Moderne Authentifizierungsmethoden

Malek Morad

Fachhochschule St.Pölten
St.Pölten, Österreich
malek-morad@hotmail.com

***Zusammenfassung*—Es gibt mittlerweile eine Vielzahl von Authentifizierungsmethoden, die sich stark voneinander unterscheiden können. Technische Herausforderungen forderten kreative und sichere Lösungen, wodurch neue Methoden zur Authentifizierung entwickelt wurden. Traditionelle Authentifizierungsmethoden mit Benutzernamen und Passwort sind bis heute die problematischsten und werden immer öfter gehackt. In dieser Arbeit werden diverse, und vor allem moderne, Authentifizierungsmethoden alternativ zur traditionellen Authentifizierungsart erläutert und aufgezeigt, warum diese in bestimmten Szenarien nützlich sind und wo ihre Stärken und Schwächen jeweils liegen.**

I. Einleitung

Die Wichtigkeit von Authentifizierung und Autorisierung ist in der heutigen Zeit jedem bekannt. Die Authentifizierung ist der Prozess der Identifikation von Benutzern, sei es im Internet oder innerhalb eines privaten Netzwerkes. Dazu gibt es diverse Authentifizierungsmechanismen, die zum Teil stark voneinander abweichen können und unterschiedliche Komplexitätsgrade aufweisen. Bei vielen Authentifizierungsmethoden findet innerhalb des Prozesses in einer Datenbank ein Datenabgleich statt, bei dem überprüft wird, ob die Identität eines Benutzers der Echtheit entspricht. Wie diese Überprüfung im genauen stattfindet und welche Daten verglichen werden, entscheidet die jeweilige Authentifizierungsmethode selbst [1]. In den letzten Jahrzehnten entwickelte sich die Form der Authentifizierung stark weiter. Viele technische Hürden konnten überwunden, und viele Sicherheitslücken geschlossen werden. Nachdem Zugänge gegen 1970 mithilfe von lokal gespeicherten Passwortdateien gewährt wurde, war schnell klar, dass Sicherheitslücken bei der Authentifizierung von Benutzern fatale Auswirkungen haben können [2]. Obwohl sich existierende Authentifizierungsprozesse und Methoden stark voneinander unterscheiden können, so greifen diese hauptsächlich auf drei Parameter zurück. Der erste Parameter bezieht sich auf Informationen, die der User selbst besitzt. Meist verlangt diese Form der Authentifizierung das Eingeben eines Benutzernamens und Passworts für die Identifikation der jeweiligen Person [1]. Der zweite Parameter bezieht sich auf Identifikationstools oder einer Identifikationsinformation im Besitz des zu authentifizierenden Users, wie beispielsweise ein Token, ein Cookie, oder ein physisches Gerät [3]. Die Charakteristik eines Benutzers stellt den dritten Parameter dar, den sich neuerlich Systeme zur Authentifizierung zunutze machen können. Mithilfe der Benutzercharakteristik, oder auch oft Qualifikation des Benutzers genannt, kann der jeweilige Benutzer innerhalb eines Systems passwortlos identifiziert werden. Hierbei zählen unter anderem die Gesichtserkennung, Gestenerkennung und der Scan des Fingerabdrucks, sprich Biometrische Detektion [2], [3]. Diese Parameter können beliebig kombiniert werden, um eine stärkere, multifaktorielle Authentifizierung möglich zu machen. In dieser Arbeit werden zunächst gängige Authentifizierungsmethoden inklusive ihrer Stärken und Schwächen erläutert, um Verständnis zu schaffen und Unterschiede zu modernen Methoden aufzeigen zu können. Anschließend werden moderne Authentifizierungsmodelle, ebenfalls jeweils mit ihren Stärken und Schwächen präsentiert.

II. Authentifizierung mit Passwort

Das wohl bekannteste Authentifizierungsmodell ist das traditionelle Authentifizieren mit einem Passwort, das nur dem Benutzer selbst bekannt ist. Bei dieser Methode existieren unterschiedliche Sicherheitsstufen, die abhängig von der Stärke des Passworts sind. Die Stärke des Passworts wird wiederum von unterschiedlichen Faktoren beeinflusst. Ein Beispiel für ein starkes Passwort ist jenes, welches Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen nutzt und eine gewisse Länge vorweisen kann [1]. Diese Methode der Authentifizierung ist weit verbreitet und meist zusätzlich zu anderen Authentifizierungsarten als Option verfügbar, bietet aber aufgrund der relativ schnellen Hackbarkeit eine geringe Sicherheit [4]. Zusätzlich zum Passwort wird eine Referenz benötigt, die meist entweder aus einer beliebigen Kombination aus Buchstaben und Zahlen oder der E-Mail des Benutzers besteht. Diese Referenz wird in der Datenbank genutzt, um während des Authentifizierungsprozesses das eingetippte Passwort des Benutzers zu validieren [4].

A. Nachteile und Schwächen

Um die Lesbarkeit eines Passworts zu schützen, wird das Passwort, bevor es in die Datenbank gespeichert wird, unter anderem durch einen von verschiedenen Algorithmen in eine Zeichenkette umgewandelt. Diesen Prozess nennt man auch „Hashen“ [2]. Das Problem mit dieser Methode ist, dass Hacker dieses Passwort theoretisch wieder in seine eigentlichen Werte umwandeln können, auch wenn es je nach Passwortstärke äußerst zeitintensiv sein kann [5]. Abgesehen davon, muss sich der Benutzer sein Passwort merken und bei einer Sicherheitslücke sind eventuell weitere Bereiche gefährdet, wenn dieser Benutzer dasselbe Passwort mehrfach verwendet hat [6].

B. Vorteile und Stärken

Die relativ simple Implementierung und Handhabung dieser Authentifizierungsmethode macht dieses Modell beliebt und weitverbreitet. Grundsätzlich wird dazu nur eine Methode zum „Hashen“, Validieren und ein Datensatz in

der Datenbank benötigt. Das simplifiziert diesen Authentifizierungsprozess nicht nur für den Programmierer, sondern auch für den Benutzer, da das Identifizieren an einer zentralen Stelle ohne weitere Faktoren erledigt werden kann [5].

III. Passwortlose Authentifizierung

Die Hackerangriffe auf Authentifizierungsmethoden mit Passwörtern nehmen seit Jahren konstant zu und bilden somit weiterhin ein ernstzunehmendes Problem [7]. Alternativ zur klassischen Authentifizierung mit Benutzernamen und Passwort gibt es mittlerweile eine Vielzahl von neuen, innovativen und sichereren Methoden zur Authentifizierung von Benutzern. Die sogenannten „Passwordless“ Authentifizierungsmethoden erlauben das passwortlose Identifizieren in Applikationen und Webanwendungen [6]. Beispiele für Passwortlose Authentifizierungsmöglichkeiten ist die Authentifizierung durch „Single Sign-On“ (SSO), „Magic Link“ und einmalige Codes [7]. In diesem Kapitel werden diese unterschiedlichen passwortlosen Authentifizierungsmethoden erläutert und auch hier wieder die Stärken und Schwächen dieser beschrieben.

A. *Single Sign-On*

Single Sign-On ist ein Authentifizierungssystem, das es Benutzern ermöglicht, sich mit nur einem Passwort für verschiedene Anwendungen und Websites sicher zu authentifizieren. Somit müssen sich Benutzer nur einmal bei ihrem Konto anmelden, um Zugang zu allen Anwendungen zu erhalten [2]. SSO basiert auf einer Vertrauensvereinbarung zwischen einem Dienstanbieter und einem Identitätsanbieter. In der Regel basiert diese Vertrauensvereinbarung auf einem Zertifikat, das zwischen dem Identitätsanbieter und dem Dienstanbieter ausgetauscht wird [8]. Ein bekanntes Beispiel ist Google, wo man sich bei Gmail anmelden kann und Zugriff auf alle Google Drive-Anwendungen hat. Wenn ein Nutzer beispielsweise versucht, Google Forms zu verwenden und dieser bereits angemeldet ist, sendet Google eine Anfrage an den Google Forms Dienst, der wiederum einen Authentifizierungsdienst aufruft. Dieser Authentifizierungsdienst stellt sicher, ob dieser Benutzer auch tatsächlich angemeldet ist. Ist er das nicht, so wird dieser zu einem Anmeldebildschirm weitergeleitet, um seine Identität zu überprüfen [2]. Vorteilhaft an dieser Authentifizierungsmethode ist der vereinfachte Benutzerzugriff auf Anwendungen und der reduzierte Aufwand durch das Wegfallen mehrerer Passwörter. Nachteilig an dieser Authentifizierung ist wiederum die Verwendung eines einzigen Passworts für die Feststellung der Identität bei mehreren Anwendungen [8].

B. *Magic Link*

Ziel und Zweck dieses Authentifizierungssystems ist es, dem Benutzer die Eingabe und das Merken eines Passwortes zu ersparen. In solch einem System muss der Benutzer nur eine E-Mail-Adresse eingeben, um sich anzumelden [9]. Diese angegebene Adresse wird benutzt, um einen Identifizierungsschlüssel für eine nachträgliche Referenz zu generieren [8]. Eine E-Mail mit einem eindeutigen Link (dem so genannten "Magic Link"), der als Token verwendet werden kann, wird dann an die angegebene Adresse geschickt. Mit diesem Link kann sich der Nutzer durch Anklicken des Links authentifizieren [9]. Vorteil dieser Authentifizierungsmethode ist die gute Benutzerfreundlichkeit, da die Benutzer auf unterschiedlichen Geräten den Link öffnen können und sich keine Passwörter merken müssen oder vergessen können. Problematisch kann jedoch das Versenden und Erhalten der E-Mails sein, da diese aus den verschiedensten Gründen fehlschlagen, zurückgewiesen, abgefangen und somit einfach missbraucht werden könnten [8].

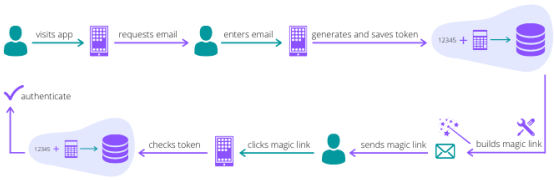

Abbildung 1 Magic link Authentifizierungsfluss [10]

IV. Benutzercharakteristische Authentifizierung

Biometrische Daten wurden bereits relative früh von Behörden traditionell für die Zugangsverwaltung im militärischen Bereich sowie für die Authentifizierung im straf- oder zivilrechtlichen Bereich eingesetzt, beides unter strenger rechtlicher und technischer Überwachung. Heute zeigen Unternehmen wie Banken, Online-Shopping und Einzelhandel eine starke Nachfrage diesbezüglich. Vor allem öffnen immer mehr Mobilfunknutzer ihre Telefone mit einem Fingerabdruck oder einem Gesicht-Scan, was in den letzten Jahren zu einem Anstieg der Anerkennung und Akzeptanz dieser Authentifizierungsmethode geführt hat [10]. Biometrische, bzw. benutzercharakteristische Daten basieren auf die einzigartigen Eigenschaften der jeweiligen Benutzer und sind daher individuell auf diesen zugeschnitten. Dadurch bietet diese Form der Authentifizierung einen hochgradig personalisierten und sicheren Authentifizierungsmechanismus [2]. Hierbei

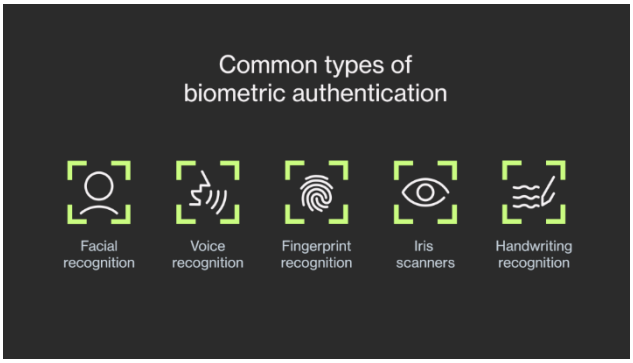

Abbildung 2 Übersicht über gängige Biometrische Authentifizierungsmethoden [16]

zählen unter anderem Fingerabdruck, Gesichtserkennung, Iris-Scan, Handgeometrie, Retina-Scan und ähnliches zur physiologischen Biometrie. Auf der anderen Seite umfasst die Verhaltensbiometrie unter anderem Stimmerkennung, Gangbild, Unterschriftenscan und Tastendruck-Scan [1]. Biometrische Authentifizierungsmethoden haben generell folgende Stärken:

- Befreit den Benutzer von der Aufgabe, sich Passwörter merken zu müssen.

- Biometrische Authentifizierungsmechanismen sind deutlich sicherer, da biometrische Merkmale nicht verloren gehen und sehr schwer zu fälschen sind.
- Die meisten biometrischen Authentifizierungsmethoden sind sehr genau [1].

Ein generelles Problem besteht bei biometrischer Authentifizierung weiterhin bezüglich des Datenschutzes aufgrund der Aufbewahrung dieser Daten. Abgesehen davon, wird zur Validierung dieser biometrischen Daten oft zusätzliche der Zugriff auf Hardware wie Kamera, Scanner und andere Geräte benötigt [10].

A. Fingerabdruck

Die gebräuchlichste biometrische Authentifizierungsmethode ist der Scan des Fingerabdrucks. Der Fingerabdruckscanner identifiziert das Bild auf dem Finger des Benutzers und gleicht es dann mit den Daten in der Datenbank ab. Jeder Benutzer hat unterschiedliche Merkmale des Fingermusters. Wenn das Fingerabdruckmuster des Benutzers in der Datenbank gespeichert ist, wandelt das System es in binäre Daten um [1]. Der Prozess des Fingerabdruckscans wurde über die Jahrzehnte immer wieder verbessert und wird in mehreren Schritten umgesetzt, die je nach Algorithmus unterschiedliche Reihenfolgen haben können [11].

Als ersten Schritt müssen die eingefangenen Fotos vom Fingerabdruck für weitere Aufgaben im Gesamtprozess vorbereitet werden. Diese Vorbereitung umfassen das Anpassen der Ausrichtung der gescannten Fotos an die Ausrichtung der in der Datenbank gespeicherten Fotos. Abgesehen davon müssen einige weitere Zwischenschritte getätigt werden, wie beispielsweise Rauschentfernung. Diese Vorverarbeitungsschritte werden durchgeführt, um eine ausreichende Genauigkeit des Endergebnisses zu erreichen [11].

In einem weiteren Schritt findet eine sogenannte „Ausdünnung“ statt, bei dem versucht wird, das eingescannte Bild, um gewisse Nachbarpixel mit minimalem Verlust zu reduzieren. Dieser Schritt vereinfacht in weiterer Folge die Extraktion von Merkmalen des Bildes [12].

Bevor der eingescannte Fingerabdruck mit dem in der Datenbank befindlichen Bildes für die Identitätsüberprüfung abgeglichen werden kann, muss vorerst die Extraktion der Merkmale stattfinden. Dieser Prozess gilt als der Schwerpunkt des gesamten Systems und ist weitgehend von der Vorverarbeitung und Ausdünnung abhängig. Er wird auch als empfindlich angesehen und soll Minutienmerkmale extrahieren. Minutien sind definiert als die Schlüsselpunkte in jedem Fingerabdruckbild und werden sowohl aus dem Originalbild als auch aus den Datensätzen ausgewählt, die eine Reihe übereinstimmender Punkte liefert [11].

Der letzte Schritt umfasst grundsätzlich das Abgleichen des eingescannten und bearbeiteten Fingerabdruckbildes mit dem Bild aus der Datenbank für die endgültige Authentifizierung des Benutzers. Bei diesem Prozess gibt es wiederum unterschiedliche Methoden, die in dieser Arbeit jedoch nicht weiter erläutert werden, um den Rahmen dieser Arbeit nicht zu sprengen [12].

B. Gesichtserkennung

Während und nach der Covid-19-Pandemie hat sich die Gesichtserkennung aufgrund der kontaktlosen Authentifizierungsmethode als potenzielle biometrische Erkennungsmethode herauskristallisiert. Die meisten Organisationen, die kontaktbasierte biometrische Systeme wie z. B. Fingerabdrücke verwendet haben, entschieden sich während der Covid-19-Pandemie dafür, diese nicht mehr für die tägliche Anwesenheitskontrolle einzusetzen [13]. Die Technologie der Gesichtserkennung erstellt Gesichtsabdrücke, indem sie Hunderte von unterschiedlichen Maßen einer zugelassenen Maske mit dem Gesicht einer Person vergleicht, die sich Zugang verschaffen will. Wie bei der Fingerabdruckerkennung wird der Zutritt gewährt, wenn genügend Maße eines Benutzers mit dem autorisierten Gesicht übereinstimmen. Die Gesichtserkennung wurde bei einer Vielzahl von Smartphones und anderen gängigen Produkten eingesetzt, kann aber ungenau sein, wenn Gesichter aus verschiedenen Blickwinkeln betrachtet werden oder wenn versucht wird, zwischen Personen zu unterscheiden, die sich ähnlichsehen, wie z. B. nahe Verwandte [10]. Ähnlich wie beim Fingerabdruckscan findet auch hier erst eine Vorverarbeitung und Filterung statt, bevor Merkmale aus dem Bild extrahiert und mit dem Bild aus der Datenbank verglichen werden können [13].

Vorteil dieser Authentifizierungsmethode ist die breite Verfügbarkeit der dazu benötigten Hard- und Software für die Gesichtserkennung. Die meisten Mobilgeräte sind mit Kameras ausgestattet, müssen kaum konfiguriert werden und besitzen oft bereits die für die Gesichtserkennung benötigten Funktionen. Auf der anderen Seite sind Gesichtserkennungsalgorithmen nicht trivial und weisen daher auch unterschiedlich große Erfolge bei unterschiedlichen Anbietern vor. Beispielsweise sind Drittanbieter oder proprietäre Implementierungen oft erfolgreicher als geräteeigene Lösungen [10].

C. Stimmenerkennung

Die Stimmauthentifizierung benötigt keine speziellen biometrischen Geräte, wie Fingerscanner oder Gesichtserkennung. Die Sprache einer Person ist das gleiche eindeutige Identifikationsmerkmal wie ihr Gesicht, oder ihre Fingerabdrücke [14]. Mit Hilfe von Stimmerkennungstechnologien können die stimmlichen Merkmale unterschieden werden. Diese Merkmale dienen als Informationen über den Benutzer und werden genutzt, um ein Stimmprofil zu erstellen, das ähnlich wie bei Gesichtsscannern in eine Datenbank gespeichert werden kann. Stimmerkennungssysteme zeichnen sich dadurch aus, dass sie den Mund und die Kehle eines Sprechers bewerten und analysieren, um einzigartige Klangeigenschaften zu erzeugen, anstatt einer Stimme "zuzuhören". Diese Methode beseitigt die Gefahren, die mit dem Versuch verbunden sind, einen Klang zu verbergen oder zu imitieren, sowie allgemeine Faktoren wie Unwohlsein oder Tageszeit, die die akustischen

Eigenschaften einer Stimme für das Ohr einer Person verändern können [10]. Stimmenerkennungssysteme sind jedoch stark von der Umgebung des Nutzers abhängig, wodurch die Genauigkeit dieser Systeme durch Veränderung der Stimme durch Krankheit oder Altersunterschied als auch laute Umgebungsgeräusche [14].

D. Augenscanner

Im Handel sind verschiedene Arten von Augenscannern erhältlich, z. B. Iris-Scanner und Retina-Scanner. Retina-Scanner arbeiten, indem sie ein blendendes Licht durch die Augen reflektieren, wodurch auffällige Gefäßformen entstehen, die vom Scanner gelesen und mit akzeptierten, in einer Datenbank gespeicherten Daten abgeglichen werden können [14]. Eine weitere Methode der Augenerkennung ist ein biometrischer Identifikator, der ein Bild der Iris aufnimmt. Diese Methode analysiert Daten aus diesem Bild und entwickelt daraus individuelle Muster. Die Technik umfasst die Identifizierung der Grenzen, der Form und der Kontur der Iris sowie die Ermittlung der Position der Pupille [2]. Dieses komplexe Muster kann sich um eine Kombination spezifischer Merkmale handeln. Diese Kombination wird dazu genutzt, um eine Zusammenfassung von Merkmalen zu erstellen [15]. Um bei der Authentifizierung das richtige Bild aus der Datenbank zu finden, ist eine sehr hochauflösende Kamera erforderlich. Moderne Kameras, die für die Iriserkennung verwendet werden, beleuchten die Iris mit Infrarot (IR). Die Netzhautanalyse ist eine weitere Technik der Augenerkennung. Bei diesem Verfahren werden die Blutgefäße im hinteren Teil des Auges erfasst und analysiert. In einem Hochsicherheitskontext gilt die Netzhautabtastung als eine der effizientesten und robustesten Methoden zur Authentifizierung von Benutzern, allerdings ist sie mit hohen Kosten verbunden [2]. Beide Arten von Augenscannern eignen sich gut für eine freihändige Überprüfung und können in einigen Fällen genauso schnell und präzise sein wie die Gesichtserkennung. Andererseits können sie aber auch ungenau sein, wenn die Personen Kontaktlinsen oder eine Brille tragen. Auch ist es bekannt, dass Fotos die Augenscanner täuschen können [10].

V. Fazit

Mit moderner Technologie und kreativer Lösungsansätze konnten bisher eine Vielzahl von neuer Authentifizierungsmethoden implementiert und verbessert werden. Traditionelle Authentifizierungsmethoden wie das eingeben eines Benutzernamens und eines Passworts weisen grobe Sicherheitslücken auf und werden immer öfter gehackt. Auf der anderen Seite scheinen biometrische Authentifizierungssysteme vielversprechend und schnell zu sein. Beispielsweise weisen Fingerabdruckscanner eine relativ hohe Sicherheit, gute Benutzerfreundlichkeit und wenige Nachteile auf. Aufgrund dieser Tatsachen und den aktuellen Entwicklungen haben diese Authentifizierungsmodelle ein hohes Potenzial.

VI. Literatur

[1] N. A. Lal, S. Prasad, and M. Farik, “A Review Of Authentication Methods,” vol. 5, no. 11, p. 4, 2016.

[2] “Modern Authentication Methods: A Comprehensive Survey.” https://www.intechopen.com/journals/1/articles/100 (accessed Nov. 13, 2022).

[3] S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and J.-J. Schwartzmann, “A Review on Authentication Methods,” *Aust. J. Basic Appl. Sci.*, vol. 7, no. 5, pp. 95–107, Mar. 2013.

[4] L. Dostalek and J. Safarik, “Strong password authentication with AKA authentication mechanism,” in *2017 International Conference on Applied Electronics (AE)*, Sep. 2017, pp. 1–6. doi: 10.23919/AE.2017.8053581.

[5] S. Biswas and S. Biswas, “Password security system with 2-way authentication,” in *2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, Nov. 2017, pp. 349–353. doi: 10.1109/ICRCICN.2017.8234533.

[6] M. Morii *et al.*, “Research on Integrated Authentication Using Passwordless Authentication Method,” in *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Jul. 2017, vol. 1, pp. 682–685. doi: 10.1109/COMPSAC.2017.198.

[7] I. Gordin, A. Graur, S. Vlad, and C. I. Adomniței, “Moving forward passwordless authentication: challenges and implementations for the private cloud,” in *2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Nov. 2021, pp. 1–5. doi: 10.1109/RoEduNet54112.2021.9638271.

[8] “A guide to magic links: how they work and why you should use them — WorkOS.” https://workos.com/blog/a-guide-to-magic-links (accessed Nov. 13, 2022).

[9] I. Matiushin and V. Korkhov, “PASSWORDLESS AUTHENTICATION USING MAGIC LINK TECHNOLOGY,” in *9th International Conference “Distributed Computing and Grid Technologies in Science and Education,”* Dec. 2021, pp. 434–438. doi: 10.54546/MLIT.2021.89.13.001.

[10] V. Parmar, H. A. Sanghvi, R. H. Patel, and A. S. Pandya, “A Comprehensive Study on Passwordless Authentication,” in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Apr. 2022, pp. 1266–1275. doi: 10.1109/ICSCDS53736.2022.9760934.

[11] S. Hemalatha, “A systematic review on Fingerprint based Biometric Authentication System,” in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, Feb. 2020, pp. 1–4. doi: 10.1109/ic-ETITE47903.2020.342.

[12] G. Aguilar, G. Sanchez, K. Toscano, M. Salinas, M. Nakano, and H. Perez, “Fingerprint Recognition,”

in *Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, Jul. 2007, pp. 32–32. doi: 10.1109/ICIMP.2007.18.

[13] M. Vasanthi and K. Seetharaman, “Facial image recognition for biometric authentication systems using a combination of geometrical feature points and low-level visual features,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 7, pp. 4109–4121, Jul. 2022, doi: 10.1016/j.jksuci.2020.11.028.

[14] S. V. Melnik and N. I. Smirnov, “Voice Authentication System for Cloud Network,” in *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*, Mar. 2019, pp. 1–4. doi: 10.1109/SOSG.2019.8706794.

[15] D. Bhattacharyya, R. Ranjan, F. Alisherov, and C. Minkyu, “Biometric Authentication: A Review,” *Int. J. U- E- Serv. Sci. Technol.*, vol. 2, Sep. 2009.