ISSN: 3066-7194
Review Article

Novel Journal of Applied Sciences Research

Cybersecurity in Biometric Authentication

Sampath Talluri*

Department of Computer Science, Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008

***Corresponding author:** Sampath Talluri, Department of Computer Science, Western Michigan University, 1903 W Michigan Ave, Kalamazoo, MI 49008.

Submitted: 27 March 2024 **Accepted:** 02 April 2024 **Published:** 10 April 2024

https://doi.org/10.63620/MKNJASR.2024.1009

Citation: *Talluri, S. (2024). Cybersecurity in Biometric Authentication. Nov Joun of Appl Sci Res, 1(2), 01-05.*

Abstract

Biometrics is the study and application of unique individual features, whether physical or behavioral, integrated for measurement or analysis to ensure security. Fingerprints, iris patterns, facial features, speech patterns, hand geometry, and behavioral aspects such as typing speed, rhythm, and stride are examples of such characteristics. Biometrics are most typically employed for identification and authentication because of their capacity to reliably distinguish individuals based on their unique characteristics. Because biometrics may make many systems and procedures more secure, they are an absolute must-have for cybersecurity professionals. Using biometrics for identity verification and multi-factor authentication can assist with defense-in-depth, commonly known as layers of security.

Keywords: Cybersecurity, Biometric Authentication, Fingerprints, Iris Patterns, Facial Features, Speech Patterns, Hand Geometry

Introduction

Background

With the increasing digitization of the society and their daily lives, there has never been a more critical time in the society for integrating cyber security [1]. With the increased advent of digitalization, the cyber threats are also increasing on a high pace. Cybercriminals and hackers are always honing their craft to exploit new holes in the systems and steal sensitive information. They are continually expanding their powers. Biometric cyber security outperforms more traditional, ineffective security solutions.

Biometric solutions that use cutting-edge biometric technology have made it easier than ever before to protect digital assets [1]. Voice recognition, fingerprint scanning, and facial recognition are just a few of the unique biological and behavioral characteristics that these systems use to verify identities and grant access. Bad actors' constant attacks on cybersecurity render traditional security processes ineffectual. Biometrics enhances our security measures by leveraging distinct behavioral and physical features.

Biometrics is a means of precisely identifying a person primarily based on physiological and behavioral factors which include their face, fingerprints, voice, or different traits. On the other hand, “Cybersecurity” refers to the process of defensive data systems, networks, records, and devices from net-primarily based attacks [2].

When it involves securing our on-line world from the steady danger posed by way of hackers and different antagonistic actors, conventional protection approaches are inadequate. Biometrics enhances our security features by leveraging wonderful behavioral and physical features.

In a global where personal identity numbers (PINs) and passwords are the norm, biometrics offer a novel solution. Unlike conventional authentication strategies that rely upon passwords or protection tokens, biometrics leverage a person's unique physiological or behavioral capabilities. This is an assessment of traditional identification verification approaches.

Despite its several benefits, biometric generation does have positive downsides. Researchers and builders are continuously improving biometric technologies to address flaws and growth security. Adding biometrics to multi-element authentication (MFA) systems that already employ different authentication elements, which include passwords or tokens, improves safety and reduces the chance of potential risks. Cybersecurity is presently doing research and improvement in a whole lot of fields, along with biometric statistics, privateness and information security, and other associated issues. To resolve those issues and maintain the integrity and secrecy of the biometric authentication procedure, efforts are ongoing to improve encryption, maintain a steady biometric information garage, and improve anti-spoofing mechanisms.

Aim, Objectives, and Research Questions

Aim

To understand the relationship between cyber security and biometric authentication.

Objectives

- To develop an understanding of the notion of cyber security and biometric authentication.
- To highlight the factors of biometric authentication.
- To outline the principles of cyber security.
- To draw on the relationship between cyber security and biometric authentication.

Research Questions

- What is the idea of cyber security and biometric authentication?
- What are the elements of biometric authentication?
- What are the fundamentals of cyber security?
- What is the link between cyber security and biometric authentication?

Research Rationale

Biometrics refers to the use of physical and behavioral characteristics to identify individuals. Fingerprints, facial traits, voice patterns, iris/retina scans, and even typing rhythm are examples of such qualities. Unlike passwords or tokens, which can be readily lost or stolen, biometrics are unique to each person, making them difficult to counterfeit or copy. Biometric identity plays an increasingly important part in our daily security. Physical characteristics are usually stable and unmistakable, especially in the case of twins. Everyone's unique biometric identification might be used to replace or supplement password systems for computers, phones, limited access rooms, and buildings.

Significance of the Research

Fingerprints are unique to each person. They may be quantified in many ways. The minutiae-based assessment uses graphs to compare ridges, while image-based measurement compares similarities between an individual's finger image and fingerprint photos already in the database. It offers a high level of security and is used for both identification and verification. However, fingerprints may be altered due to aging or disease/injury. Common applications include authentication on mobile devices and identity in the workplace. Physical biometrics assesses intrinsic physiological characteristics such as the anatomy of the eye, face, hand, or voice. For example, iPhone biometrics allows you to unlock your phone using your fingerprint. When you walk through a scanner at the airport, the system compares your scanned face structure to the data in your passport.

Literature Review

Factors Affecting the Integration

Biometric security is a kind of security that uses behavioral and physical characteristics to identify individuals. It is the most accurate and reliable physical security solution for identity verification. Biometric authentication indicates that individuals may be accurately recognized based on their inherent behavioral or physical characteristics. Biometrics are often used in security systems where physical protection is required and theft is a problem. These biometric security solutions store and employ physical characteristics that are consistent over time, such as hand patterns, face recognition, retinal patterns, and fingerprints [3, 4].

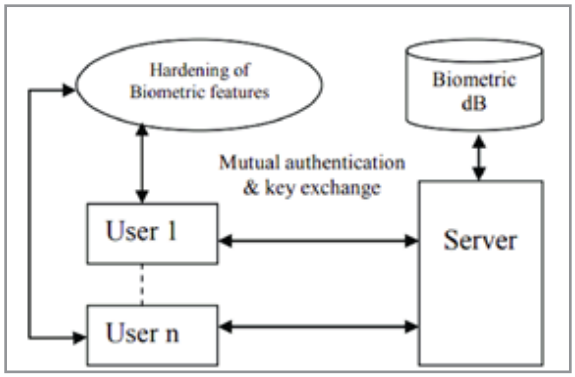

Figure 1: Biometric System [Source: Sheikh and Majid, 2019]

Face features such as nose distance, lips, ears, facial length, and skin tone are used for verification and identification. Fog, eyewear, aging, and other factors may all reduce accuracy. Patterns detected in the eye are unique and may be used for both identification and recognition. Devices for testing the retina are expensive; hence, they are less common. Diseases like cataracts may affect iris patterns.

Impact on Business Efficiency, Security, and Compliance

Biometric security refers to the use of biometric information for identification, access control, and authentication. Biometric data is recorded by hardware components such as cameras or fingerprint scanners and then scanned and algorithmically compared to information stored in a database [5]. If the two pieces of data match, the identification is verified, and access is granted.

The biometric system is vulnerable to several harmful assaults that may be carried out by various types of threats. Malicious assaults on a biometric machine pose a security concern and reduce the system's performance. There are various limitations to biometric systems, such as spoof attacks, noisy sensor data, interclass variations, and interclass similarities.

There are almost 20 different types of biometric data, including fingerprints, face, and voice. Each sort of biometric information may be hacked in a variety of ways. Installing a skimmer on ATMs or other biometric scanning equipment is a common and long-standing method of obtaining fingerprints. It scans fingerprints and creates phony reproductions that may be used to gain access to devices or sensitive data.

Framework for HRMS's and IAM's Successful Integration

of deepfake technology has made biometric hacking far more sophisticated while also making it more accessible to hackers. By launching a biometric spoofing attack, hackers may breach a protected system by using users' selfies, images, and videos from social media to create bogus identifiers such as face, voice, or even fingerprints.

"While we are the owners of our own faces and voices, we are not the only ones with access to them," said Warmenhoven. "People have left so much biometric data throughout the years of being active social media users that the present capabilities of artificial

intelligence to construct deepfakes make it a weapon against our privacy. Only this time, without our original permission."
Biometric data required to unlock a gadget is difficult to get since it is often stored in the device as encrypted binary code. However, providing applications with biometric data or allowing them to exploit it is not always a secure idea. Users may provide biometric information without understanding who the app's makers are or how the collected data will be used [6, 7].

Various Integration Approaches
New technology breakthroughs bring new faults and concerns, making cyber security a major concern. Along with these developments, we must remember that hackers are constantly innovating and continue to pose a threat to cyberspace. Because traditional methods of protection, such as passwords, are ineffective, more organizations and people are adopting biometric security as the preferred option to defend their cyberspace from threat actors. Facial recognition and fingerprint scanning are already widely used technologies.

Methodology

Data Collection

When conducting research, collecting relevant information or data is standard practice.

Figure 2: Secondary Data Collection [Source: Bhat, 2018]

Getting secondary data requires reading and investigating previously published items, including books, journals, and other written works. An in-depth literature study will be used to collect secondary data for this project. It is predicted that by doing this literature study, the article would gather current and relevant information on HRMS and IAM system integration. The primary sources of information for this study will include whitepapers, industry reports, and scholarly works released in the last few years.

Search Strategy

A systematic search approach will be applied to discover topic-relevant literature. As part of our plan, the study seeks to evaluate numerous prominent academic databases, including Web of Science, Scopus, and Google Scholar. Some keywords included during the search are identity and access management (IAM) integration with security, compliance, and efficiency.

Data Analysis

The acquired data will be submitted to theme analysis for qualitative analysis. The objective of thematic analysis is to uncover, examine, and interpret a dataset's underlying themes or patterns. This technique will be applied to thoroughly comprehend HRMS and IAM integration by extracting significant findings from the literature, recognizing crucial trends, and developing a holistic vision.

Tools and Techniques

The study will explore the existing literature and assess the issue using the correct methodologies and processes. It will be completely referenced management software and will be utilized to arrange and supervise the data that has been acquired methodically. This will make it much simpler to find certain works of literature. This analytic method may greatly simplify coding, subject finding, and data understanding.

Ethical Consideration

The examination will be carried out in line with the strictest ethical standards. The research project must always rigorously adhere to the norms of anonymity, secrecy, and informed consent. To ensure academic integrity, all sources must be accurately attributed. This research will also not gather primary data from people or groups.

Findings and Analysis

The following section's objectives include developing a solid conclusion and reviewing the literature read thus far.

The Need

Every day, it seems that there are more stories about data breaches affecting both large and small businesses. As these incidents continue, businesses are realizing that they must immediately implement additional security measures. Companies are gradually moving away from passwords in favor of biometric authentication technologies, without fully considering all the implications. While there are apparent advantages to biometrics, it is critical to thoroughly weigh each option.

Nonetheless, even if biometric data is stored on the server or cloud of a respectable app developer, it is far more dangerous since there is always the possibility of a data breach. Furthermore, biometrics hacking assault might be carried out by interception of data transfer between the user's device and storage [8].

The Impact of this Integration

The high assaults are important to any biometric system that is to be researched, and countermeasures must be included when developing the biometric system. The various assaults against biometric systems with the advancement of technology, hackers may now submit a phone biometric sample to a sensor to get access to the biometric system. Some examples of such harmful assaults on the sensor are fake face masks, silicon fingerprints, eye lenses, and so on. In this attack, a data stream from the biometric system is introduced between the sensor and the processing system. A repeat assault might be a two- or three-phase tactic. It first intercepts or duplicates the sensor transmission and then alters or modifies the data before replaying it.

Primary Considerations for the Integration

Spoofing the Feature Set: The process of replacing the feature set with fake or changed features is known as data spoofing.

These types of spoofing attacks are often used to target many networks, spread malware, and steal sensitive information. A template is a set of key characteristics summarizing a person's biometric data (signal) [9, 10]. The templates may be modified to get a high verification score regardless of whatever picture is provided to the system. Templates recorded in the database may be replaced, stolen, or updated. As a result, the system suffers as genuine users' scores fall. Template-generating algorithms have been categorized as one-way algorithms.

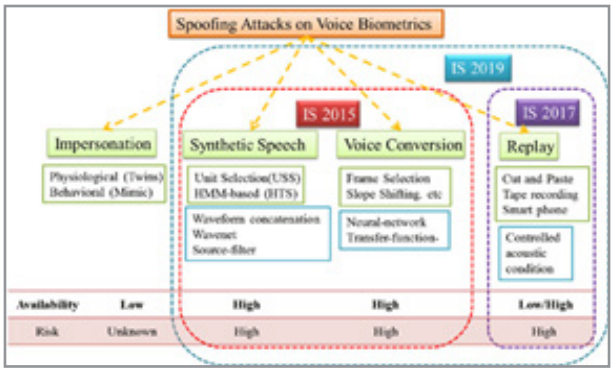

Figure 3: Data Spoofing Attacks [Source: Kamble, et al., 2020]

Pitch, voice modulation, and tone are among the variables examined. Security is medium, and since people' voices are similar, it is frequently used for verification. The accuracy may be affected because of noise, ageing, or illness.

DNA is unique and remains constant throughout life. Thus, security is good and may be used for both identification and verification. Eye identification uses the unique pattern of an individual's iris or retina to identify them. Because this kind of biometric authentication is more complex to deploy, it is less common than the other biometric authentication options. To be accurate, an iris scan needs an infrared light source, an IR-capable camera, and little light pollution. Despite its limitations, it is one of the most accurate biometric identification systems known if certain parameters are satisfied. Eye recognition is often used in contexts where security is crucial, such as nuclear research facilities etc.

Challenges, Benefits, and Best Practices

Integrating IAM with HRMS has captured and mapped many biometric data, and it is saved to be matched with future attempts at access. Most of the time, this data is e-encrypted and stored on the device or a distant server. Biological material, such as DNA extracted from blood, saliva, or hair samples, is very accurate and is often used as evidence in criminal trials. However, biological biometric analysis is currently too slow to be used for security control in most cases. Behavioral biometrics measures differentiating characteristics expressed in your external activities. Everyone's handwriting differs, and everyone writes on a keyboard and walks differently enough that artificial intelligence can accurately identify people based on those characteristics. Surfing behaviors and the specific gear used may even be combined to generate a distinct surfing fingerprint.

Biometric scanners are pieces of technology that collect biometric data for the purpose of verifying identification [11]. These scans compare the stored database to allow or prohibit access to the system. Global cybercrime is expected to generate $8 trillion in revenue by 2023, making it the world's third-largest economy behind China and the United States. In fact, it is expected to exceed $10.5 trillion every year by 2025, but expenditure on cybersecurity protection measures will only total $1.75 trillion from 2021 to 2025. Given the massive increase in cybercrime, it's clear that traditional security mechanisms such as passwords, PINs, and tokens no longer provide enough protection. This suggests that community financial institutions (CFIs) should use every tool at their disposal to resist increasingly sophisticated cyberattacks. Biometrics is a potentially valuable weapon in their arsenal.

Conclusion

Biometric technology, which includes fingerprint ID, retinal scanning, and face recognition, uses unique human behavioral or physical characteristics and indicators to verify identities and authenticate transactions. Passive speech recognition, also known as AI-based conversational biometrics, may detect an individual's usage of words, language, and grammar. In other words, biometric security uses your body as the "key" to open your access. Biometric IDs are unique and impossible to forge, making it very unlikely that an unauthorized user would get access to sensitive information. Even if a biometric template is produced, it cannot be used correctly since it needs the physical presence of the individual.

Biometrics are identification methods that use an individual's physiological and behavioral attributes, such as face, fingerprint, voice, or other characteristics, to precisely identify them. Depending on the use case and criticality, some systems employ biometrics as a form of authentication, while others use it as needed. Regardless, biometrics has improved security. Most organizations choose the latter since it requires both something you know/have (passwords, authentication devices) and something you are (biometrics) for authentication. This provides an additional layer of security and ensures a person's precise identification. Consequently, it reduces infractions. For example, some very secure server rooms use face recognition in conjunction with a password to allow access.

Recommendations

A biometrics degree combines skills from a variety of disciplines, including biology, computer science, engineering, statistics, and electrical engineering. Cybercrime is becoming more prevalent as internet technology advances. The cyber security sector has grown significantly in recent years. As the level of Internet espionage and terrorism rises around the world, so does the demand for cyber security experts. Due to the increased complexity of cybercrime, the training required to enter the field becomes more stringent as the number of cybersecurity jobs available grows. Recent high-profile hackings of government and commercial sector websites have prompted the training and certification of additional security staff.

For decades, governments have collected biometric data, starting with paper records of basic physical features like eye color, hair color, and height. For more than a century, police have used fingerprints collected at crime scenes to build databases of suspects and offenders. At the start of World War, I, Britain and other countries started issuing passports with basic physical identifiers to allow governments to screen immigrants and differentiate be-

tween citizens (who have certain rights) and non-citizens (who may have hostile intent).

References

1. Möller, D. P. F. (2023). Cybersecurity in digital transformation. Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Springer Nature Switzerland, 1-70.
2. Narayan, R., Balaji, N. V., Kalanandhini, G., Mahalle, P. N., & Wasim, J. (2023). Developing the Role of Firewalls in Enhancing Web Security for Wireless Networks. 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 1-6.
3. Sharif, M., Raza, M., Shah, J. H., Yasmin, M., & Fernandes, S. L. (2019). An overview of biometrics methods. Handbook of Multimedia Information Security: Techniques and Applications, 15-35.
4. Sheikh, Y., & Majid, M. I. (2019). ATM & Biometric Solutions: A Case Study. International Journal of Experiential Learning & Case Studies, 4, 237-253.
5. Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. Expert Systems with Applications, 143, 113114.
6. Tait, B. L. (2021). Aspects of biometric security in internet of things devices. Digital Forensic Investigation of Internet of Things (IoT) Devices, 169-186.
7. Bhat, A. (2018). Secondary Research- Definition, Methods and Examples. QuestionPro. https://www.questionpro.com/blog/secondary-research/
8. Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., & Praveen, S. (2021). A comprehensive overview of privacy and data security for cloud storage. International Journal of Scientific Research in Science Engineering and Technology, 8, 113-152.
9. Zhang, L. B., Peng, F., Qin, L., & Long, M. (2018). Face spoofing detection based on color texture Markov feature and support vector machine recursive feature elimination. Journal of Visual Communication and Image Rsepresentation, 51, 56-69.
10. Kamble, M. R., Sailor, H. B., Patil, H. A., & Li, H. (2020). Advances in anti-spoofing: from the perspective of ASVspoof challenges. APSIPA Transactions on Signal and Information Processing, 9, 2.
11. Singh, G., Bhardwaj, G., Singh, S. V., & Garg, V. (2021). Biometric identification system: security and privacy concern. Artificial intelligence for a sustainable industry 4, 245-264.