JeWe17] J. Jerwan, A. Wehrhahn-Aklender: Benutzeridentifikation mit Sensoren, Seminararbeit, Westfälische Hochschule (2017).

[LWMZ16] A. Laghari, Waheed-ur-Rehman, Dr. Memon, A. Zulfiqari: Biometric Authentication Technique Using Smartphone Sensor. IN: 13th International Bhurban Conference on Applied Sciences & Technology (2016).

[MTSH18] M. Mehrnezhad, E. Toreini, S. F. Shahandashti, F. Hao: Stealing PINs via mobile sensors: actual risk versus user perception. IN: International Journal of Information Security, Volume 17 (2018) 291-313.

[SLY+16] C. Shen; Y. Li, T. Yu, S. Yuan, X. Yio, X. Guan: Motion-Sensor Behavior Analysis for Continuous Authentication on Smartphones. 12th World Congress on Intelligent Control and Automation (2016).

[Stat16a] Statista: https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/ Abruf: 24.10.2016.

[Stat16b] Statista: https://de.statista.com/statistik/daten/studie/500579/umfrage/prognose-zur-anzahl-der-smartphonenutzer-in-deutschland/ Abruf: 24.10.2016.