Sri Lanka Institute of Information Technology

BSc Honors in Information Technology Specializing in Cyber Security

Biometric Security and Cyber Security

Individual Assignment

IE2022 – Introduction to Cyber Security

Submitted by:

Name	Student Registration Number
NAWARATHNA.N.P.D.T	IT22117496

Main topics

1.Abstract

This report provides a thorough analysis of biometric security, a rapidly developing area at the forefront of identification and access management in the digital era. We explore the fundamental ideas behind biometrics, the technology that supports it, practical applications, and ethical issues that affect how it is used. With its roots in the distinctive biological and behavioral characteristics that make each of us unique, biometric security is a potent tool for enhancing both security and user comfort. This research examines the many modalities that allow for biometric authentication, ranging from voice and behavioral biometrics to fingerprint and facial recognition. In order to maintain the crucial balance between security and individual rights, we also highlight the ethical issues related to the collecting and administration of biometric data. This paper outlines the potential future of biometric security as it continues to develop and become more pervasive in our daily lives, highlighting the significance of research, standardization, and the ethical development of these game-changing technologies.

2.Introduction

A secure and convenient authentication process is essential in a time when many parts of our life are being digitally transformed. The use of distinctive physiological and behavioral features for identity verification through biometric security has grown significantly in popularity. This paper explores the ideas, technologies, applications, and ethical issues surrounding the field of biometric security. The basis for biometric identification is the idea that every person has unique biometric characteristics, such as fingerprints, facial features, iris patterns, and voiceprints. The foundation for secure identification and access management is these distinctive qualities. Biometrics offers a more reliable and convenient means of authentication than more conventional techniques like passwords or Pins. Beginning with an explanation of the numerous biometric modalities and the technology used to collect, process, and match biometric data, the study goes on to discuss biometrics in general. It examines the difficulties with biometric security, including privacy issues, potential flaws, and the requirement for stronger anti-spoofing safeguards. Examples from the real world show how important and useful biometric security is in a variety of fields, such as financial services, border control, and smartphone security. The development and use of biometric technologies must give careful thought to ethical issues. The discussion in the paper covers topics including privacy, consent, surveillance, bias, and the ethical handling of biometric data. It draws attention to moral issues and the need for a careful balance between personal freedom and security.

3.Biometric security

Evolution of Biometric Security:

1.1 Early adoption

An important turning point in the history of security and identity was highlighted by the early deployment of biometric security. It paved the way for the complex biometric systems in use today, improving the security and dependability of identification verification. Here, we examine this historical journey using actual instances and turning points.

In some examples,

1. Ancient Civilizations and Handprints

   The history of biometric security identify trough early civilizations. Around 1900 BC, fingerprint impressions were used as signatures on clay tablets in ancient Babylon. Like how modern seals feature distinctive engravings, ancient Egyptians used them to confirm identity. These early examples indicate how humans naturally recognize the singularity of certain physical traits, such as handprints.

2. The Formation of the FBI and National Databases:

Division of the FBI which is called The Criminal Justice Information Services (CJIS) was founded in 1924 and was initially known as the Identification Division. This signaled a significant advancement in the use of biometric security. For law enforcement agencies all throughout the nation to access and contribute to a consolidated repository of fingerprint records, the FBI was charged with maintaining and growing a national fingerprint database. The modernization of the American criminal justice and identification systems was made possible in large part by this program. [1]

3. London fingerprint bureau turns 100:

The Henry Classification System, developed by Englishman Edward Henry in 1901, allowed for the systematic categorization and arrangement of fingerprint records. The Fingerprint Bureau at Scotland Yard was built on this breakthrough. The usefulness of fingerprint identification to solving crimes was demonstrated by actual criminal cases, such as the infamous 1905 case of the "Bovingdon Cuckoo Twins," Alfred and Albert Stratton. A crucial turning point in the acceptability of biometric security was reached with their convictions based on fingerprint evidence. [2]

1.2 Mobile device integration

A contemporary change in how we authenticate and secure our smartphones and other portable devices has been brought about by the incorporation of biometric security into mobile devices. Our daily interactions with technology have been made simpler because of this shift, which has also increased the security of our devices. The development of mobile device integration in biometric security and its practical ramifications will be discussed in this conversation.

PINs (Personal Identification Numbers) and passwords served as the starting point for the transition to biometric security in mobile devices. However, these techniques included built-in flaws including stealing propensity, forgetfulness, or openness to observation.

In some examples,

1.Apple's touch ID:

The first apple's touch id released in 2013 with the iPhone 5s. The practicality and ease of biometric security in mobile devices were proved by Touch ID. Users only needed to press their registered finger on the home button to unlock their iPhones. Along with enhancing security, it also made procedures like Apple Pay mobile payments simpler. The success of Touch ID paved the way for other biometric advancements. [3]

2.Apple’s face ID (Face recognition)

First apple’s face ID released in November 2017 with iPhone X. It is the next major advancement of biometric security in the world. That system works with sensors and the camera to identify the face and work it for the purpose. This mechanism is used to unlock devices, secure the payments, secure the apps that are even safer and simpler. [4]

3.Mobile Banking Apps

The integration of biometric security measures in mobile banking apps improves the security of financial transactions and account access while providing a practical and user-friendly experience. Users gain from the security that biometric authentication provides, knowing that their financial information is well guarded**.** According to the information I got from the internet the best mobile banking app in the world is “Citi Mobile”. It can be used by both android and iOS users on their mobile devices. That app is more secure with biometric security. [5]

1.3 Diverse modalities

Different biometric security modalities signify a strategic change in how we verify and authenticate people. Diverse modalities use a combination of special biological and behavioral qualities to increase the accuracy and security of identity verification rather than depending exclusively on one biometric characteristic, such a fingerprint or facial scan. This multidimensional strategy acknowledges that every person has a variety of distinguishing characteristics, from the ridges on their fingertips to the tone of their voice.

In some examples,

1. Fingerprint Recognition

   One of the most often used biometric modalities is this one. It examines the individual ridge and valley patterns on a person's fingertip. Because each person's fingerprints are unique, they serve as a trustworthy biometric attribute.

2.Face Recognition

The facial traits of a person are used in facial biometrics to identify them. It examines distinctive facial features such the separation between the eyes, nose shape, and facial curves.

3. Voice Recognition

   This mechanism requires users voice, including pitch, tone, and speech patterns. Systems for voice authentication frequently use it.

4. Hand Geometry

   In cybersecurity, the term "hand geometry" refers to a biometric authentication technique that recognizes people based on the physical traits of their hands. This method records and examines the dimensions and proportions of a person's hand, including the size and length of the fingers, the spacing between joints, and other aspects. For authentication reasons, hand geometry systems compare a digital representation of the hand to a template that is maintained using specialized cameras or scanners. This technique is well-known for being dependable, simple to use, and inexpensive, making it a viable choice for access control and identity verification in a variety of contexts with high security requirements. Even if it works well, privacy issues and the potential for duplication still exist, which has led to the combination of hand geometry with other biometric technologies to improve overall security measures. In addition,

improvements in machine learning and artificial intelligence are constantly enhancing hand geometry systems, making them more reliable and precise, hence broadening their application in a variety of cybersecurity scenarios.

1.4 Ai and machine learning

In order to recognize and authenticate people based on their distinctive biological or behavioral attributes, artificial intelligence (AI) and machine learning have revolutionized biometric security. The data preparation and feature extraction processes at the heart of these systems automatically extract pertinent features from raw biometric data using deep learning models like Convolutional Neural Networks (CNNs) and AI algorithms. After that, supervised machine learning methods are used for pattern recognition, utilizing labeled datasets to train models that can recognize or validate people. These models compute similarity scores between the retrieved characteristics and saved templates using matching algorithms like Support Vector Machines (SVMs) or Random Forests. Through access restriction and encryption, AI is also essential in ensuring the security of biometric templates. Additionally, it makes use of the anomaly detection powers of deep learning to identify and counteract spoofing efforts. AI increases system robustness by enabling continuous

authentication and flexibility to be changing biometric features. Additionally, AI makes it possible to combine many biometric modalities for better accuracy, and data security is guaranteed by privacy preservation techniques like federated learning. In general, AI and machine learning enable biometric security systems to provide extremely precise, flexible, and safe means of user authentication and identification in a variety of applications, from smartphones to high-security access control. [6]

In some examples,

1.Image Recognition

Most important applications of machine learning and artificial intelligence is image recognition. In essence, it is a method for locating and detecting an element or object within a digital image. Further analysis using this method includes pattern recognition, face detection, face recognition, optical character recognition, and many other things.

2.Voice Recognition

A biometric authentication method is voice authentication. The use of distinctive physical characteristics like fingerprints, facial features, or even someone's iris as a method of user verification is known as "biometrics," a particular word. Voice authentication

uses a user's speech to verify their identity. Voice recognition is a type of biometrics. Voice and user speech can act as a distinctive marker of a person's ID, like fingerprints and facial scans. Because of this, speech authentication offers many of the same benefits as other biometric technologies. [7]

1.5 Privacy Concerns

Biometric security system privacy issues are complex and call for serious attention. The possibility of identity theft and data breaches is one of the main worries. People are susceptible if databases containing their biometric templates are breached since, unlike passwords, biometric data cannot be easily changed once it has been compromised. Mass surveillance is another urgent issue, since the widespread use of biometric technology in public places and government organizations raises concerns about ongoing monitoring that could violate people's civil liberties and privacy. Furthermore, serious risks to personal privacy come from the collecting of biometric data without people's awareness or agreement, as well as from its potential exploitation for unintended uses. Inaccuracy in biometric systems can lead to false accusations and invasions of privacy. These privacy issues are further complicated by the lack of defined regulations for the collecting and storage of biometric data as well as worries about

data security, permission, algorithmic bias, and function creep. The appropriate and ethical use of biometric technology while preserving people's right to privacy must be ensured, which calls for strong data protection measures, transparency, and explicit legislation.

In some examples,

1. Government Use of Facial Recognition:

   Face recognition technology has been used by several nations to monitor people in public areas, airports, and government facilities. Mass surveillance and the possible misuse of this technology to track citizens' whereabouts without their permission have drawn criticism.

2. Smartphones and Fingerprint Data:

   Privacy issues have been brought up by biometric authentication techniques like smartphone fingerprint recognition. Law enforcement authorities have on occasion made people use their fingerprints to unlock their phones, raising concerns about forced self-incrimination and the security of biometric information.

3. Healthcare and Biometric Data Breaches:

Data breaches have happened in healthcare institutions that employ biometric data for patient identification and access control. These hacks disclose patient biometric data in addition to sensitive medical information, raising worries about fraud and identity theft.

4. Facial Recognition in Schools:

   For security reasons, some schools have installed facial recognition technology. However, this has raised debate concerning the monitoring of pupils, highlighting issues with respect to privacy, permission, and the possibility for data exploitation.

5. Healthcare and Biometric Data Breaches:

   Data breaches have happened in healthcare institutions that employ biometric data for patient identification and access control. These hacks disclose patient biometric data in addition to sensitive medical information, raising worries about fraud and identity theft. Under this topic there are lots of examples which related foe this. They are,

1.Tricare Data Breach.

A data breach involving personally identifiable and protected health information (PII/PHI) affecting an estimated 4.9 million military clinic and hospital patients was reported by Science Applications International on Wednesday, according to TRICARE, which offers civilian health benefits for service members, retirees, and their dependents. The breach, which SAIC reported on September 14, involved backup tapes from an electronic medical record that was used by the military health system (MHS) to collect patient data from 1992 to September 7, 2011. [8] [9] [10]

1. Community Health Systems Data Breach

A significant US hospital network claimed to have fallen victim to a cyber-attack that stole the personal information of 4.5 million patients. The attack took place between April and June of this year, and according to Community Health Systems, it had Chinese origins. Names, residences, birthdates, phone numbers, and social security numbers of the patients were among the information. Affected patients are currently being notified by the company, which manages 206 hospitals in 29 states. The information might be used to steal people's identities, a security expert cautioned. The FBI acknowledged to the news organization Reuters that it was looking into the incident. Community Health Systems emphasized that it didn't think any credit card information or medical records were taken.

2. UCLA Health Data Breach

In October 2014, UCLA Health discovered suspicious behavior on its network and asked the FBI for assistance. Although it was first believed that hackers did not access the areas of the network that were used to hold patient medical information, the forensic examination proved that hackers had been successful in accessing its network. On May 5, 2015, UCLA announced that the hackers may have accessed or copied names, addresses, dates of birth, Medicare IDs, health insurance information, and Social Security numbers after gaining access to portions of the network that included patients' protected health information. The incident affected 4.5 million patients in all.

2.Future Developments in Biometric Security:

2.1 continuous authentication

A cutting-edge approach to biometric security called continuous authentication redefines the traditional concept of single-point authentication. Continuous authentication continuously monitors and confirms the user's identity

throughout their active session or interaction with a system, as opposed to only authenticating a user once at the point of login or first access. This preventative strategy is aware that security threats can still exist even after the initial login because sessions could be abandoned or unauthorized users could access an authenticated session. Continuous authentication makes use of a range of biometric and behavioral characteristics, including heart rate monitoring and gait analysis as well as fingerprint, facial, voice, and facial expression identification. At regular intervals, it gathers and examines information from these factors and compares it to the reference template created during the first authentication. To identify when deviations are serious enough to warrant responses, such as demanding re-authentication, locking the session, or alerting administrators, thresholds are specified. This technique adds an extra layer of defense against potential security breaches and is particularly useful in high-security settings like financial transactions or healthcare systems. It continuously monitors user identity while also working to limit disturbance to the user experience and address significant privacy issues by disclosing data gathering to users and offering opt-out choices.

According to some real-world examples,

1. Voice Recognition in Call Centers:

Voice recognition software is frequently used in call centers to verify clients. Continuous authentication makes it possible to confirm that the caller is the same as the identity-verification source.

2. Smartphones and Mobile Devices:

   Smartphones frequently utilize continuous authentication, such as fingerprint or facial recognition, to make sure the user is the same throughout their interactions with the device.

3. Airport Security and Passport Control:

   In order to confirm that a passenger boarding a flight is the same person who checked in at the airport and passed through security, biometric techniques like face recognition are utilized for continuous authentication at international airports.

4. Vehicle Security:

   Continuous authentication is used for access control in some high-end autos. During the trip, the car may keep an eye on the driver's face or fingerprint to make sure they are the authorized user.

5. Video Conferencing Security:

As remote work becomes more prevalent, video conferencing services may employ continuous authentication to confirm that the individual joining a conference is the authorized user.

2.2 Multi modal biometric

Multimodal biometric authentication is a cutting-edge biometric security strategy that uses numerous biometric characteristics or modalities to simultaneously confirm a person's identification. Utilizing the advantages of different biometric traits, this method offers a more reliable and precise method of verification. Each biometric modality has advantages and disadvantages, and multimodal systems are made to get around these restrictions.

A multimodal biometric system collects and compares a variety of biometric data, including fingerprints, face features, iris scans, voice recognition, and even behavioral patterns like gait analysis. The system can improve accuracy and security by utilizing several modalities. For instance, integrating a fingerprint scan with facial recognition can greatly lower the risk of unwanted access, even if a fingerprint scan alone may be vulnerable to problems like false positives caused by damaged skin or latent prints.

Systems using multimodal biometrics provide several benefits. They are more resistant to spoofing and impersonation efforts since it would be very difficult for an attacker to imitate many biometric features at once. They also offer improved precision and dependability, which lowers the possibility of false positives and false negatives. Additionally, multimodal systems are more flexible to a variety of real-world settings and can function well even in difficult situations, such as dimly lit areas or when users have special needs that limit the usability of some biometric modalities.

In this system have many advantages, they also have drawbacks, including more demanding hardware and processing needs, potential privacy issues, and the necessity for good fusion algorithms to efficiently combine data from many sources. Multimodal systems, however, play a crucial role in meeting the requirement for better, more dependable authentication techniques across a wide range of applications, healthcare, as biometric security continues to advance.

When we use this to real world examples,

1. Border Control and Immigration:

   Global border control organizations now frequently use biometrics. For reliable and quick identification of citizens and foreign visitors, many nations throughout the world are

deploying or have already implemented biometric border security systems. To track and manage the flow of people across borders, border security biometric systems use national database deployments in entry and exit systems, immigration, and e-passports. More advanced technology, such as multimodal biometric identification, are now thought to be more trustworthy for enhancing border control security.

*Why border control and immigration use multi modal biometrics?

Disasters like the attack on the twin towers in the US on September 11, 2001, and the missing of Malaysian Airlines Flight MH370 have sparked concern about the need for precise identification in ports of entry and other border control settings. Additionally, the terrible escalation of conflict and bloodshed in many nations at the start of the twenty-first century has resulted in a sharp surge in the number of people fleeing their homes across borders in order to avoid persecution and violence. Governments are also being pressured to consider tighter border control security standards as a result of the tragedy of human

trafficking and an increase in criminal activity. Recently, the terrorist organization ISIS attacked Iraq and issued an international call for additional terrorists to join them. The warriors arrived using false passports. This is why lots of countries use multi modal biometric for their immigration and border process. [11]

2.3 Ethical consideration

Since the implementation of biometric technologies has significant ramifications for people's privacy, autonomy, and civil liberties in biometric security are crucial. First and foremost, privacy issues are raised by the collecting and storage of biometric data. Because each person's fingerprints, iris scans, or facial features are unique, biometric data is incredibly sensitive. The collection and storage of this data by businesses without explicit authorization is unethical, as is the possibility of data breaches or misuse.

The potential for tracking and surveillance is a crucial ethical factor. When used extensively, biometric technologies can enable widespread surveillance, raising concerns about mass surveillance and the diminution of personal freedoms. To avoid the unauthorized use of biometric technologies for ongoing monitoring or tracking, it is crucial to establish defined

boundaries. Additionally, the consent issue is crucial. The right of individuals to decide how their biometric data is gathered, used, and shared should exist. Consent must be freely given, informed, and explicit, and people should be able to revoke it at any time. Transparency should also be maintained regarding who has access to and how biometric data is used.

Additionally, ethical issues with biometric security include bias and prejudice. If they are not sufficiently designed and tested across various demographic groups, biometric technologies may show bias. This may have discriminatory effects, especially on disadvantaged groups. To avoid unfair treatment based on race, gender, or other protected characteristics, ethical considerations include guaranteeing fairness and minimizing bias. Biometric data storage over time and potential abuse are additional issues. To avoid unauthorized use or data breaches, it is essential to ensure safe storage and access controls.

Some examples for ethical consideration,

1.The Password less Future:

In the future world most companies will use passwords less concept for their systems. They are currently examining the primary subjects of discussion, which include how biometric data is used,

stored, preserved, and disclosed. In many parts of the world, securing personal data is not only required by law but is also strictly regulated. This is important for business owners. The General Data Protection Regulation (GDPR) of the European Union, for instance, considers biometric data to be sensitive information that requires the subject's informed consent. Legal penalties and fines for breaking GDPR regulations could harm a company's reputation. Several federal and state laws also apply to biometrics in the United States. The repercussions of breaking these laws and regulations are just as serious as breaking the GDPR. The Biometric Information Privacy Act (BIPA) made Illinois the first state in the United States to pass biometric law in 2008. Since then, more than 25 states including Texas, Washington, California, New York, Louisiana, Oregon, and Arkansas—have passed laws requiring the use of biometrics in some capacity. These state laws govern the gathering, storage, disclosure, and disposal of biometric data as well as other matters. [12]

2.4 Enhanced anti-spoofing.

A significant development in biometrics which focuses on preventing fraudulent efforts to trick biometric authentication systems is enhanced anti-spoofing in biometric security. The deliberate use of false biometric information, such as made-up voice recordings, pictures, or fingerprints, to pass for a real user and get access without authorization is known as spoofing. The security and dependability of biometric systems are strengthened by enhanced anti-spoofing solutions that are intended to recognize and foil these spoofing efforts. Several advanced strategies are used to produce stronger anti-spoofing.

Utilizing liveness detection, a typical strategy, seeks to evaluate the "liveness" of the supplied biometric feature. For instance, sensors can distinguish between a living finger and a static, lifeless object in the case of fingerprint recognition by detecting characteristics like pulse or skin flexibility. In order to confirm the presence of a real person, facial recognition systems may examine blinking or facial movements.

Multi-modal biometrics, which combine various biometric characteristics to cross-verify the user's validity, is another method. For instance, it becomes significantly more difficult for an attacker to effectively spoof both modalities when fingerprint and iris scans are combined. Algorithms for artificial intelligence and machine learning are also used to continuously adjust and enhance anti-spoofing defenses. The ability of these algorithms to spot trends and anomalies in biometric data makes it harder for spoofers to trick the system. In the implementation of improved anti-spoofing methods, ethics come first. It's crucial to strike a balance between user privacy and strong security. Although strict anti-spoofing techniques increase security, they must not violate people's rights or introduce unfair practices.

In some real-world examples,

1.ATMs and Cash Machines:

In the current world, ATMs, which allow for cash transfers and withdrawals, are used by almost everyone. This work's base is the ATM System's fingerprint technology. We chose this field in order to improve transactional efficiency and personal safety. Each individual's fingerprints are unique. There is no risk of losing an ATM card, and you are not required to always have one with you. When comparing various ATM security solutions, fingerprint technology performs more reliably and safely than others. These factors make this mechanism a simple and secure means of transaction and also provide a consistent environment between customers and ATMs. The newest technology for electronic cash transactions is this. [13]

2.E-Government Services:

The value of having safe and effective public services in the modern world cannot be overstated. Government organizations are entrusted with delivering essential services to citizens while simultaneously protecting their private and sensitive information, from healthcare to transportation. Many government entities are using biometrics as a method of identification verification to increase security and efficiency.

A very secure and accurate technique of identifying people is provided by biometric technology, which includes iris, fingerprint, and facial recognition. Government organizations that place a high priority on protecting sensitive information will find this technology to be extremely helpful. Government organizations can ensure that only authorized people have access to sensitive information by utilizing biometric technology, reducing fraud and identity theft. [14]

4.Conclusion

A crucial part of contemporary identification, biometric security now provides a safe and practical way to confirm identity. The key components of biometric security have been clarified in this paper, from its fundamental theories and technological underpinnings to its practical applications and moral issues. It is critical to solve current issues and discover new opportunities as biometric security technologies develop further. Future research should focus on improving anti-spoofing safeguards to guard against fraud attempts, reducing bias and discrimination in biometric systems, and developing ethical standards for the responsible use of biometric information.

It is impossible to exaggerate the value of biometric security in protecting sensitive data and guaranteeing secure access in a society where digital interactions are pervasive. Biometric security will be crucial in influencing the future of safe authentication in the digital age through ongoing research and ethical issues.

Despite the noteworthy advancements made in biometric security, there are still problems and opportunities for additional research and improvement. For example, improved anti-spoofing methods are essential to thwart fraudulent attempts to trick biometric systems. To remain ahead of possible attackers that try to exploit flaws in these systems, ongoing study in this field is crucial.

As biometric security becomes increasingly prevalent, interoperability and standardization are topics that require attention. For greater adoption and integration, it is crucial to make sure that various biometric systems can cooperate easily and follow similar guidelines.

The accuracy of biometrics must continually be improved. For a more seamless and dependable user experience, biometric systems should work to minimize false positives and false negatives. This calls for improving matching algorithms and investigating fresh approaches to data analysis. Scalability is a problem that needs to be addressed in biometric security research and development. Biometric systems must be able to accommodate different user groups and operating circumstances as they are implemented in bigger and more varied locations.

Future research should focus on creating biometric systems that can adjust to changes in an individual's biometric characteristics over time, such as aging or injury. It is vital to guarantee that users may access systems and services even if their biometric characteristics change. There is a lot of room for more study in the field of behavioral biometrics. Continuous authentication and improved fraud detection can be achieved by the monitoring of behavioral features, such as gait analysis and keystroke dynamics. The goal of this research should be to improve algorithms and broaden the use of certain behavioral characteristics.

5.Refferencess

[1] Z. Whittaker, "/tech," 8 8 2017. [Online]. Available: https://www.zdnet.com/article/fbi-to-keep-secret-biometrics-database-justice-department/.

[2] Associated Press, "dessertnews," deseret, 1 7 2001. [Online]. Available: https://www.deseret.com/2001/7/1/19594053/london-fingerprint-bureau-turns-100. [Accessed 13 10 2023].

[3] J. Weatherbed, "the verge," theverge, 12 9 2023. [Online]. Available: https://www.theverge.com/23868464/apple-iphone-touch-id-fingerprint-security-ten-year-anniversary. [Accessed 12 10 2023].

[4] Wikipedia, "Face id," 8 10 2023. [Online]. Available: https://en.wikipedia.org/wiki/Face_ID. [Accessed 13 10 2023].

[5] C. Horton, "fordes advisor," forbes, 3 10 2023. [Online]. Available: https://www.forbes.com/advisor/banking/best-mobile-banking-apps/. [Accessed 13 10 2023].

[6] A. Vasilchenko, "mobidev," mobidev.biz, 22 4 2022. [Online]. Available: https://mobidev.biz/blog/ai-biometrics-technology-authentication-verification-security. [Accessed 13 10 2023].

[7] R. Pinto, "1kosmos," 1kosmos, 28 9 2021. [Online]. Available: https://www.1kosmos.com/biometric-authentication/voice-authentication/#:~:text=Voice%20recognition%20is%20a%20form%2

0of%20biometrics%2C%20and,as%20a%20unique%20marker%20of%20a%20user%E2%80%99s%20ID.. [Accessed 13 10 2023].

[8] e. kost, "Data Breaches," upguard, 3 9 2023. [Online]. Available: https://www.upguard.com/blog/biggest-data-breaches-in-healthcare. [Accessed 13 10 2023].

[9] M. Merrill, "healthcareitnews," healthcareitnews, 29 9 2011. [Online]. Available: https://www.healthcareitnews.com/news/tricare-breach-puts-49m-milatry-clinic-hospital-patients-risk#:~:text=The%20breach%20was%20reported%20by%20SAIC%20on%20Sept.,even%20though%20the%20patients%20were%20receiving%20treatment%20elsewhere.. [Accessed 13 10 2023].

[10] Community Health Systems has 206 hospitals across the US, "news," bbc, 18 8 2014. [Online]. Available: https://www.bbc.com/news/technology-28838661. [Accessed 13 10 2023].

[11] A. Hussain, "betanews," betanews, 10 10 2014. [Online]. Available: https://betanews.com/2014/10/30/how-multimodal-biometrics-improves-border-control-security/. [Accessed 12 10 2023].

[12] J. Lunter, "ethical implication," solutionsreview, 24 8 2022. [Online]. Available: https://solutionsreview.com/identity-management/the-ethical-implications-and-legal-responsibilities-of-biometric-data-security/. [Accessed 9 10 2023].

[13] M. K. A. a. M. K. T Sangeetha, "iopScience," iop, 23 2 2022. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1916/1/012033. [Accessed 13 10 2023].

3
]

[khumopancy counsulting, "linkedin," linkedin, 7 2 2023. [Online].
1 Available: https://www.linkedin.com/pulse/biometrics-government-
4 improving-security-efficiency-/. [Accessed 13 10 2023].
]