Biometric Authentication for Secure Health Information Management

Slotta Michelene*

Department of Mechanical Engineering, University of Alberta, Canada

Correspondence to:

Slotta Michelene
Department of Mechanical Engineering,
University of Alberta, Canada,
Email: michelene@shaw.ca

Citation: Michelene S (2023). Biometric Authentication for Secure Information Management. EJBI. 19 (2):160-161.

DOI: 10.24105/ejbi.2022.19.2.160-161

Received: 04-Feb-2023, Manuscript No. ejbi-23-93728;
Editor assigned: 07-Feb-2023, Pre QC No. ejbi-23-93728 (PQ);
Reviewed: 21-Feb-2023, QC No. ejbi-23-93728;
Revised: 23-Feb-2023, Manuscript No. ejbi-23-93728(R);
Published: 27-Feb-2023

1. Introduction

In the healthcare industry, there is a constant need to ensure that patient data is kept secure and confidential. With the increasing amount of sensitive data being stored digitally, it has become essential to implement strong authentication mechanisms to protect patient privacy. Biometric authentication is one such mechanism that has gained popularity in recent years. Biometric authentication involves using a person‘s unique physiological or behavioral characteristics to verify their identity. Some common examples of biometric data include fingerprints, facial recognition, iris scans, and voice recognition. Biometric authentication is more secure than traditional authentication methods like passwords and PINs because it is difficult to replicate or steal biometric data.

Healthcare organizations can implement biometric authentication in several ways. For example, hospitals can use biometric authentication to access electronic health records (EHRs) or prescription information. Patients can also use biometric authentication to verify their identities when accessing their health records or making appointments. One major benefit of biometric authentication in healthcare is the improved security it provides. With biometric authentication, patient data is more secure and less vulnerable to cyber-attacks. Additionally, biometric authentication can help healthcare organizations comply with regulations like HIPAA, which mandate the protection of patient data. However, there are also some challenges associated with biometric authentication. One major challenge is the need for specialized hardware and software to collect and store biometric data. Additionally, there are concerns around the privacy and ethical implications of collecting and storing biometric data.

Biometric authentication is a technology that uses human physiological and behavioral characteristics to verify the identity of an individual. In healthcare, biometric authentication has become increasingly important for securing sensitive patient health information. This paper explores the use of biometric authentication for secure health information management. The paper discusses the advantages and challenges of biometric authentication in healthcare, including the accuracy and reliability of biometric technology, the ethical concerns associated with biometric data collection, and the potential benefits of biometric authentication for patient privacy and security.

With the growing use of electronic health records (EHRs) and digital healthcare systems, there is a need for secure methods of authentication to ensure that patient health information is kept confidential and protected from unauthorized access. Biometric authentication is a technology that can help address these concerns. Biometric authentication uses an individual‘s unique physiological or behavioral characteristics to verify their identity. Examples of biometric identifiers include fingerprints, facial recognition, voice recognition, and iris scans. Biometric authentication can help ensure that only authorized individuals have access to sensitive patient health information, while also improving the overall efficiency of healthcare delivery [1].

Advantages of Biometric Authentication

The use of biometric authentication in healthcare has several advantages. First, biometric authentication provides a high level of accuracy and reliability in verifying an individual‘s identity. Biometric identifiers are unique to each individual and cannot be easily replicated, making it difficult for unauthorized users to gain access to sensitive patient health information. Additionally, biometric authentication eliminates the need for passwords or other traditional forms of authentication that can be easily lost or stolen [2].

While biometric authentication offers many advantages, there are also several challenges associated with its use in healthcare. One of the biggest challenges is the accuracy and reliability of biometric technology. While biometric identifiers are unique to each individual, there can be variations in the way that the biometric data is captured and processed, which can lead to errors in authentication. Additionally, there are ethical concerns associated with the collection and use of biometric data, particularly with regards to patient privacy and data security [3].

In conclusion, biometric authentication is a promising technology that can improve security in healthcare organizations. However, it is essential to carefully consider the potential benefits and challenges associated with biometric authentication before implementing it in healthcare settings biometric authentication is an important technology for securing sensitive patient health

information. While there are challenges associated with the use of biometric technology in healthcare, such as accuracy and ethical concerns, the potential benefits for patient privacy and security make it a valuable tool for healthcare providers. As the use of digital healthcare systems continues to grow, the use of biometric authentication is likely to become more widespread [4].

Tencent is developing a number of medical services and systems. These include Tencent Doctorwork, WeChat Intelligent Healthcare, and AI Medical Innovation System (AIMIS), a diagnostic medical imaging service powered by artificial intelligence [5]. Applications that employ AI to provide medical consultation based on user medical histories and general medical knowledge include Babylon Health‘s GP at Hand, Ada Health, AliHealth Doctor You, KareXpert, and Your.MD. Users enter their symptoms through the app, which compares them against a database of ailments using speech recognition. After that, Babylon provides a suggested course of action while taking the user‘s medical history into account. Seven business model models have been successfully used by healthcare entrepreneurs to provide AI solutions to the market. These archetypes depend on the value produced for the target user (e.g., the focus on patients versus the focus on healthcare providers and payers) and value capture techniques (e.g. providing information or connecting stakeholders).

2. Conclusion

However, it is essential to carefully consider the potential benefits and challenges associated with biometric authentication before implementing it in healthcare settings biometric authentication is an important technology for securing sensitive patient health information. While there are challenges associated with the use of biometric technology in healthcare, such as accuracy and ethical concerns, the potential benefits for patient privacy and security make it a valuable tool for healthcare providers. As the use of digital healthcare systems continues to grow, the use of biometric authentication is likely to become more widespread.

3. References

1. Doukas C, Pliakas T, Maglogiannis I. Mobile healthcare information management utilizing Cloud Computing and Android OS. In2010 Annual International Conference of the IEEE Engineering in Medicine and Biology 2010; 1037-1040). IEEE.
2. Chaudhry B, Wang J, Wu S, Maglione M, Mojica W, Roth E, et al. Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. Ann Intern Med. 2006; 144(10):742-52.
3. Cheng P, Gilchrist A, Robinson KM, Paul L. The risk and consequences of clinical miscoding due to inadequate medical documentation: a case study of the impact on health services funding. Health Inf Manag J. 2009; 38(1):35-46.
4. Braa J, Monteiro E, Sahay S. Networks of action: sustainable health information systems across developing countries. MIS quarterly. 2004; 337-62.
5. Barnes SJ. Information management research and practice in the post-COVID-19 world. Int J Inf Manage. 2020; 102175.