VILNIUS UNIVERSITY
FACULTY OF MATHEMATICS AND INFORMATICS
INSTITUTE OF COMPUTER SCIENCE
DEPARTMENT OF COMPUTATIONAL AND DATA MODELING

Term project for informational security management course

Biometric authentication

Done by:

Kazimieras Vitkus

Vilnius
2024

Contents

Introduction

In today's digital world, where personal information is increasingly stored and accessed online, ensuring the security of our digital identities has become a paramount concern. Traditional methods of authentication, such as passwords and PINs, are no longer sufficient to protect sensitive data from unauthorized access. As a result, there is a growing need for more robust and reliable authentication mechanisms.

Biometric authentication has emerged as a promising solution to this challenge. By leveraging unique physical or behavioral characteristics of individuals, such as fingerprints, facial features, or voice patterns, biometric authentication offers a higher level of security and convenience compared to traditional methods. It provides a more personalized and reliable way to verify the identity of individuals, making it harder for impostors to gain unauthorized access.

This essay aims to explore the concept of biometric authentication and its potential to enhance security in the digital age. We will delve into the various biometric modalities, their strengths and limitations, and the challenges associated with their implementation. Additionally, we will discuss the ethical and privacy considerations surrounding biometric authentication, as well as its implications for the future of cybersecurity.

1 Understanding biometric authentication

Biometric authentication in means of cybersecurity is a process that verifies users identity by evaluating their unique physical or behavioral features. Biometric authentication typically is more secure and reliable than traditional methods of authentication.

General trend for biometric authentication market share growth is exponential. According to Markets and Markets report[1] biometric system market is on trend to double by year 2027. According to the report, main driver for this growth is increasing use of biometric technology in consumer electronics for authentication and identification purposes. Also, huge driver for biometric authentication popularity was COVID-19 pandemic, which increased demand for contactless authentication methods. Moreover, biometric authentication is getting integrations with various machine learning (ML) and artificial intelligence (AI) models[2]. As a result, systems are becoming more accurate and reliable.

1.1 Types of biometric systems

As an alterantive to standard password authentication, these are the most popular biometric based alterantives.

Fingerprint Recognition: Arguably the most familiar form of biometric authentication, fingerprint recognition relies on capturing and analyzing the unique patterns present in an individual's fingerprints. Widely used in smartphones, laptops, and access control systems, fingerprint recognition offers a balance of security and user convenience. However, concerns about spoofing and privacy have led to advancements in this technology, such as the incorporation of liveness detection.

Facial Recognition: The advent of facial recognition technology has sparked both excitement and controversy. By analyzing facial features such as the distance between the eyes, nose, and mouth, facial recognition systems can accurately identify individuals. From unlocking smartphones to enhancing surveillance systems, this technology offers unparalleled convenience. Nevertheless, ethical debates surrounding privacy invasion and potential biases in algorithmic decision-making underscore the need for responsible deployment and regulation.

Iris Recognition: Delving deeper into the realm of biometrics, iris recognition stands out for its accuracy and reliability. By capturing the intricate patterns of the iris, which are unique to each individual, this technology offers robust authentication. Commonly used in high-security environments such as border control and government facilities, iris recognition boasts low false acceptance rates. However, concerns about user acceptance, cost, and environmental factors such as lighting conditions pose challenges to widespread adoption.

Voice Recognition: The human voice, with its distinct pitch, tone, and cadence, serves as a powerful biometric identifier. Voice recognition technology analyzes these vocal characteristics to verify the identity of individuals. From call centers to smart home devices, voice authentication offers a seamless user experience. Nevertheless, factors such as background noise, variations in speech patterns, and the potential for voice recordings raise concerns about security and reliability.

Behavioral Biometrics: Beyond physical traits, behavioral biometrics focus on unique patterns in human behavior. This includes typing rhythm, mouse movements, and even gait analysis. By analyzing these behavioral cues, authentication systems can passively verify users without requiring explicit actions. While behavioral biometrics offer continuous authentication and resistance to spoofing, concerns about user privacy and the need for transparent consent mechanisms loom large.

There are even more specialized biometric metrics that can be used for authentication , such as retinal scans, hand geometry analysis, scent identification, finger vein scanning, thermodynamic biometric matching, gait identification, keystroke matching, ear shape analysis, signature confirmation.

1.2 But how does biometric authentication work?

The process of authentication independantly on type of biometric system is quite similar. The first stop on authentication roadmap is to map out the data of the selected biometric trait. Eligible biometric traits involve several different parts of the human body, such as fingerprints, iris, voice, gait, facial features, DNA and many more features.

Enrollment process is the first step in biometric authentication. Before authentication method can be employed, the user firstly must enroll their biometric data into a secure system. During this process, a user's biometric traits are captured and converted into digital templates using specialized hardware such as fingerprint scanners, iris scanners, or cameras. For instance, in fingerprint authentication, the unique ridges and patterns of a person's fingerprint are scanned and converted into a mathematical algorithm that represents the fingerprint's unique characteristics. This algorithm is then securely stored in a database for future comparison.

Authentication process is a second part of biometric authentication. When a user attempts to access a system or device that utilizes biometric authentication, the system prompts them to provide their biometric data for verification. The captured biometric data is then compared with the stored template in the database. In the case of fingerprint authentication, for example, the user's presented fingerprint is scanned, and its unique features are compared with the stored algorithm. If the presented data closely matches the stored template within an acceptable margin of error, access is granted. Otherwise, the authentication fails.

Biometric authentication systems employ robust encryption techniques to ensure the security and privacy of biometric data. Instead of storing raw biometric data, systems typically store encrypted templates that cannot be reverse-engineered to reconstruct the original biometric information. Additionally, stringent measures are in place to protect against unauthorized access to the biometric database.

Moreover, many biometric authentication systems incorporate liveness detection mechanisms to prevent spoofing attempts. These mechanisms assess the liveliness of the presented biometric data, such as detecting pulse in fingerprint scans or monitoring facial movements during facial recognition.

2 The good, the bad and the ugly

Biometric authentication brings not only security and integrity but also convenience to the everyday digital operations. From unlocking smartphones to enhancing surveillance systems, this technology offers unparalleled convenience. Nevertheless, ethical debates surrounding privacy invasion and potential biases in algorithmic decision-making underscore the need for responsible deployment and regulation.

2.1 The good

Biggest advantage of biometric authentication - enhanced security. It is way harder to steal a fingerprint or a face than a password. This brings second advantage - convenience. Biometric authentication substitutes the need to remember passwords - also mitigates the risk of password getting compromised.

Accuracy of the operation - the fingerprint is more consistent than the same finger typing the password. This also brings the advantage of the speed of the operation - it is faster to scan a fingerprint or look into a camera than to type a password.

Data integrity and accountabilty. Biometric data is inherently tied to an individual , providing strong evidence of who performed a particular action, which can be crucial for accountability and legal purposes.

2.2 The bad

There are some privacy concerns with biometric authentication. Biometric data is highly sensitive and personal, and its misuse can have serious consequences. For example, if a biometric database is hacked, it can lead to identity theft and other forms of fraud. Additionally, biometric data is not easily revocable, meaning that once it is compromised, it is difficult to change or replace.

Another potential drawback of biometric authentication is the risk of false positives. While biometric systems are designed to be highly accurate, there is still a small chance of false positives, where the system incorrectly identifies an individual as someone else. This can lead to access being granted to unauthorized users, compromising security.

Moreover, biometric authentication systems can be expensive to implement and maintain. The hardware and software required for biometric authentication can be costly, and there may be additional costs associated with training and support. This can be a barrier to adoption for some organizations, especially smaller ones with limited resources.

2.3 The ugly

One of the biggest challenges facing biometric authentication is the risk of security vulnerabilities. While biometric systems are designed to be secure, they are not immune to attacks. For example, biometric data can be stolen or spoofed, leading to unauthorized access. Additionally, biometric systems can be susceptible to other forms of cyber attacks, such as malware or phishing.

Another challenge is the potential for bias and discrimination in biometric systems. Biometric data is often used to make important decisions, such as granting access to a building or verifying a person's identity. If the biometric system is biased or inaccurate, it can lead to unfair outcomes, such as denying access to certain

There are some legal and ethical concerns surrounding biometric authentication. For example, there are questions about who owns and controls biometric data, and how it can be used. There are also concerns about the potential for biometric data to be used for surveillance or tracking purposes, infringing on individuals' privacy and civil liberties.

Finally, there are concerns about the reliability and accuracy of biometric systems. While biometric authentication is generally considered to be more secure and reliable than traditional methods, it is not foolproof. Factors such as environmental conditions, user behavior, and system errors can all affect the accuracy of biometric systems, leading to false positives or false negatives.

3 Future for biometric authentication

In one sentence - future for biometric authentication looks promising. With continuous advancements in technology, biometric authentication is expected to become more secure, reliable, and user-friendly.

3.1 Enhanced security

Multi-modal biometrics looks to be the way of future authentication. Combining multiple biometric modalities (such as fingerprint, facial recognition, iris scanning, voice recognition, etc.) for enhanced accuracy and security will become more common. Multi-modal systems can provide stronger authentication compared to single-modal systems. Continuous authentication is another area of development. Instead of a one-time authentication process, continuous authentication systems monitor user behavior and biometric data throughout the session to ensure that the user remains authenticated. This can help prevent unauthorized access in case of a security breach or a change in user behavior.

3.2 Improved user experience

Biometric authentication is expected to become more user-friendly and convenient. Advancements in biometric sensors and algorithms will make the authentication process faster and more accurate. For example, the use of 3D facial recognition technology can improve the accuracy of facial recognition systems and reduce the risk of spoofing. Additionally, biometric authentication systems are expected to become more integrated with other technologies, such as smart home devices, wearables, and IoT devices, to provide a seamless user experience.

3.3 Widespread adoption

Biometric authentication is likely to see increased adoption across various industries and applications. The rise of digital banking and e-commerce is expected to drive the demand for biometric authentication solutions to enhance security and combat fraud. Additionally, the integration of biometric authentication into smartphones, laptops, and other consumer devices will make it more accessible to the general public. As biometric technology becomes more affordable and user-friendly, it is expected to become a standard feature in many digital products and services.

4 Biometric authentication not limited to humans?

The principles of biometric authentication are not limited to humans. In fact, biometric authentication can be applied to a wide range of applications beyond human identification. For example, ships also have a 'biometric' signature. As presented in the podcast "Pavojai Baltijos jūroje"[3] navy ships have unique acoustic, electromagnetic and pressure signatures. Based on these principles "smart" naval mines are being deployed in the contested waters. These mines can identify the signature of a specific ship and detonate only when the target is identified.

Conclusions

The rapid digitization of our world has underscored the critical need for robust and reliable authentication mechanisms to safeguard our digital identities and sensitive data. Biometric authentication emerges as a promising solution, leveraging unique physical or behavioral traits to provide a higher level of security and convenience compared to traditional methods.

As outlined in this discussion, biometric authentication offers a diverse array of modalities, from fingerprint and facial recognition to iris scanning and voice authentication. While each modality presents its own strengths and limitations, the overarching trend towards enhanced security, improved user experience, and widespread adoption remains evident.

However, alongside its undeniable benefits, biometric authentication also raises important ethical, privacy, and security considerations. Privacy concerns, potential biases, and the risk of security vulnerabilities underscore the importance of responsible deployment, regulation, and ongoing research and development in this field.

Looking to the future, continuous advancements in technology promise to further enhance the security, reliability, and user-friendliness of biometric authentication. Multi-modal systems, continuous authentication, and integration with emerging technologies are poised to redefine the landscape of cybersecurity, making biometric authentication an integral component of our digital lives.

In this dynamic and evolving landscape, it is imperative to strike a balance between innovation and accountability, ensuring that biometric authentication continues to evolve responsibly to meet the evolving challenges and opportunities of our digital age. By doing so, we can harness the full potential of biometric authentication to enhance security, protect privacy, and empower individuals in our increasingly interconnected world.

References

[1] "Biometric System Market Size, Share & Industry Growth Analysis Report by authentication type" by Markets and Markets, 2022. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/biometric-system-market-697.html.

[2] Biometric Authentication & Identification Market Size, Share, Growth, and Industry Analysis, By Type (Hardware, Software, Service and Others), By Application (Government, Banking and Finance, Commercial Application and Others) and Regional Insights and Forecast to 2031 https://www.businessresearchinsights.com/market-reports/biometric-authentication-identification-market-110643

[3] "Pavojai Baltijos jūroje" Lietuvos Kariuomenė 2024 https://www.youtube.com/watch?v=eVhCDfvb9xU