18. August 2020 Studie · Privatsphäre & Krypto · Mobile Sicherheit · 23 Min. Lesezeit

Privacy-Preserving Service Composition

Archiviert. Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

Quelle https://technology2.a-sit.at/veroeffentlichungen/privacy-preserving-service-compositon/

Service-Kompositionen werden durch das Zusammenspiel von Akteuren verschiedener Organisationen implementiert. Viele Kompositionssysteme verwenden eine Middleware, die die Service-Aufrufe nach festgelegten Workflows koordiniert. Diese Middlewares stellen ein bestimmtes Datenschutzproblem dar, da sie potentiell alle ausgetauschten Daten lesen können. Darüber hinaus können Service-Kompositionen erfordern, dass nur ausgewählte Teilmengen von Daten, die ursprünglich vom Benutzer bereitgestellt wurden, vorhanden sind und den empfangenden Akteuren offengelegt werden. Traditionelle Public-Key Verschlüsselung mit öffentlichen Schlüsseln ermöglicht ausschließlich die Verschlüsselung für eine bestimmte Partei während ausdrucksstärkere Zugriffskontrollen für eine effiziente One-to-Many-Kommunikation nicht möglich sind.

Neben den Anforderungen zur Wahrung der Privatsphäre kann es erforderlich sein, dass Teilnehmer an Service-Kompositionen überprüfen können, welcher Akteur während eines Prozesses Daten modifiziert oder hinzugefügt hat, um die Verantwortlichkeit der durchgeführten Aktionen sicherzustellen.

In diesem Projekt wird ein Konzept für eine effiziente, datenschutzschonende Service-Komposition vorgestellt, die eine attributbasierte Verschlüsselung in Kombination mit einer ausgelagerten Entschlüsselung sowie eine kollaborative Schlüsselverwaltung durch mehrere Akteure verwendet. Unser Konzept ermöglicht eine Ende-zu-Ende Verschlüsselung und Integrität in einer One-to-Many-Kommunikation mit fein-granularen Zugriffskontrollen bei gleichzeitiger Minimierung des Entschlüsselungsaufwands für Geräte mit geringer Rechenkapazität, wodurch Smartphones auf der Clientseite verwendet werden können. Die Machbarkeit der vorgeschlagenen Lösung wird durch einen implementierten Proof-of-Concept, einschließlich einer Performance-Evaluierung, demonstriert.

1. Einführung

Die Verwendung biometrischer Merkmale in Authentifizierungsprozessen ist mittlerweile weit verbreitet (Rui und Yan, 2019, Ahmed et al, 2017, Ferbrache, 2016) und löst traditionelle, mittlerweile als unsicher eingestufte Authentifizierungsmechanismen, wie die Eingabe eines Passworts/PIN, ab. Biometrische Authentifizierungsfaktoren beziehen sich auf physiologische eindeutige Merkmale des menschlichen Körpers, die zur Identifizierung verwendet werden können. Die Bankenbranche erkannte früh das Potential für den Einsatz biometrischer Merkmale, wie Fingerabdrücke oder Gesichtserkennung um eine sichere und benutzerfreundliche Authentifizierung für das Online-Banking zu ermöglichen. Zudem stieg auch das Interesse von Regierungen biometrische Merkmale für die Authentifizierung von Bürger*innen zu verwenden (Unar, 2014).

Mittlerweile wird die Sicherheit biometrischer Authentifizierungsmerkmale durch zahlreiche mögliche Angriffsvektoren aus verschiedenen Gründen hinterfragt. Die Probleme einer biometrischen Authentifizierung hängen mit der Natur physischer Merkmale zusammen. Zum Beispiel können Sprachaufzeichnungen für die Authentifizierung hingegen einer Spracherkennungssoftware eingesetzt werden, oder Fingerabdrücke mit anspruchsvollen 2D- oder 3D-Techniken gedruckt werden (Matsumoto et al, 2012, Ghiani et al, 2017, Cao und Jain, 2016). Die Verwendung von © A-SIT, Partner für Sicherheitsfragen gegossenen Fingerabdrücken aus Gummi wird als Fingerprint-Spoof Angriff bezeichnet. Biggio et al, 2012 haben in ihrer Arbeit darauf aufmerksam gemacht, dass 70% der Spoofing Angriffe die Sicherheit eines Fingerabdruckerkennungssystems umgehen können. Angesichts der wachsenden Angriffsmöglichkeiten auf Fingerabdrucksysteme arbeitet die Forschung derzeit intensiv an sogenannten Fingerprint Liveness Detection (FLD) Systemen, um die Echtheit eines Fingerabdrucks zu verifizieren (Ghiani et al 2017, Mura et al 2017, Marcel et al 2014). Ein FLD ist ein System, welches Angriffe auf den Fingerabdruck-Scanner durch maschinelles Lernen verhindert. Dazu werden Bilder von lebenden und gefälschten Fingern unterschieden. Zusätzlich kann durch Messen von Vitalwerten, wie z.B. der Herzschlag, eine bessere Erkennungsrate der Lebendigkeit sichergestellt werden (Chugh und Jain, 2019). Schlussfolgernd führt erst der Einsatz von FLD oder ähnlichen Detektoren zu einer hohen Sicherheit in Fingerabdruckerkennungssystemen.

Deutschland führte 2015 ein automatisiertes Grenzkontrollsystem ein, das auf einer Gesichtserkennung basiert (PASS, 2014). Die jahrzehntelange Erfahrung in der Signalverarbeitung führte zu einer besseren Genauigkeit und Zuverlässigkeit der Algorithmen und soll damit den Einsatz dieser Systeme auch für unterschiedliche Anwendungen im E-Government ermöglichen. Dennoch unterliegen Gesichtserkennungssysteme zahlreichen Anfälligkeiten im realen Einsatz. Der einfachste, aber dennoch effektive Angriffsvektor ist die simple Verwendung von Bildern einer Person, die potentiell öffentlich verfügbar sind. Diese Bilder können dann zur Herstellung von mit Silikon-Masken verwendet werden, die kostengünstig herstellbar sind (Ramachandra und Busch, 2017). Darüber hinaus, beschreibt Duc und Minh schon 2009, wie Gesichtserkennungssysteme auf Laptops gefälscht werden können. Aus diesem Grund arbeitet die Forschung derzeit intensiv an Erkennungssystemen für Angriffe auf Gesichtserkennungssysteme. Dazu werden Methoden die Bewegungen und Zwinkern der Augen oder die Reflektion des Lichtes auf der Haut berücksichtigen, in sogenannten Real-Time Liveness Detection Systeme (RT-LDS) erforscht (Pan, 2007, Pan, 2008). Die Genauigkeit moderner RT-LDS wird durch Deep Learning Algorithmen unterstützt. Deep Learning wird dazu eingesetzt, abstrakte Merkmale menschlicher Gesichter autonom zu extrahieren (Liu et al, 2019, Ito, 2019). Diese RT-LDS Systeme sind allerdings in der Praxis noch nicht weit verbreitet.

Im März 2019 führte Österreich die Smartphone App “Digitales Amt“ ein, wodurch viele behördliche Aktivitäten einfach am mobilen Geräte durchgeführt werden können. Die Authentifizierung von Bürger*innen in der Digitales-Amt App (DAA) basiert auf einer Mehrfaktor-Authentifizierung. Einen dieser Faktoren stellt der Besitz von kryptographischen Schlüsselmaterial dar, welches im Authentifizierungsprotokoll zur Identifikation einer Person eingesetzt wird. Dieses Schlüsselmaterial ist in einer sicheren Hardware des Smartphones gespeichert und kann nicht extrahiert werden. Der Zugriff auf das Schlüsselmaterial wird durch einen, lokal am Gerät verfügbaren, Zugriffsmechanismus geschützt. In der DAA kann hierfür zwischen einem Fingerabdruck-Scan oder Gesichtserkennung gewählt werden, was die Verfügbarkeit dieser lokalen modernen Authentifizierungsmethoden voraussetzt. Diese Arbeit soll Potentiale zur Steigerung der Sicherheit der DAA App durch den Einsatz von verhaltensbasierter Authentifizierung untersuchen und mögliche Gefahren und Risiken identifizieren.

2. Verhaltensbasierte Authentifizierung

Verhaltensbasierte Authentifizierung bezieht sich auf individuelle Verhaltensmuster einer Person. Dies umfasst beispielsweise die charakteristische Art und Weise wie jemand auf seiner Computertastatur schreibt, die Art, wie jemand den Touch-Screen seines Smartphones benutzt etc. Das Verhalten einer Person kann sich zeitlich verändern, weshalb verhaltensbasierte Authentifizierungsmechanismen auch tolerant gegenüber diesen Veränderungen sein müssen. Aus diesem Grund basieren verhaltensbasierte Authentifizierungsmechanismen auf Deep-Learning-Technologien, wie in Abbildung 1 dargestellt, mit denen Verhaltensänderungen von Personen berücksichtigt werden können. Deep-Learning Technologien analysieren verschiedene Interaktionssignale und aggregieren die gesammelten Daten zu einer Art “Cyber DNA“ (Chrobok, 2020). Die Verhaltensbiometrie basiert also auf dynamischen Merkmalen und nicht statischen Informationen wie biometrische Merkmale. Dies ermöglicht einen erhöhten Schutz von Authentifizierungsverfahren gegen fortgeschrittene Bedrohungen.

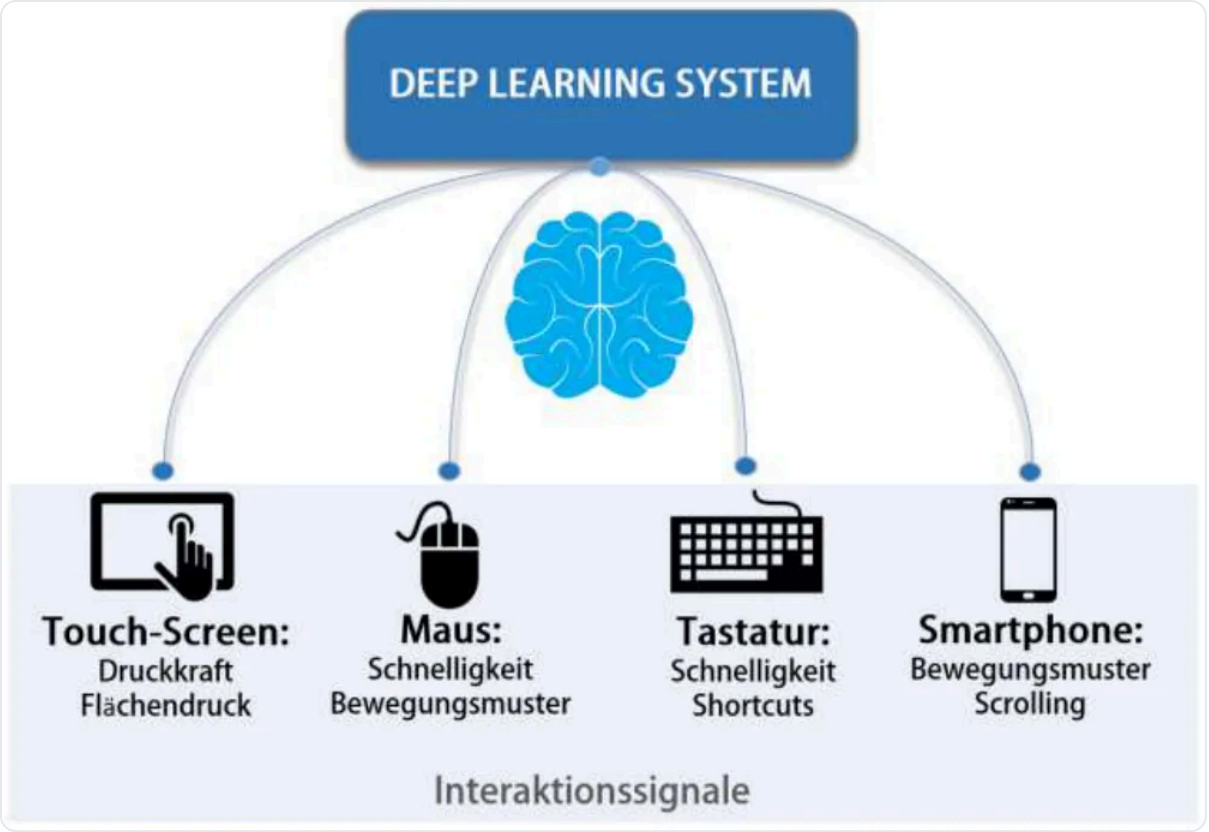


Abbildung 1: Interaktionssignale für Deep Learning Technologien verhaltensbasierter Authentifizierungssysteme

2.1 Erste Anwendung im Bankenbereich

Durch die stark steigende Nutzung von Online-Banking und der damit einhergehenden steigenden Anzahl an Betrugsangriffen finden Verfahren für eine verhaltensbasierte Authentifizierung erste Anwendungen in einigen Finanzinstituten. Hauptsächlich konzentriert sich der Schutz auf die folgenden Schutzszenarien:

- Schutz bei der Kontoeröffnung eines Kunden
- Schutz vor einer unbefugten Übernahme des Kontos
- Erkennung von Social-Engineering Betrugsfällen

Schutz bei der Kontoeröffnung eines Kunden: Im Jahr 2020 wurden 88% mehr Kreditkartenkonten und 33% mehr Bankkonten unter Identitätsdiebstahl eröffnet, was den Banken dazu veranlasst erhöhte und fortgeschrittene Sicherheitsmaßnahmen einzusetzen, die auf Machine-Learning Algorithmen basieren (Federal Trade Commission, 2021). Bspw. analysieren diese Tools das Benutzerverhalten (Navigation am Smartphone, Tippverhalten, Schnelligkeit) während der Kontoeröffnung. Die gesammelten Daten ermöglichen es Dienstanbietern zwischen legitimen Antragstellern und Kriminellen zu unterscheiden.

Schutz vor einer unbefugten Übernahme des Kontos: Angriffe, die auf eine Kontoübernahme abzielen, haben sich seit 2019 verdreifacht. Häufige Angriffsvektoren sind sogenannte Remote Access Tools (RAT), die auf die Übernahme eines Endgeräts, nach einer erfolgten Anmeldung, abzielen. Dies kann durch die Verbreitung von Banking Malware in betrügerischen Smartphone Apps realisiert werden (Stone, 2020). Hier kann eine verhaltensbasierte Authentifizierung Abhilfe verschaffen, indem Profile aus dem Verhalten von echten Benutzern und Betrügern analysiert werden. Beispielsweise werden Muster wie eine hohe

Vertrautheit mit Daten mit echten Benutzern in Verbindung gebracht, während hohe Computerkenntnisse oft mit betrügerischem Verhalten in Verbindung gebracht werden. Ein anderes Beispiel wäre die Schnelligkeit bzw. das Zögern eines Benutzers beim Abschluss einer Geldüberweisung. Social-Engineering Angriffe haben einen signifikanten Anstieg der Schnelligkeit zufolge, was darauf hindeutet, dass eine Überweisung möglicherweise unter Zwang oder unter Zeitdruck durchgeführt wird (Bleau, 2020). Verhaltensbiometrie verhindert eine Kontoübernahme somit durch einen kontinuierlichen Überwachungsprozess, der die Identität des Benutzers nicht nur durch eine einmalige Login-Funktion, sondern während der gesamten Sitzung überprüft.

Erkennung von Social-Engineering Betrugsfällen: Social-Engineering zielt auf die menschliche Psychologie ab, um Personen dazu zu bringen, wichtige Informationen freizugeben oder Transaktionen unter falschem Vorwand durchzuführen. Ein populäres Beispiel wäre ein Telefonanruf von einem Betrüger, der sich als Bankberater ausgibt und das Opfer dazu bringt, Geld zu Sicherheitszwecken auf ein anderes Konto zu überweisen. Da diese Transaktionen meistens von autorisierten Benutzern durchgeführt werden, sind diese Angriffe schwer zu identifizieren. Verhaltensbasierte Authentifizierungsmechanismen analysieren das Verhalten eines Benutzers während einer Sitzung und erkennt dabei Unterschiede zwischen freien Handlungen oder Handlungen, die unter Zwang von Kriminellen passieren (BioTech, 2020).

Alle diese Bedrohungsszenarien sind ebenso für die Digitales-Amt App (DAA) zu betrachten. Eine sichere Authentifizierung von Bürger*innen stellt die Basis für E-Government Aktivitäten dar.

2.2 Interaktionssignale für eine verhaltensbasierte Authentifzierung

Um einen adäquaten Schutz durch verhaltensbasierte Authentifizierung zu erreichen, ist es notwendig eine Vielzahl an verschiedener Daten einer Person zu sammeln, die diese charakterisieren. Patel et al. beschreiben Sensoren und Zubehör, die derzeit für moderne Smartphones zur Verfügung stehen um eine Person kontinuierlich zu authentifizieren. Alle Interaktionssignale werden in Abbildung 2 dargestellt und sinngemäß laut Patel et al. wiedergegeben:

Touch-Screen: Eines der am häufigsten verwendeten Verhaltensmerkmale ist die Berührungsdynamik am Touch-Screen eines Smartphones. Dazu zählen unter anderem Wisch- und Schreibmuster einer Person. Technische gesehen, wird während der Bedienung des Smartphones ein Vektor aus den aus den aufgezeichneten Berührungsdaten errechnet. Mit diesem Vektor wird ein diskriminativer Klassifikator zur Authentifizierung trainiert. Diskriminative Klassifikatoren werden im Machine-Learning verwendet, um Unterscheidungen verschiedener Datenklassen zu ermöglichen. Als weiteres Merkmal kann der Fingerdruck oder die Geschwindigkeit der Wisch- und Schreibgesten berücksichtigt werden.

Global Positioning System (GPS): Die GPS Funktion kann in Smartphones für die Erkennung von Bewegungsmustern und damit für die Erstellung eines Verhaltensprofils verwendet werden. Der Standort einer Person wird durch einen Längen- und Breitengrad angegeben und ermöglicht eine Klassifizierungsbewertung jedes Wertepaares mithilfe von Support Vector Machines (SVM). Bei SVM handelt es sich um ein mathematisches Verfahren zur Mustererkennung (Friedman et al., 2015).

Accelerometer und Gyroskop: Beschleinigungsmesser in Smarpthone sind notwendig um verschiedene Bewegungsarten von Personen zu klassifizieren und diese für eine kontinuierliche verhaltensbasierte Authentifizierung zu verwenden. Hierbei wird bspw. die Beschleunigung oder generell die Geschwindigkeit

einer Person beim Gehen als oder die Handhabung des Telefons als Klassifikator herangezogen. Mithilfe von gemessenen Daten durch ein Gyroskop kann zusätzlich die Ausrichtung des Telefons in der Tasche einer Person abgeschätzt werden (Mahfouz et al., 2017).

Thermometer : Mittlerweile gibt es eine Reihe von Smartphone Apps, mit denen die Temperatur eines mobilen Geräts sowohl innen, als auch außen gemessen werden kann. Die Umgebungstemperatur kann demnach als Datenquelle für eine kontinuierliche verhaltensbasierte Authentifizierung eingesetzt werden.

Apps: Schon sehr früh entstanden Ansätze zur Erstellung von Verhaltensprofilen der Benutzer zielen auf die Nutzung von Apps am mobilen Gerät ab. Hierbei werden bspw. die Anzahl der Aufrufeeiner App, der Zeitpunkt der Verwendung oder die Anwendungszeit über einen bestimmten Zeitraum gemessen und zu charakteristischen Aktivitätsprofilen zusammengefasst. In diesen Systemen werden Benutzerprofile durch die Überwachung der Benutzeraktivitäten über einen Zeitraum erstellt und mit den aktuellen Aktivitätsprofilen des Benutzers verglichen (Moreau et al., 1997).

Kamera : Die Kamera von modernen mobile Geräten bietet diverse Möglichkeiten, charakteristische Daten für eine kontinuierliche Authentifizierung einzubinden. Eine berühmte und vielseitig eingesetzte Methode ist die Gesichtserkennung. Dabei erfolgt die Analyse der Bilder in mehreren Schritten. Als erstes werden Gesichter von Personen detektiert und danach ganzheitliche lokale Merkmale extrahiert. Schließlich können diese Merkmale zur Authentifizierung zur Klassifikation verwendet werden.

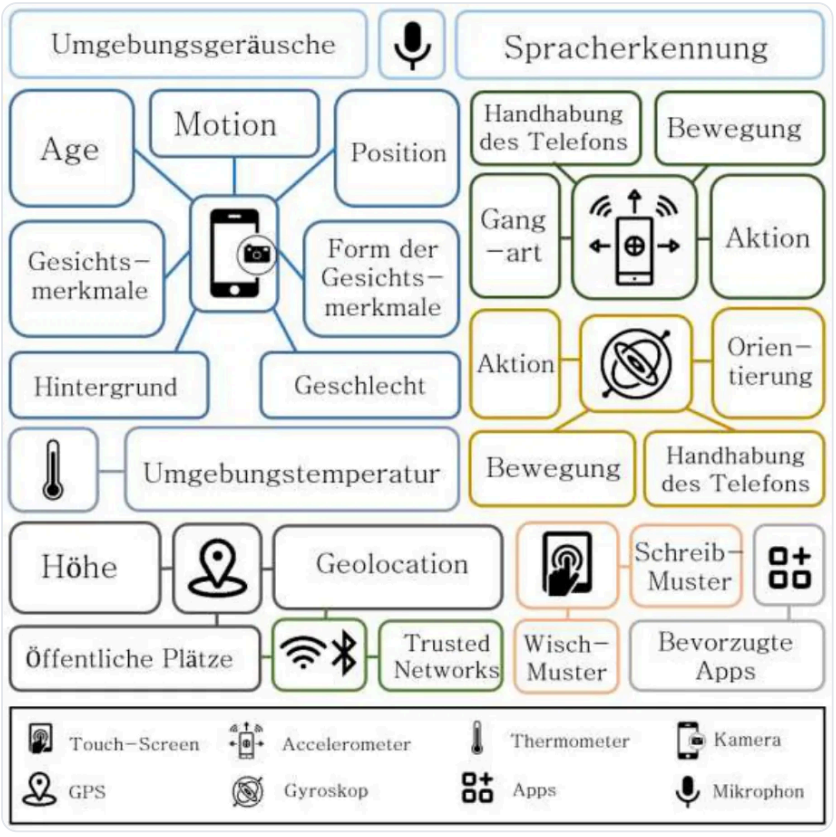


Abbildung 2: Darstellung aller möglicher Interaktionssignale am Smartphone

Mikrophon: Integrierte Mikrophone können zur Spracherkennung und Erkennung von Umgebungsgeräuschen genutzt werden, woraus charakteristische Sprachmuster einer Person erstellt werden.

3. Authentifizierung in Digitales Amt App

Die Authentifizierung von Bürger*innen in der Digitales-Amt App (DAA) basiert derzeit auf der Handy-Signatur. Bei einer erstmaligen Anmeldung in der App muss ein Benutzer das Signaturpasswort eingeben. Das Signaturpasswort dient als Authentifizierungsmittel gegenüber einem Vertrauensdiensteanbieter (VDA), der die Signaturschlüssel von Bürger*innen in speziell gesicherter Hardware verwaltet. Nur mit Angabe dieses Passworts ist eine Verwendung des Schlüsselmaterials zur Erstellung der qualifizierten Signatur möglich, was eine unautorisierte Verwendung durch bspw. den VDA selbst ausschließt.

3.1 Kryptographische Bindung zur Erhöhung der Benutzerfreundlichkeit

Aus Gründen der Benutzerfreundlichkeit des Anmeldeprozesses, wird nach einer erstmaligen Authentifizierung via Handy-Signatur (qualifizierte Signatur) ein asymmetrisches Schlüsselpaar (öffentlicher- und privater Schlüssel) in der App des Benutzers erzeugt und beim VDA registriert. Im Zuge dieser Registrierung wird ein Sicherheitszertifikat erzeugt, das den öffentlichen Schlüssel und weitere zertifikats- oder personenbezogene Daten beinhaltet und 5 Jahre gültig ist. Das Zertifikat beim VDA ist somit mit dem privaten Schlüssel im Smartphone des Benutzers verbunden, auch als kryptographische Bindung bezeichnet. Bei zukünftigen Anmeldevorgängen wird die Authentifizierung basierend auf einer Signatur durchgeführt, die mit dem privaten Schlüssel eines Benutzers erzeugt wurde. Der VDA verwendet das registrierte Zertifikat eines Benutzers um eine Signaturverifizierung durchzuführen. Nach Ablauf der Gültigkeitsdauer des Sicherheitszertifikats, muss eine erneute Authentifizierung via Handy-Signatur sowie die Registrierung von neuem Schlüsselmaterial beim VDA durchgeführt werden.

Die Verwendung des privaten Schlüssels im Smartphone des Benutzers wird durch eine lokale Authentifizierungsmethode geschützt, wodurch unautorisierte Zugriffe verhindert werden. Die DAA ermöglicht eine Identifikation per Fingerabdruck oder Gesichtserkennung. Bürger*innen müssen eine dieser beiden Authentifizierungsmethoden durchführen, um ihr Schlüsselmaterial während eines Authentifizierungsvorgangs zu verwenden. Der Signaturschlüssel ist dadurch vor unbefugten Zugriffen geschützt und in spezieller Hardware (Android: Secure Element, iOS: Secure Enclave) nicht extrahierbar gespeichert. Diese speziellen Hardware-Elemente und biometrischen Authentifizierungsmethoden sind allerdings nur in modernen Smartphones verfügbar. Eine Installation der DAA auf Geräten älterer Generationen ist daher nicht möglich.

Die DAA stellt derzeit folgende Systemanforderungen für Android- und iOS Geräte:

Col1	Betriebssystemversion	Anforderung
Android	6 oder höher	Bildschirmsperre mit Fingerabdruck muss aktiviert sein.
iOS	11 oder höher	Bildschirmsperre mit Fingerabdruck oder Face ID muss aktiviert sein.

3.2 Von biometrischer- zu verhaltensbasierter Authentifizierung

Die vereinfachte Benutzerauthentifizierung von, am VDA, registrierten Bürger*innen unter Verwendung des gebundenen Sicherheitszertifikats in der DAA basiert somit auf biometrischen Identitätsmerkmalen. Die in der Einführung erwähnten Spoofing-Angriffe auf Fingerabdrucksysteme und Gesichtserkennungssysteme zeigen, dass Angriffe unter hohem Aufwand theoretisch möglich sind. Mit moderne Smartphones können

Daten aller Interaktionssignale die in Abbildung 2 dargestellt sind gemessen werden, mit Ausnahme einer Messung der Umgebungstemperatur, da Thermometer in Smartphones nicht standardmäßig verbaut werden.

Die Erstellung von Verhaltensprofilen auf Basis der Messung diverser Interaktionssignale kann somit einen zusätzlichen Schutz der Authentifizierung durch verhaltensbasierte Merkmale einer Person, zumindest technisch gesehen, ermöglichen. Zukünftig werden auch weitere Informationen durch das Smartphone ausgewertet und gesammelt werden können. Ein Beispiel dafür wären Barometer mit einer mikrometer-dünnen Siliziummembran zur Messung des Umgebungsdrucks oder die Auswertung von Umgebungslichtsensoren bestehend aus Fotodioten sowie Näherungssensoren, die Infrarotstrahlung verwenden. Diese Entwicklung weist auf eine steigende Anzahl an Sensoren hin, die zukünftig in Smartphones integriert werden und Interaktionen mit dem Nutzer messen können (Bochkor, 2020). Das Potential verhaltensbasierter Authentifizierungsmechanismus ist damit steigend.

4. Privatsphäre in Verhaltensbasierter Authentifizierung

Die Sammlung und Klassifizierung von Daten mithilfe von Deep Learning Algorithmen erfolgt in verhaltensbasierten Authentifizierungsmechanismen durch externe Server, da Smartphones die technischen Voraussetzungen, die für die Erstellung von Benutzerprofilen notwendig sind, derzeit noch nicht bereitstellen, was durch zahlreiche Veröffentlichungen bestätigt wird (Govindarajan et al., 2013, Sun, 2015, Govindarajan et al., 2013). Der Austausch der biometrischen- oder Verhaltensmerkmale zwischen Client und Server stellt eine potentielle Gefährdung für die Privatsphäre der gesammelten Benutzerdaten dar, da diese ein attraktives Ziel für potentielle Angriffe darstellen. Folglich werden in der Forschung verschiedene Ansätze untersucht, die den Datenschutz bei verhaltensbasierten Authentifizierungsmechanismen berücksichtigen. Im Grunde werden zum Schutz der Privatsphäre fortgeschrittene kryptographische Methoden und Protokolle eingesetzt, von denen einige nachfolgend beschrieben werden.

4.1. Homomorphe Verschlüsselung

Álvarez et al., 2021 haben datenschutz-schonende, sensorbasierte kontinuierliche Authentifizierungsmethoden für die Erstellung von Benutzerprofilen untersucht. Ein möglicher Ansatz ist die Verarbeitung ausschließlich verschlüsselter Daten mithilfe von homomorpher Verschlüsselung (Fully Homomorphic Encryption). Diese besondere Verschlüsselungsart verfügt über Eigenschaften, die eine Berechnung auf verschlüsselten Daten ermöglicht, die dem Ergebnis von mathematischen Operationen auf unverschlüsselte Daten entspricht. Dadurch werden Berechnungen verschlüsselter Daten ohne Zugriff auf einen geheimen Schlüssel möglich, was den Schutz der Privatsphäre bei einer Übermittlung der Informationen an einen externen Server sicherstellt (Singh, 2014). Shahandashti et al. haben ein verhaltensbasiertes kontinuierliches Authentifizierungssystem entwickelt, das auf homomorphen Operationen basiert und den Datenschutz von personenbezogenen Daten gegenüber böswilligen Angriffen gewährleistet. Dies wird durch die Einbeziehung eines erstellten Benutzerprofils als zusätzlicher Faktor im Authentifizierungsvorgang sichergestellt. Das Benutzerprofil wird anhand des Verlaufs von Benutzeraktionen auf dem mobilen Gerät im Laufe der Zeit erstellt und auf einem externen Server gespeichert. Bei einer notwendigen Authentifizierung eines Benutzers enthält die Zugriffsanfrage (Request)

des Clients einen Vektor der jüngsten Messungen der Merkmale auf dem Client-Gerät, die im Zuge der Authentifizierung mit den gespeicherten Merkmalen am Server verglichen werden. Dieser Vergleich basiert ausschließlich auf verschlüsselten Daten, was einen adäquaten Schutz der Privatsphäre ermöglicht.

Allerdings stellt der praktische Einsatz von homomorpher Verschlüsselung aufgrund verschiedener Aspekte eine Herausforderung dar. Die Implementierung gilt als kompliziert und das Verfahren im allgemeinen als äußerst rechenintensiv. Derzeit stehen nur wenige Tools für die Implementierung von homomorpher Verschlüsselung zur Verfügung.

4.2. Euklidischer Abstand und Manhattan-Distanz

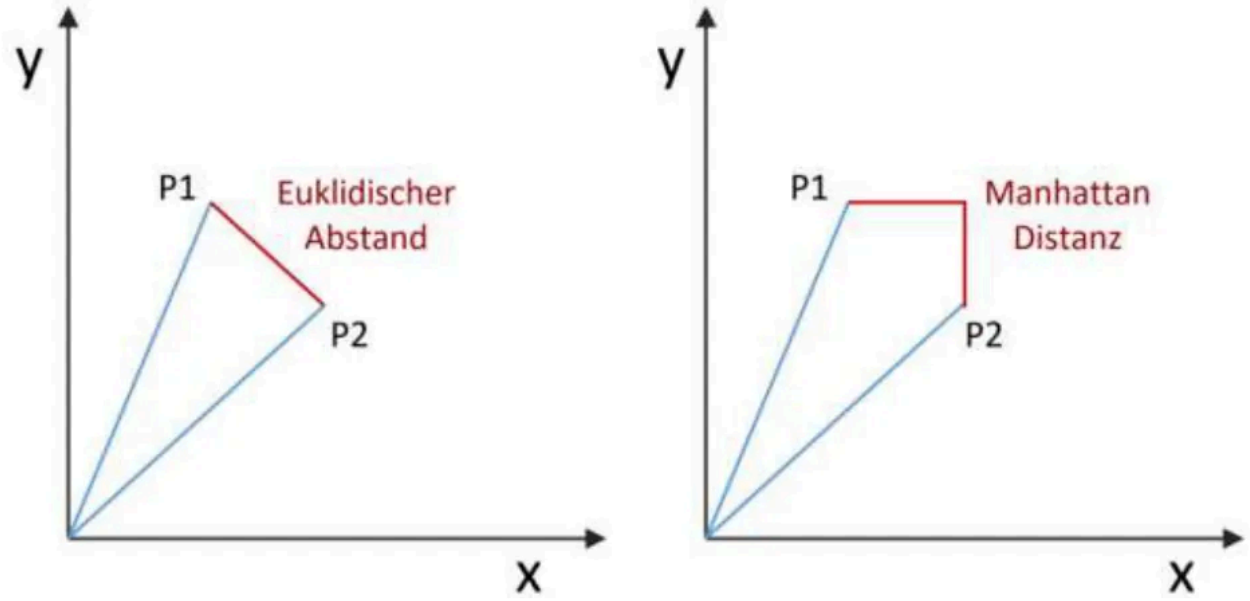
Govindarajan et al. veröffentlichten sichere Client-Server Protokolle für eine kontinuierliche Authentifizierung, basierend auf skalierten Manhattan- und euklidischen Distanzen. Die Manhattan-Distanz ist eine Metrik, die die Distanz zweier Punkte als absolute Differenz zwischen zwei Einzelkoordinaten angibt (Royer, 2001). Die Euklidische Distanz stellt die Länge eines gemessenen Abstandes dar, der zwei Punkte verbindet. Der Euklidische Abstand und die Manhattan Distanz unterscheiden sich dadurch, dass in beim Euklidischen Abstand die Länge des direkten Weges zweier Punkte angegeben wird, wie in Abbildung 4 dargestellt. Die Manhattan Distanz gibt die kürzeste Länge an, die auf der x- und y-Achse zurückgelegt werden muss, um zwei Punkte zu verbinden.

Abbildung 3: Euklidischer Abstand und Manhattan-Distanz Beispielsweise können mit diesen Metriken die Ähnlichkeit zwischen zwei Wörtern berechnet werden. Ist der Abstand gleich eins, dann haben die beiden Wörter keine gemeinsamen Buchstaben, wohingegen sich ein Abstand von 0 ergeben würde, wenn alle Buchstaben ident sind.

Der Euklidische Abstand und die Manhattan-Distanz stellen sich als besonders geeignet für verhaltensbasierte Authentifizierungsmechanismen, die auf dem Tippverhalten eines Benutzers basieren, heraus (Killourhy und Maxion, 2009). Mit ihnen wird die Fehlerquote bei der Eingabe eines Textes in Prozent gemessen. Dieser Wert wird in der Veröffentlichung von Govindarajan et al. als Equal Error Rates (EER) bezeichnet. Dieser Ansatz erweist sich als geeignetes Verfahren für Smartphones.

4.3. Datenschutz-wahrende biometrische Erkennungssysteme

Derzeit befasst sich die Forschung intensiv mit dem Schutz der Privatsphäre von Spracherkennungssystemen. Vor allem cloudbasierte Systeme zur Sprachanalyse stehen im Fokus. Diese extrahieren nützliche Informationen aus einer Sprachaufnahme mithilfe fortgeschrittener Spracherkennungstechniken. Neben dem textuellen Inhalt einer Sprachaufnahme können weitere Informationen analysiert werden, die den emotionalen Zustand einer Person beschreiben. Aus diesem Grund entwickelten Aloufi et al. ein Spracherkennungssystem, welches die Sprachaufnahme einer Person dahingehend mit Transformationsfunktionen bereinigt, bevor sie an einen externen Server gesendet werden. Ahmed et al. veröffentlichten ein Spracherkennungssystem, das neben dem Schutz der akustischen Merkmale und emotionalen Informationen einer Sprachaufnahme, auch einen Schutz der Privatsphäre hinsichtlich der textuellen Information bietet. Dieses cloudbasierte System verwendet Dienste um eine Sprachdatei zu transkribieren, nachdem eine Reihe von Vorgängen zum Schutz der Privatsphäre auf der Benutzerseite angewendet wurde.



Die Forschung beschäftigt sich außerdem intensiv mit datenschutz-wahrenden Gesichtserkennungssystemen. Mao et al. haben bspw. einen Algorithmus entwickelt, der verschiedene Schichten eines Bildes analysiert. Basierend auf diesem Algorithmus wird ein Trainingsschema für die Gesichtserkennung entwickelt, welches die Privatsphäre der Benutzer hinsichtlich ihrer biometrischen Eigenschaften berücksichtigt. Ma et al. veröffentlichten ein Gesichtserkennungssystem, das auf einem neuronalen Netzwerk basiert und die Privatsphäre der Gesichtsmerkmale einer Person und der verwendeten Lernparametern für den Machine-Learning Algorithmus schützt.

Neben der Srach- und Gesichtserkennung können auch digitalisierte Fingerabdrücke die Privatsphäre von Personen gefährden. Die meisten Ansätze basieren auf der Beifügung eines zufälligen Rauschens, das die Extraktion von privaten Merkmalen durch Angriffe verhindern soll (Tao et al. 2021). Darüber hinaus gibt es fortschrittlichere Mechanismen zum Schutz der Privatsphäre von Fingerabdrucksystemen, die auf homomorpher Verschlüsselung basieren (Taeyun et al. 2020)

4.4. Kryptographische Protokolle

Da in verhaltensbasierten Authentifizierungssystemen Daten zu Analysezwecke an externe Server gesendet werden müssen, werden verschiedene kryptographische Protokolle für die Kommunikation zwischen dem Client Gerät und dem Server eingesetzt. Álvarez et al. beschreiben die am häufigsten eingesetzten Protokolle für die Implementierung einer sicheren kontinuierlichen Authentifizierung:

- *Shamir Secret Sharing (SSS):* Bei diesem Protokoll wird eine Information in n Nachrichten zerlegt und an n Parteien gesendet. Die Teilinformationen selbst sind nutzlos, können jedoch gemeinsam mit allen anderen Teilinformationen kombiniert werden, um die ursprüngliche Information zu rekonstruieren (Alvarez und Encinas, 2008). Beispielsweise kann ein geheimer Schlüssel in mehrere Teile zerlegt und unter mehreren Akteuren verteilt werden. In verhaltensbasierten Authentifizierungssystemen könnte ein geheimer Schlüssel aus verschiedenen biologischen oder verhaltensbasierten Merkmalen bestehen. Die Kombination aller Merkmale ermöglicht die Verwendung des geheimen Schlüssels, der für eine Authentifizierung notwendig ist.

- *Secure Multiparty Computation (SMPC):* In SMPC werden Berechnungen unter Verwendung von Eingaben verschiedener Parteien durchgeführt. Jede Partei kennt dabei nur ihren eigenen Eingabewert und erhält keine Kenntnis über Eingabewerte anderer Parteien. Demnach können die Daten verschiedener Client-Geräte, die biologische oder verhaltensbasierte Merkmale sammeln, verwendet werden um unter Berücksichtigung des Datenschutzes eine Authentifizierung zu gewährleisten (Zhao et al., 2019). Auch Wearables und IoT Geräte können hierbei neben Smartphones als mögliche Client-Geräte, die Daten für eine kontinuierliche Authentifizierung liefern, in Betracht gezogen werden.

- Zero-Knowledge Proof (ZKP): Diese Protokolle ermöglichen es einer Partei, einer anderen Partei zu demonstrieren, dass sie bestimmte Informationen hat bzw. kennt, ohne die Information selbst preiszugeben. Durch den Einsatz von ZKP in verhaltensbasierten Authentifizierungssystemen ist es möglich biologische und verhaltensbasierte Merkmale ohne deren Offenlegung zu verwenden.

Goh und Ngo, 2003 demonstrieren die Nützlichkeit dieser Protokolle zum einen für die Berechnung kryptografischer Schlüssel unter Verwendung biometrischer Daten über SSS und zum anderen durch die Verwendung des ZKP-Protokolls, um die Privatsphäre der verwendeten biometrischen Merkmale zu schützen.

5. Fazit

Aktuelle Entwicklungen im Bereich der Benutzerauthentifizierung weisen auf eine deutliche Zunahme von verhaltensbasierten Erkennungssystemen hin, die auf einer kontinuierlichen Datensammlung verhaltensspezifischer Merkmale basieren. Die Bankenbranche stellt sich als Vorreiter heraus, die verhaltensbasierte Authentifizierungssysteme erstmals in den praktischen Einsatz bringt. Der zusätzliche Sicherheitsmechanismus dieser Systeme wird durch moderne Machine-Learning Algorithmen ermöglicht, die auf externen Servern oder in cloudbasierten Systemen laufen. Eine Implementierung dieser Algorithmen auf externen Servern ist notwendig, da diese teilweise kostenintensive Berechnung durchführen, die auf Smartphones derzeit noch nicht effizient durchführbar sind. Die Übermittlung der Interaktionssignale eines Benutzers mit dem Client-Gerät an einen Server stellt dabei ein zusätzliches Sicherheitsrisiko dar, da potentielle Angriffe auf einen Diebstahl privater Informationen abzielen könnten. Die Forschung beschäftigt sich intensiv mit datenschutz-wahrenden Mechanismen zur Sammlung diverser Interaktionssignale am Smartphone. Für eine gesicherte Client-Server Kommunikation werden kryptographische Protokolle entwickelt, die die Privatsphäre von Benutzerinnen sichern.

Die Digitales-Amt-App erfordert derzeit die Verwendung von Smartphones älterer Generationen, die zumindest Fingerabdruckscanner und Gesichtserkennungssysteme bereitstellen. Diese Smartphones ermöglichen die Sammlung von Daten, die aus sämtlichen Interaktionssignalen stammen, die in veröffentlichten verhaltensbasierten Systemen verwendet werden. Technisch gesehen bieten diese Client-Geräte damit die Datenbasis, die für die Entwicklung von kontinuierlichen Benutzerprofilen erforderlich ist. Allerdings gibt es momentan keine öffentlich geltenden Standards für einen gesicherten Austausch von verhaltensbasierten Merkmalen zwischen einem Client und einem Server. Viele wissenschaftliche Arbeiten bieten Vorschläge für Protokolle, die auf fortgeschrittener Kryptographie basieren. Die Entwicklung eines verhaltensbasierten Authentifizierungssystems für die Digitales-Amt App setzt damit die Kenntnis komplexer Machine-Learning Algorithmen, sowie deren korrekte Implementierung und Methoden zum Schutz der Privatsphäre von Lernparametern, für einen praktischen Einsatz voraus.

Als fortführende Forschungsarbeit ist es notwendig, geeignete Interaktionssignale zu identifizieren die in der DAA zur Erstellung eines kontinuierlichen Benutzerprofils verwendet werden können. Daneben ist ein Architekturentwurf notwendig, der den Einsatz erforderlicher Systemkomponenten des verhaltensbasierten Authentifizierungssystems und die Kommunikation aller beteiligten Akteure modelliert. Die Kommunikation zwischen einem Client-Gerät und einem Server muss durch entsprechende Privatsphäre-wahrende Mechanismen geschützt sein.

Zudem ist in der Kommunikation nach außen die entsprechende Awareness zu schaffen, dass sämtliche verhaltensbasierte Daten durch kryptografische Mechanismen anonym verarbeitet werden, da zu keinem Zeitpunkt direkte verhaltensbasierte Daten unverschlüsselt verspeichert werden und somit außerhalb des jeweiligen Kontext zu einer Identifikation der jeweiligen Person genutzt werden können.

6. Literaturverzeichnis

Ahmed Mahfouz, T. M. (2017). *A survey on behavioral biometric authentication on smartphones.* Journal of Information Security and Applications, vol. 37, pp. 28-37. B. Biggio, Z. A. (2012). *Security Evaluation of Biometric Authentication Systems under Real Spoofing Attacks .* IET Biometrics, vol. 1, no. 1, pp. 11-24. Biocatch. (2020). Von https://www.biocatch.com/blog/types-social-engineering-attacks abgerufen Bleau, H. (2020). *Biocatch* . Von https://www.biocatch.com/blog/every-click-and-swipe-tells-a-story how-digital-behavior-can-detect-account-takeover abgerufen Bochkor, O. (2020). *Sensoren in modernen Smartphones.* Busch, R. R. (2017). *Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey.* ACM Comput. Surv. 50, 1, Article 8 (April 2017), 37 pages. DOI: https://doi.org/10.1145/3038924. Chrobok, M. (2020). *Physical Biometrics vs. Behavioral Biometrics* . Von https://www.revelock.com/en/blog/physical-biometrics-vs-behavioral-biometrics abgerufen Ferbrache, D. (2016). *Passwords are broken – the future shape of biometrics.* Biometric Technology Today, Volume 2016, Issue 3, 2016, pp 5-7. G. Pan, L. S. (2007). *Eyeblink-based anti-spoofing in face recognition from a generic webcamera .* IEEE 11th International Conference on Computer Vision, pages 1–8, 2007. G. Pan, Z. W. (2008). *Liveness detection for face recognition. Recent Advances in Face Recognition.* Govindarajan, S., Gasti, P., & Balagani, K. (2013). *Secure privacy-preserving protocols for outsourcing continuous authentication of smartphone users with touch data.* Proceedings of the 2013 IEEE 6th International Conference on Biometrics: Theory, Applications. Hernández-Álvarez, L., de Fuentes, J., González-Manzano, L., & Encina, H. (2020).

SmartCAMPP—Smartphone-based Continuous Authentication leveraging Motion sensors with Privacy Preservation. Pattern Recognit. Lett. 2020. Hernández-Álvarez, L., de Fuentes, J., González-Manzano, L., & Encinas, H. (kein Datum).

SmartCAMPP—Smartphone-based Continuous Authentication leveraging Motion sensors with Privacy Preservation. Pattern Recognit. Lett. 2020. Hernández-Álvarez, L., de Fuentes, J., González-Manzano, L., & Hernández Encinas, L. (2021).

Privacy-Preserving Sensor-Based Continuous Authentication and User Profiling: A Review. Sensors 2021, 21, 92. https://doi.org/10.3390/s21010092. Jain, K. C. (2016). *Hacking mobile phones using 2D Printed Fingerprints.* Jain, T. C. (2019). *Fingerprint Presentation Attack Detection: Generalization and Efficiency .* International Conference on Biometrics (ICB), 2019, pp. 1-8, doi: 10.1109/ICB45273.2019.8987374. K. Ito, T. O. (2017). *Recent advances in biometrie security: A case study of liveness detection in face recognition.*

Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pp. 220-227. L. Fridman, S. W. (2015). *Active authentication on mobile devices via stylometry, GPS location, web browsing behavior, and application usage patterns.* IEEE Syst. J. L. Ghiani, D. A. (2017). *Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015 .* Image and Vision Computing, vol. 58, pp. 110-128. Liu S, S. Y. (2019). *An Identity Authentication Method Combining Liveness Detection and Face Recognition. Sensors. .* 19(21):4733. https://doi.org/10.3390/s19214733 . Mahfouz, A. &. (2017). *A Survey on Behavioral Biometric Authentication on Smartphones.* Journal of Information Security and Applications. 37. 28-37. 10.1016/j.jisa.2017.10.002. Network., F. T. (2021). *Consumer Sentinel Network* . Von https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf abgerufen Özlem Ege Oruç, Ç. T. (2017). *An investigation of factors that affect internet banking usage based on structural equation modelling Computers in Human Behavior.* Computers in Human Behavior, vol. 66, pp. 232-235. PASS., Easy. (2014). *EasyPASS – Grenzkontrolle einfach und schnell* . Von http://www.bundespolizei.de/DE/01Buergerservice/Automatisierte-Grenzkontrolle/EasyPass/_easyPass_anmod.html abgerufen S. Marcel, M. S. (2014). *Handbook of Biometric Anti-Spoofing.* Springer. Stone, J. (2020). *Cyberscoop* . Von https://www.cyberscoop.com/contact-tracing-hacking-security anomali/ abgerufen Sun, Y. U. (2015). *Secure and privacy preserving data processing support for active authentication.* Inf. Syst. Front. 2015, 17, 1007–1015. T. Matsumoto, H. M. (2012). *Impact of artificial gummy fingers on fingerprint systems.* Proc. SPIE, vol. 4677, pp. 275-289. Unar, J. S. (2014). *A review of biometric technology along with trends and prospects. Pattern Recognit.* 47, 2673-2688. V. M. Patel, R. C. (2016). *Continuous User Authentication on Mobile Devices: Recent progress and remaining challenges.* IEEE Signal Processing Magazine, vol. 33, no. 4, pp. 49-61, doi: 10.1109/MSP.2016.2555335. V. Mura, G. O. (2018). *LivDet 2017 Fingerprint Liveness Detection Competition 2017.* Proc. ICB, pp. 297-302. Y. Moreau, H. V. (1997). *Detection of mobile phone fraud using supervised neural networks: A first prototype.* Proc. Int. Conf. Artificial Neural Networks, pp. 1065–1070. Yan, Z. R. (2019). *A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification .* IEEE Access, vol. 7, pp. 5994-6009, doi: 10.1109/ACCESS.2018.2889996. Singh, V.K.; Dutta, M. *Analyzing Cryptographic Algorithms for Secure Cloud Network* . Int. J. Adv.

Stud. Comput. Sci. Eng. 2014, 3, 1–9. Shahandashti, S.; Safavi-Naini, R.; Safa, N. *Reconciling User Privacy and Implicit Authentication for Mobile Devices* . Comput. Secur. 2015, 53, 215–233 Alvarez, G.; Hernández Encinas, L.; Martín del Rey, A. *A multisecret sharing scheme for color images based on cellular automata.* Inf. Sci. 2008, 178, 4382–4395. Zhao, C.; Zhao, S.; Zhao, M.; Chen, Z.; Gao, C.Z.; Lif, H.; Tan, Y.A. *Secure Multi-Party Computation: Theory, practice and applications.* Inf. Sci. 2019, 476, 357–372 Goh, A.; Ngo, D. *Computation of Cryptographic Keys from Face Biometrics* . In Proceedings of the IFIP International Conference on Communications and Multimedia Security, Torino, Italy, 2–3 October 2003; pp. 1–13 Govindarajan, S.; Gasti, P.; Balagani, K. *Secure privacy-preserving protocols for outsourcing continuous authentication of smartphone users with touch data* . In Proceedings of the 2013 IEEE 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA, 29 September–2 October 2013; pp. 1–8 Christian Royer: *Simultane Optimierung von Produktionsstandorten, Produktionsmengen und Distributionsgebieten* . Utz, Wiss., München 2001, ISBN 3-8316-0042-2, S. 55 K. Killourhy and R. Maxion. *Comparing anomaly-detection algorithms for keystroke dynamics* . In DSN-09, 2009