NEURALSLATE OPEN ACCESS JOURNALS
International Journal of Responsible Artificial Intelligence

Evaluating the Efficacy of Biometric Authentication Techniques in Healthcare

Irfan Ahmed
University of Balochistan, Quetta

Amina Asghar
Women's University, Multan
asgar65@gmail.com

Abstract

With the rapid advancement in digital healthcare, protecting patient data has become paramount, necessitating more robust and reliable authentication techniques. Biometric authentication, using unique physical or behavioral characteristics, is being increasingly adopted due to its potential for enhanced security. This study undertakes an in-depth comparison and evaluation of the effectiveness of various biometric authentication techniques in healthcare settings, focusing on five principal biometric techniques: fingerprint recognition, facial recognition, iris recognition, voice recognition, and hand geometry. These methods were compared in terms of accuracy, cost-effectiveness, user acceptance, and suitability for different healthcare scenarios, such as in-person visits and telemedicine consultations. The findings indicate that while all five techniques have potential for authentication in healthcare, their suitability varies depending on specific circumstances. Fingerprint recognition was found to be widely acceptable due to its ease of use and cost-effectiveness, despite concerns related to data privacy. Facial recognition, though highly accessible and non-contact, displayed issues with accuracy due to variable factors such as lighting and aging. Iris recognition showed high accuracy and stability, but its implementation was hindered by high costs and practical usage constraints. Voice recognition offered potential for remote patient authentication, but accuracy levels were compromised in noisy environments or due to voice changes from illness or aging. Hand geometry, while unique and reliable, required specialized equipment and had issues concerning user comfort and hygiene. the study suggests that a multi-factor authentication approach, combining two or more methods, may offer increased security and accuracy in healthcare settings. However, further research is needed to investigate this approach's feasibility, considering potential increases in cost and complexity.

Indexing terms: Biometric Authentication, Healthcare Data Security, Fingerprint Recognition, Multi-factor Authentication, Digital Healthcare

Introduction

Biometric authentication technologies have grown in importance and prevalence as the need for secure identification and personal verification in today's digital age has increased. These techniques are based on unique biological or behavioral characteristics that individuals possess. This includes fingerprints, facial features, voice patterns, iris and retinal patterns, among others. Such attributes are unique to every individual, making biometric authentication one of the most secure and convenient ways of verifying someone's identity.

Among the different biometric authentication techniques, fingerprint recognition is one of the most commonly used due to its simplicity and ease of use. The uniqueness of every individual's fingerprints has been well-established, making them an excellent means of identification. In this technique, an individual's fingerprint is scanned, and an image is captured. This image is then analyzed for unique patterns such as arches, loops, and whorls, as well as minutiae details such as bifurcations and ridge endings. A digital representation of these features is stored in a database for future comparison. When an individual needs to be identified, a new scan is compared to the stored representation to verify the identity.

Facial recognition is another popular biometric authentication technique. This method uses the unique features of a person's face for identification. Facial recognition software

maps an individual's face to create a mathematical representation, focusing on key features like the distance between the eyes, the width of the nose, the shape of the cheekbones, and other distinct facial features. The resulting data is then stored and used for future identification. With advancements in AI and machine learning, these systems have become increasingly sophisticated, capable of identifying individuals even when their faces are partly obscured or in different lighting conditions [1].

Iris recognition, on the other hand, is a relatively newer technique and is considered one of the most accurate forms of biometric authentication. The iris, the colored ring around the pupil of the eye, has a highly intricate and unique pattern. The process involves using a high-resolution camera to capture an image of the iris. This image is then processed using computer algorithms to identify and store distinct patterns. The high degree of uniqueness in iris patterns, coupled with the non-invasive and contactless nature of this technique, makes it extremely reliable and efficient.

Similarly, voice recognition is another biometric authentication technique that leverages the unique characteristics of a person's voice. This technique works by analyzing the physical configuration of an individual's speech organs, as well as the way in which the person speaks, including rhythm, speed, and pitch. The system creates a voiceprint that can be stored and used for future identification. This method is often used in conjunction with other biometric methods to improve accuracy.

Finally, there's behavioral biometrics, which rely on unique patterns of behavior exhibited by users. Examples include keystroke dynamics - the unique way a person types on a keyboard, or gait analysis - identifying people by the way they walk. These methods, while not as common, are growing in use as they can be passive, unobtrusive, and difficult to spoof.

However, the application of biometric authentication techniques also raises privacy and security concerns. The stored biometric data, if compromised, can lead to serious privacy invasions since unlike passwords, biometric data cannot be changed. Moreover, the biometric systems themselves can be subject to various attacks like presentation attacks (spoofing), and therefore need to have appropriate countermeasures in place.

Biometric authentication in healthcare has emerged as a key technology for ensuring the security and privacy of patients' health information. As healthcare systems are increasingly digitized, the importance of strong, reliable authentication methods has become crucial. Biometric authentication provides an effective solution to the challenges of identity theft, unauthorized access, and fraud, which are particularly significant in the context of sensitive health data [2].

One of the primary uses of biometrics in healthcare is patient identification. Patient misidentification can lead to serious errors in medical treatment, including medication errors, testing errors, and surgical errors. Biometric authentication, such as fingerprint or iris recognition, provides a way to reliably identify patients, reducing the risk of identification errors. In this context, a patient's biometric data is captured and stored. When the patient needs to be identified, their biometric data is captured again and compared to the stored data, providing a high level of confidence in the identification.

Biometric authentication also plays a critical role in protecting electronic health records (EHRs) [3]. EHRs contain highly sensitive personal and health information, and unauthorized access can lead to significant privacy breaches [4]. Biometric authentication can be used to secure access to EHRs, ensuring that only authorized individuals, such as the patient and their healthcare providers, can access the data [5]–[7]. For instance, a healthcare provider might use a fingerprint or facial recognition system to authenticate their identity before accessing a patient's HER [8].

These digital systems allow healthcare providers to access and update patients' medical information, enabling faster decision-making and coordinated care during times of heightened health crises. During the COVID-19 pandemic, EHRs have been instrumental in tracking and managing cases, enabling real-time data sharing between

healthcare facilities, and assisting in research efforts. COVID-19, caused by the novel coronavirus SARS-CoV-2, emerged in late 2019 and led to a global pandemic [9]. The symptoms of COVID-19 can range from mild to severe and may appear 2 to 14 days after exposure to the virus [10]–[12]. Common symptoms include fever, cough, shortness of breath, fatigue, muscle or body aches, loss of taste or smell, sore throat, congestion, and headache [13]–[15]. In severe cases, patients may develop pneumonia, acute respiratory distress syndrome (ARDS), and multi-organ failure, requiring intensive medical intervention.

Throughout history, the world has experienced various pandemics and endemics caused by infectious diseases. One of the deadliest pandemics was the Spanish Flu, which occurred between 1918 and 1919. Caused by the H1N1 influenza A virus, it infected about one-third of the global population and led to millions of deaths. Unlike typical influenza strains, the Spanish Flu predominantly affected young adults. Its devastating impact shaped modern epidemiology and influenced global public health measures.

Another ongoing pandemic is HIV/AIDS, which was first recognized in 1981. The Human Immunodeficiency Virus (HIV) causes Acquired Immunodeficiency Syndrome (AIDS), weakening the immune system and making individuals susceptible to infections and diseases. Since its discovery, HIV/AIDS has claimed over 32 million lives, and millions still live with the virus today. While antiretroviral therapies have improved the quality of life for those infected, a cure remains elusive. Ebola virus outbreaks have sporadically affected Central and West Africa since 1976. Ebola virus disease (EVD) causes severe hemorrhagic fever, with mortality rates ranging from 25% to 90%, depending on the strain [16], [17]. Containment efforts involve strict quarantine measures, contact tracing, and community education to limit its spread.

In 2015-2016, the Zika virus gained global attention during an outbreak. Primarily transmitted through infected mosquitoes, Zika virus infections were mostly mild, but it posed significant risks to pregnant women, linked to severe birth defects like microcephaly in babies [18]. Public health efforts focused on mosquito control and advising pregnant women to avoid affected areas.

Cholera is an endemic disease in many parts of Africa, Asia, and Latin America, leading to periodic outbreaks due to contaminated water sources and poor sanitation. It causes severe diarrhea and dehydration, which can be fatal without prompt treatment. Improved sanitation, clean water access, and oral rehydration therapies have been essential in controlling cholera outbreaks [19], [20].

Malaria, caused by the Plasmodium parasite transmitted through mosquitoes, remains endemic in tropical regions, causing significant morbidity and mortality, especially among young children and pregnant women. Vector control measures such as insecticide-treated nets and indoor residual spraying, along with antimalarial medications, have been crucial in reducing malaria-related deaths. Tsutsugamushi disease, also known as scrub typhus, is caused by the bacterium Orientia tsutsugamushi, which is transmitted to humans through the bites of infected chiggers (larval mites) [21]. The disease is prevalent in some parts of Asia, the Pacific Islands, and parts of northern Australia. The symptoms of scrub typhus typically appear 10 to 14 days after being bitten by an infected chigger. Initial symptoms may include fever, headache, muscle aches, and a characteristic eschar (a black, scab-like lesion) at the site of the chigger bite. As the disease progresses, patients may develop more severe symptoms such as rash, swollen lymph nodes, cough, gastrointestinal symptoms, and in some cases, organ failure.

The ability to swiftly retrieve patient histories, lab results, and treatment plans through EHRs has helped in identifying at-risk individuals, monitoring disease progression, and optimizing resource allocation. Furthermore, EHRs have aided in the integration of telemedicine, reducing physical interactions and enhancing remote healthcare services. The application of biometrics in healthcare isn't limited to patients and healthcare providers [22], [23]. It also extends to other areas such as pharmacy dispensing, where

biometric systems can ensure that prescription medications are dispensed to the correct patient, and in hospital security, where biometric systems can control access to restricted areas [24], [25].

Moreover, biometric authentication can streamline the workflow in healthcare settings. For instance, by replacing traditional time-consuming methods of identification such as ID cards or passwords, biometrics can speed up patient check-in procedures and reduce administrative burdens on healthcare staff. Despite the numerous benefits, the use of biometrics in healthcare also presents challenges. Privacy and security of biometric data is a significant concern. Biometric data is sensitive personal information, and its theft or misuse can have severe consequences. Therefore, healthcare organizations must ensure they have robust data protection measures in place, including encryption of stored data and secure communication protocols [26].

In addition, biometric systems in healthcare must also be designed to accommodate a wide range of individuals, including those with disabilities or conditions that may make it difficult to capture biometric data. This might require the use of multiple types of biometric systems, or alternative methods of authentication for individuals who cannot use the biometric systems.

Efficacy of biometric authentication techniques in healthcare

Fingerprint recognition:

Fingerprint recognition is a biometric technique that leverages the uniqueness of an individual's fingerprints for identification or authentication purposes. It is one of the most commonly used biometric systems, owing to its numerous advantages. Notably, fingerprints provide an inexpensive, convenient, and highly accurate way to verify an individual's identity. From smartphones to secure entry systems, the use of fingerprint scanners has become commonplace. Each individual has a unique set of fingerprints that remain stable over time, making this biometric technique reliable and highly accurate. Fingerprints consist of ridges and furrows, with the uniqueness determined by the minutiae points located on the ridges, including ridge endings and bifurcations.

One of the reasons for the wide adoption of fingerprint recognition is the relatively low cost of implementing this technology. The hardware required for capturing fingerprint data, such as optical, capacitive, or ultrasonic sensors, has decreased in price significantly over the years. Additionally, advancements in technology have allowed for the miniaturization of these sensors, enabling them to be integrated into a wide variety of devices and systems. Nowadays, fingerprint scanners can be found in smartphones, laptops, door locks, and many other everyday items, illustrating the broad applicability of this biometric technique [27].

However, the effectiveness of fingerprint recognition can be impacted by various environmental and physical factors. Dirt, grease, sweat, or other substances present on the fingers can interfere with the ability of the scanner to accurately capture the fingerprint image. Furthermore, physical conditions such as cuts, abrasions, or other injuries to the fingers can affect the reliability of fingerprint recognition. These factors can lead to false rejections, where a legitimate user is not recognized by the system, or false acceptances, where an imposter is incorrectly identified as a legitimate user.

Another concern associated with fingerprint recognition systems is the potential for privacy issues. Fingerprint data is highly sensitive and personal, and the misuse of this data can lead to serious privacy breaches. The way fingerprint data is stored and transmitted needs to be carefully managed to ensure the protection of this information. Encryption and secure transmission protocols are essential to protect the data from potential hackers or unauthorized access.

Additionally, there is a fear that biometric data, once stolen, can be used for various malicious activities as it can't be changed or replaced like a password. Fingerprints can be replicated from a variety of surfaces and then used to trick fingerprint scanners.

There have been instances where artificial fingerprints, created using information stolen from fingerprint databases, have been used to bypass security systems. This underscores the importance of securing biometric data both at rest and in transit.

Moreover, unlike passwords or PIN numbers, fingerprints cannot be altered or reset if they become compromised. This immutable nature of biometric data, combined with the potential for permanent loss or theft, makes it critical that stringent security measures are in place to protect this information. The irreversible nature of biometric data exposure also underscores the need for robust legal frameworks to protect individuals' rights in the event of a data breach [28].

Facial recognition:

Facial recognition is another biometric technique that has gained prominence in recent years, especially with the development of advanced artificial intelligence algorithms [19]. It operates by analyzing the characteristics of a person's face to distinguish and identify individuals. The prominent advantage of facial recognition is its non-contact nature, which makes it more convenient and less intrusive than other biometric techniques. Also, facial recognition can be integrated into existing camera systems, allowing for easy implementation in a variety of environments such as airports, shopping malls, and even on smartphones [29].

The increasing utilization of facial recognition technology is linked with the evolution of artificial intelligence, and particularly machine learning and deep learning algorithms. These sophisticated computational models can learn to identify and differentiate between facial features in a way that is much more complex and accurate than previous systems [30], [31]. Deep learning, a subfield of machine learning, utilizes neural networks with many layers (hence the name "deep") to analyze faces. The algorithms can be trained to recognize complex patterns and variations in facial features, improving the accuracy of identification and verification tasks [32].

However, despite its potential and increasing use, facial recognition technology does face several challenges. One of the main challenges is the sensitivity of the system to variations in lighting, the person's expression, the angle at which the face is presented, as well as aging. Changes in a person's appearance, such as a new hairstyle, the presence of glasses or makeup, and natural aging, can all impact the system's ability to accurately recognize an individual. Moreover, differences in the lighting conditions between when the reference image was taken and when a new image is analyzed can lead to identification errors. These factors can increase the likelihood of false acceptances and false rejections, thus affecting the overall reliability of the system .

In addition to these technical challenges, facial recognition technology brings with it a host of privacy and ethical considerations. The widespread use of facial recognition systems raises significant concerns about privacy and consent, as these systems can potentially be used to track individuals without their knowledge or permission. It’s a matter of public record when someone enters a secure building using a fingerprint scanner, but when a person's face is scanned in a public space for the purpose of identification, it is often done without explicit consent, leading to potential privacy violations.

Moreover, there is also the risk of data breaches. As with fingerprint data, facial recognition data is highly sensitive and personal. If this data is not properly secured, it could fall into the wrong hands, leading to potential misuse. Similarly, the immutable nature of biometric data applies here as well. Unlike a password, facial data cannot be changed or reset, which means once it is compromised, the risk is permanent.

Legal frameworks have struggled to keep up with the rapid development and deployment of facial recognition technologies. Current laws often do not adequately address the unique challenges posed by these systems, leaving gaps in the protection of individuals' privacy rights. The combination of these legal gaps with the potential for

abuse of this technology has led to calls for stricter regulations and guidelines regarding the use of facial recognition systems.

Iris recognition:

Iris recognition is another biometric identification method that is gaining traction due to its exceptional accuracy and the stability of the iris pattern over time. The human iris, a circular structure in the eye that gives it its color, has a fine texture that is formed during prenatal life and remains stable throughout a person's lifetime. This unique and highly complex pattern offers an almost foolproof method of identification, making iris recognition one of the most accurate biometric techniques available.

The process of iris recognition involves capturing a high-resolution image of the iris and then using algorithms to analyze the complex patterns within it. Iris patterns are characterized by a host of distinctive features such as rings, furrows, freckles, and the corona. These features are then transformed into a digital template, which can be compared to stored templates in the database for identification or verification. This entire process can be completed in a matter of seconds, offering a quick and highly accurate method of identifying individuals. Despite its high accuracy and robustness, iris recognition is not without its limitations. One of the primary barriers to the widespread adoption of iris recognition systems is the cost. Iris scanners are more expensive than other biometric technologies such as fingerprint or facial recognition systems. They require high-resolution cameras to capture the intricate details of the iris, which can drive up the cost. This makes them less accessible for applications where budget constraints are a significant consideration [33].

Another practical challenge associated with iris recognition is the need for the user to be in close proximity to the scanner. Users must position their eyes a certain distance from the scanner and often need to remain still for the scanning process. In certain settings, such as healthcare facilities, this might not be feasible or practical. Patients with certain conditions or those who are unable to stay still may find it difficult to use these systems. This need for close proximity and user cooperation can limit the applicability of iris recognition in certain contexts [34], [35].

Like all biometric techniques, iris recognition also raises privacy concerns. Iris scans result in the creation of sensitive biometric data, which needs to be stored and transmitted securely to prevent unauthorized access. Any breach of this data can lead to serious privacy infringements, as the data can't be changed or replaced like traditional passwords. Furthermore, there are potential concerns about the acceptability and perceived invasiveness of iris recognition. Some people may feel uncomfortable with a camera scanning their eyes, and there could be misconceptions or fears about potential harm to the eyes, even though the infrared light used by iris scanners is safe [36].

Voice recognition:

Voice recognition, also known as speaker recognition, is a biometric modality that identifies individuals based on their unique vocal characteristics. It has been gaining attention as a viable biometric technique, particularly for remote authentication applications such as telemedicine, call centers, and smart home devices. The attractiveness of voice recognition lies in its non-contact, non-invasive nature, and its ability to work remotely over the phone or internet, thus providing a high level of convenience and accessibility.

The process of voice recognition involves two main stages. The first stage is feature extraction, where unique characteristics of the speaker's voice, such as pitch, tone, cadence, and accent, are captured and transformed into a digital format. These characteristics are determined by both the physiological structure of the speaker's vocal tract and their learned speech behavior [37]. The second stage is the matching process, where the extracted features are compared with stored voiceprint templates in a database to verify or identify the speaker [38]–[40].

Despite its potential and conveniences, voice recognition also has its set of challenges. One of the most significant challenges is the susceptibility of this biometric modality to background noise. Ambient noise in the environment where the voice sample is being collected can interfere with the system's ability to accurately capture and analyze the voice features. Moreover, the use of different recording devices or communication channels with varying quality can also affect the performance of voice recognition systems.

Changes in the speaker's voice due to factors such as illness, mood, or aging can also impact the system's accuracy. Illnesses such as a cold or sore throat can alter a person's voice significantly, and natural variations in voice due to emotional states or tiredness can also cause discrepancies. Aging is another factor that can affect the characteristics of a person's voice over time. These variations can potentially lead to a higher rate of false rejections, thereby impacting the system's overall reliability.

Privacy and security issues are another significant concern for voice recognition systems. Voice data, like other biometric data, is highly personal and sensitive. Therefore, securing this data from potential breaches is of utmost importance. Moreover, voice samples can be recorded and mimicked, leading to potential spoofing attacks. Therefore, anti-spoofing measures are necessary to ensure the integrity of voice recognition systems [41]. Despite these challenges, the convenience and remote capabilities of voice recognition make it a promising technique for a wide range of applications. The rise of smart speakers and virtual assistants, along with the growing demand for remote healthcare services such as telemedicine, provides ample opportunities for the application of voice recognition.

Hand geometry:

Hand geometry recognition is a type of biometric identification that involves measuring and analyzing the physical structure of an individual's hand. The parameters evaluated typically include finger length, width, and thickness, as well as the overall surface area of the hand. This data is then transformed into a digital template for comparison against stored templates in a database. Because hand geometry has a relatively low false acceptance rate and doesn't require the same level of precision as some other biometric techniques, it has found use in various healthcare applications, including patient identification and access control in secure areas.

Healthcare environments often require reliable and quick identification methods to manage patient records efficiently and accurately. Hand geometry can offer a solution in such scenarios by allowing easy identification of patients, thereby reducing errors and ensuring that the correct medical data is always linked to the right individual [42]. In terms of access control, hand geometry readers have been deployed in areas that need to limit access to authorized personnel only, such as operating rooms or medical storage facilities. Despite the potential benefits of hand geometry recognition, there are several limitations that could hamper its wider adoption. One of these is the requirement for specialized equipment. Hand geometry scanners are typically bulkier and more expensive than other biometric devices, such as fingerprint or iris scanners. This additional cost and the need for space can make it less attractive for organizations with budget or space constraints [7], [43].

Another concern associated with hand geometry recognition is user comfort and hygiene. The user has to place their hand onto a scanner, which can raise concerns about hygiene, especially in settings like healthcare facilities where there's a high risk of disease transmission. Frequent cleaning of the scanner surface might be necessary to maintain sanitary conditions, but this adds to the overall maintenance requirements of the system.

In terms of user comfort, some individuals may find the process of placing their hand on the scanner uncomfortable or unnatural. Others may have physical conditions or injuries that make it difficult to place their hand in the correct position for scanning. This could result in inaccurate readings or failed identification attempts, potentially

leading to frustration for users and administrators alike. Lastly, hand geometry, as with any other biometric modality, carries concerns about privacy and data security. Ensuring that the collected biometric data is stored and processed securely is critical to maintaining user trust and adhering to data protection laws. Also, since hand geometry data is less distinctive than other biometric traits such as fingerprints or iris patterns, there is a slightly higher risk of false acceptances, which could potentially lead to unauthorized access.

Conclusion

The importance of robust and reliable authentication techniques in digital healthcare cannot be overstated. As the healthcare industry increasingly adopts digital technologies to store sensitive patient information and facilitate seamless communication among healthcare providers, ensuring the security and privacy of these systems becomes paramount. Robust authentication techniques serve as the first line of defense against unauthorized access and potential data breaches. The consequences of a security breach in the healthcare sector can be severe, ranging from compromising patient confidentiality to the manipulation of medical records, leading to incorrect diagnoses or treatments. Therefore, implementing authentication methods that are resistant to various attacks, such as brute force or social engineering, is essential to safeguard patient data and maintain trust in digital healthcare systems.

In this study, five biometric authentication techniques were thoroughly compared and evaluated to assess their efficacy in securing digital healthcare environments. Biometric techniques rely on unique physiological or behavioral characteristics of individuals, such as fingerprints, iris patterns, voice, face, or even gait, for authentication purposes. Such methods offer the advantage of being inherently personal and difficult to forge, providing a higher level of security compared to traditional password-based systems. However, not all biometric techniques are equally reliable and suitable for the healthcare context.

The first biometric technique evaluated in the study was fingerprint recognition. Fingerprint biometrics have been widely adopted due to their long-standing use in law enforcement and the accessibility of fingerprint sensors on modern devices. They generally offer high accuracy, speed, and user-friendliness. However, concerns arise regarding the potential of latent fingerprints on shared surfaces and the need for a clean environment for accurate scans. The second technique examined was iris recognition. Iris patterns are highly distinctive and stable, making them a robust choice for authentication. They also present a non-invasive method, promoting user acceptance. Nonetheless, iris recognition systems can be sensitive to lighting conditions, and certain eye conditions might affect their reliability.

Next, the study assessed voice recognition, which uses voiceprints to identify individuals. Voice authentication is convenient and well-suited for remote applications. However, it can be susceptible to environmental noise and variations in the speaker's voice, such as due to illness. The fourth technique under evaluation was facial recognition. Facial biometrics have become increasingly popular in various applications, including smartphones and security systems. They offer ease of use and unobtrusiveness. However, concerns related to privacy and the potential for false positives or negatives have been raised. The study then explored gait recognition, a relatively less common biometric technique. Gait refers to an individual's walking pattern, which can be analyzed through sensors or video footage. Gait recognition can be useful in scenarios where other biometric traits are not available, but it might require additional hardware and present challenges in accuracy and user acceptance [44].

Robust and reliable authentication techniques are vital for securing digital healthcare systems and protecting sensitive patient information. The comparison and evaluation of the five biometric techniques highlighted their individual strengths and weaknesses. Understanding these nuances is crucial for healthcare organizations to make informed decisions about implementing the most suitable biometric authentication method that

aligns with their security requirements and user needs. By adopting the right authentication approach, the healthcare industry can ensure a safer and more secure digital landscape for both patients and healthcare providers [45].

The study's findings open up an intriguing opportunity for enhancing the security and accuracy of digital healthcare authentication through the combination of two or more methods, commonly known as multi-factor authentication (MFA). By leveraging the strengths of different biometric techniques, MFA can create a more robust and reliable system, significantly mitigating the risks associated with single-factor authentication methods [46]. One of the key advantages of using multi-factor authentication is the increased security it provides [47]. When multiple biometric factors are combined, an attacker would need to compromise all the different authentication methods simultaneously, making it exponentially more challenging to breach the system. For instance, if a digital healthcare application utilizes both fingerprint and iris recognition for MFA, an attacker would need to clone fingerprints and replicate iris patterns, which is highly improbable. MFA can act as a powerful deterrent against various types of attacks, including brute force attacks, credential stuffing, and social engineering [48].

Moreover, combining multiple biometric methods can enhance accuracy and reduce the chances of false positives and negatives. Each biometric trait has its own strengths and limitations, and by using complementary biometrics, the weaknesses of one can be compensated for by the strengths of another. For instance, if facial recognition alone is used, it may face challenges in accurately identifying individuals under varying lighting conditions or when partial facial data is available. However, when combined with voice recognition or fingerprint authentication, the overall accuracy of the system improves, as these traits may excel in scenarios where facial recognition struggles .

Furthermore, multi-factor authentication can increase user confidence and acceptance. Traditional single-factor methods like passwords or PINs are often cumbersome and can be forgotten, leading to user frustration. Biometric authentication on its own can also occasionally present reliability issues, especially in certain environments or for specific individuals. However, when users experience the convenience and reliability of MFA, their trust in the system grows, encouraging greater adoption of digital healthcare technologies.

While MFA offers significant benefits, it is essential to consider potential challenges, such as the additional hardware or software requirements for implementing multiple biometric techniques. Moreover, the usability and user experience should be carefully designed to strike the right balance between security and convenience. In certain situations, a higher level of security might warrant the inclusion of more biometric factors, but this should be balanced with the user's ease of access and the resources required for implementation.

References

[1] J. Ashbourn, *Biometrics in the new world: The cloud, mobile technology and pervasive identity*. New York, NY: Springer, 2014.

[2] Y. Mintz and R. Brodie, “Introduction to artificial intelligence in medicine,” *Minim. Invasive Ther. Allied Technol.*, vol. 28, no. 2, pp. 73–81, Apr. 2019.

[3] Z. Che, Y. Cheng, S. Zhai, Z. Sun, and Y. Liu, “Boosting Deep Learning Risk Prediction with Generative Adversarial Networks for Electronic Health Records,” in *2017 IEEE International Conference on Data Mining (ICDM)*, 2017, pp. 787–792.

[4] K. Nova, “Generative AI in Healthcare: Advancements in Electronic Health Records, facilitating Medical Languages, and Personalized Patient Care,” *JAAHM*, vol. 7, no. 1, pp. 115–131, Apr. 2023.

[5] Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, and C. Wu, “Generating stable biometric keys for flexible cloud computing authentication using finger vein,” *Inf. Sci.* , vol. 433–434, pp. 431–447, Apr. 2018.

[6] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, “Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-

Based Industrial Internet of Things Deployment," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.
[7] S. Venkatraman and I. Delpachitra, "Biometrics in banking security: a case study," *Inf. Manage. Comput. Secur.*, vol. 16, no. 4, pp. 415–430, Jan. 2008.
[8] M. K. Baowaly, C.-C. Lin, C.-L. Liu, and K.-T. Chen, "Synthesizing electronic health records using improved generative adversarial networks," *J. Am. Med. Inform. Assoc.*, vol. 26, no. 3, pp. 228–241, Mar. 2019.
[9] A. Bodepudi and M. Reddy, "The Rise of Virtual Employee Monitoring in Cloud and Its Impact on Hybrid Work Choice," *Journal of Artificial Intelligence and Machine Learning in Management*, vol. 5, no. 1, pp. 25–50, 2021.
[10] J. Hindson, "COVID-19: faecal–oral transmission?," *Nat. Rev. Gastroenterol. Hepatol.*, vol. 17, no. 5, pp. 259–259, Mar. 2020.
[11] D. Mallick, L. Goyal, P. Chourasia, M. R. Zapata, K. Yashi, and S. Surani, "COVID-19 Induced Postural Orthostatic Tachycardia Syndrome (POTS): A Review," *Cureus*, vol. 15, no. 3, p. e36955, Mar. 2023.
[12] K. Yuki, M. Fujiogi, and S. Koutsogiannaki, "COVID-19 pathophysiology: A review," *Clin. Immunol.*, vol. 215, p. 108427, Jun. 2020.
[13] A. Kessler, M. Heightman, and E. Brennan, "Post-COVID-19 respiratory problems: burden and management," *Curr. Opin. Support. Palliat. Care*, vol. 16, no. 4, pp. 203–209, Dec. 2022.
[14] U. Birberg Thornberg, A. Andersson, M. Lindh, L. Hellgren, A. Divanoglou, and R. Levi, "Neurocognitive deficits in COVID-19 patients five months after discharge from hospital," *Neuropsychol. Rehabil.*, pp. 1–25, Oct. 2022.
[15] M. Abdelghany *et al.*, "CRT-200.08 outcomes of acute coronary syndrome in patients with Coronavirus 2019 infection: A systematic review and meta-analysis," *Cardiovascular Interventions*, vol. 15, no. 4_Supplement, pp. S29–S30, Feb. 2022.
[16] P. J. Hotez, "Neglected Tropical Diseases in the Anthropocene: The Cases of Zika, Ebola, and Other Infections," *PLoS Negl. Trop. Dis.*, vol. 10, no. 4, p. e0004648, Apr. 2016.
[17] A. Siddharta *et al.*, "Virucidal Activity of World Health Organization–Recommended Formulations Against Enveloped Viruses, Including Zika, Ebola, and Emerging Coronaviruses," *J. Infect. Dis.*, vol. 215, no. 6, pp. 902–906, Feb. 2017.
[18] S. K. Palo *et al.*, "Effective interventions to ensure MCH (Maternal and Child Health) services during pandemic related health emergencies (Zika, Ebola, and COVID-19): A systematic review," *PLoS One*, vol. 17, no. 5, p. e0268106, May 2022.
[19] K. Nova, "AI-Enabled Water Management Systems: An Analysis of System Components and Interdependencies for Water Conservation," *ERST*, vol. 7, no. 1, pp. 105–124, Jun. 2023.
[20] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptogr. Commun.*, vol. 2, no. 1, p. 1, Jan. 2018.
[21] N. Patil *et al.*, "Spot the dot: solve the mystery: tsutsugamushi disease," *Res. J. Pharm. Biol. Chem. Sci.*, vol. 7, no. 1, pp. 1752–1755, 2016.
[22] T. Bhattasali, K. Saeed, N. Chaki, and R. Chaki, "A Survey of Security and Privacy Issues for Biometrics Based Remote Authentication in Cloud," in *Computer Information Systems and Industrial Management*, 2014, pp. 112–121.
[23] D. Shah and V. Haradi, "IoT Based Biometrics Implementation on Raspberry Pi," *Procedia Comput. Sci.*, vol. 79, pp. 328–336, Jan. 2016.
[24] P. Rajeswari, S. Viswanadha Raju, A. S. Ashour, and N. Dey, "Multi-fingerprint Unimodel-based Biometric Authentication Supporting Cloud Computing," in *Intelligent Techniques in Signal Processing for Multimedia Security*, N. Dey and V. Santhi, Eds. Cham: Springer International Publishing, 2017, pp. 469–485.
[25] H.-H. Zhu, Q.-H. He, H.-H. Zhu, H. Tang, and W.-H. Cao, "Voiceprint-biometric template design and authentication based on cloud computing security," in *2011 International Conference on Cloud and Service Computing*, 2011, pp. 302–308.
[26] K. Nova, A, Umaamaheshvari, S. S. Jacob, G. Banu, M. S. P. Balaji, and S, Srithar, "Floyd–Warshalls algorithm and modified advanced encryption standard for secured communication in VANET," *Measurement: Sensors*, vol. 27, p. 100796, Jun. 2023.

[27] S. Das, B. Wang, Z. Tingle, and L. Jean Camp, "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review," *arXiv [cs.CR]*, 16-Aug-2019.
[28] A. Nallathambi and K. Nova, "Deep Learning-Enabled Edge Computing and IoT," in *Convergence of Deep Learning and Internet of Things: Computing and Technology*, IGI Global, 2023, pp. 71–95.
[29] M. Reddy, A. Bodepudi, M. Mandapuram, and S. S. Gutlapalli, "Face Detection and Recognition Techniques through the Cloud Network: An Exploratory Study," *ABC j. adv. res.*, vol. 9, no. 2, pp. 103–114, Dec. 2020.
[30] F. Pesapane, C. Volonté, M. Codari, and F. Sardanelli, "Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States," *Insights Imaging*, vol. 9, no. 5, pp. 745–753, Oct. 2018.
[31] A. de Melo e Silva, J. J. Costa Gondim, R. de Oliveira Albuquerque, and L. J. García Villalba, "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence," *Future Internet*, vol. 12, no. 6, p. 108, Jun. 2020.
[32] R. K. Banyal, P. Jain, and V. K. Jain, "Multi-factor Authentication Framework for Cloud Computing," in *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation*, 2013, pp. 105–110.
[33] A. Bodepudi and M. Reddy, "Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review," *IJIC*, vol. 4, no. 1, pp. 1–18, Jan. 2020.
[34] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, Dec. 2019.
[35] V. Talreja, T. Ferrett, M. C. Valenti, and A. Ross, "Biometrics-as-a-service: A framework to promote innovative biometric recognition in the cloud," in *2018 IEEE International Conference on Consumer Electronics (ICCE)*, 2018, pp. 1–6.
[36] A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy, and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications," *IEEE Netw.*, vol. 33, no. 2, pp. 82–88, Mar. 2019.
[37] M. Reddy and A. Bodepudi, "Analysis of Cloud Based Keystroke Dynamics for Behavioral Biometrics Using Multiclass Machine Learning," *RRST*, vol. 2, no. 1, pp. 120–135, Oct. 2022.
[38] I. Sarhan and M. Spruit, "Open-CyKG: An Open Cyber Threat Intelligence Knowledge Graph," *Knowledge-Based Systems*, vol. 233, p. 107524, Dec. 2021.
[39] K. El Asnaoui, Y. Chawki, and A. Idri, "Automated Methods for Detection and Classification Pneumonia Based on X-Ray Images Using Deep Learning," in *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*, Y. Maleh, Y. Baddi, M. Alazab, L. Tawalbeh, and I. Romdhani, Eds. Cham: Springer International Publishing, 2021, pp. 257–284.
[40] J. Zhao, Q. Yan, J. Li, M. Shao, Z. He, and B. Li, "TIMiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data," *Comput. Secur.*, vol. 95, p. 101867, Aug. 2020.
[41] A. Bodepudi and M. Reddy, "Spoofing Attacks and Mitigation Strategies in Biometrics-as-a-Service Systems," *ERST*, vol. 4, no. 1, pp. 1–14, Feb. 2020.
[42] K. Nova, "Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence," *International Journal of Information and Cybersecurity*, vol. 6, no. 1, pp. 21–42, 2022.
[43] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and Accuracy of Fingerprint-Based Biometrics: A Review," *Symmetry* , vol. 11, no. 2, p. 141, Jan. 2019.
[44] A. Bodepudi and M. Reddy, "Cloud-Based Gait Biometric Identification in Smart Home Ecosystem," *International Journal of Intelligent Automation and Computing*, vol. 4, no. 1, pp. 49–59, 2021.
[45] K. Nova, "Machine Learning Approaches for Automated Mental Disorder Classification based on Social Media Textual Data," *CIBSS*, vol. 7, no. 1, pp. 70–83, Apr. 2023.
[46] M. Sajjad *et al.*, "CNN-based anti-spoofing two-tier multi-factor authentication system," *Pattern Recognit. Lett.*, vol. 126, pp. 123–131, Sep. 2019.

[47] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Comput. Secur.*, vol. 63, pp. 85–116, Nov. 2016.
[48] J.-J. Kim and S.-P. Hong, "A method of risk assessment for multi-factor authentication," *Journal of Information Processing Systems*, 2011.