ISSN: 2165-7866

Journal of Information Technology & Software Engineering

OPEN ACCESS Freely available online

Short Communication

Improving and Protecting the Cyber Threats with Biometric Technology

Caroline Steve*

Department of Electronics and Electrical Communications Engineering, Case Western Reserve University, Cleveland, USA

DESCRIPTION

Biometric technology has emerged as a solution to many of the problems faced by people, organizations, and governments in a time when convenience and security are top priorities. We are seeing a dramatic change in how we access our cellophanes, verify ourselves, and safeguard our data as a result of the fast adoption of biometrics in our daily lives. However, this changing environment poses significant concerns about how to strike a balance between the evident benefits of biometrics and the requirement to safeguard people's privacy and civil freedoms [1]. Biometrics is a technology that uses a person's distinctive physical or behavioural characteristics to confirm their identity. Some of the common methods of biometric identification include DNA analysis, iris scanning, voice recognition, facial recognition, and fingerprint and facial recognition. These technologies are swiftly finding their way into a number of industries, including consumer electronics, law enforcement, healthcare, and finance. Although biometrics has many potential benefits, they also raise a number of difficult ethical and privacy issues [2-4].

One of the most significant advantages of biometric technology is its ability to enhance security. Traditional methods of authentication, such as passwords or PINs, are susceptible to being forgotten, stolen, or shared. Biometric identifiers, on the other hand are unique to each individual and difficult to replicate. Fingerprint recognition, for instance offers a higher level of security than a simple four-digit PIN, reducing the risk of unauthorized access to personal or sensitive information [5]. They can eliminate the need to remember multiple complex passwords or carry physical identity documents. In a world where we are inundated with accounts and digital services, the ease of using a fingerprint or facial scan to unlock a device or access an app can't be overstated. This convenience not only saves time but also simplifies our lives. Furthermore, biometric technology has practical applications in a wide range of industries [6]. In healthcare, biometrics can help ensure patient identity, reduce medical errors, and protect sensitive health information. In law enforcement, it assists in identifying suspects and locating missing persons. The financial sector employs biometrics to enhance security and combat fraud. These examples demonstrate the enormous potential that biometrics hold in transforming various sectors for the better [7].

However, as we access the conveniences and security benefits of biometric technology, we must also address the ethical concerns and potential dangers that accompany its widespread adoption. Biometric data, which is highly sensitive and personal, is collected and stored in various databases. Governments, corporations, and even criminals seek access to this data, raising questions about who controls this information and how it is used [8]. While proponents argue that it can help identify and apprehend criminals more effectively, critics express grave concerns about mass surveillance, potential abuse of power, and the infringement on civil liberties. Cases of misidentification and bias have also come to the fore, highlighting the need for stringent regulations to ensure fair and accurate usage of these technologies. In addition to the privacy concerns, there is also the risk of data breaches and identity theft. Biometric data, once compromised, is irreplaceable. While we can change a password, but we cannot change our fingerprint or facial features [9]. The theft of biometric data can have devastating consequences for individuals, potentially leading to identity theft, unauthorized access, and financial losses. Therefore, the security of biometric databases must be a paramount concern, with robust encryption and protection mechanisms in place [10].

Moreover, the issue of consent and opt-in/opt-out policies remains a significant point of contention. Users often unknowingly provide biometric data when using certain services or devices. To strike a fair balance, individuals should have the choice to opt-in or out of using biometrics for authentication. Consent should always be informed and freely given, ensuring that users have control over their personal information. Facial recognition systems, for instance, have been criticized for having higher error rates in people with darker skin tones, raising questions about algorithmic bias. These inaccuracies can lead to wrongful arrests or unfair treatment, further underscoring the need for transparency and accountability in the development and deployment of biometric technologies [11].

Governments must establish clear and comprehensive regulations governing the use of biometrics, especially in areas where they intersect with individual privacy and civil rights.

Correspondence to: Caroline Steve, Department of Electronics and Electrical Communications Engineering, Case Western Reserve University, Cleveland, USA, E-mail: carste@kjga.edu

Received: 25-Aug-2023, Manuscript No. JITSE-23-27747; **Editor assigned:** 29-Aug-2023, PreQC No. JITSE-23-27747 (PQ); **Reviewed:** 12-Sep-2023, QC No. JITSE-23-27747; **Revised:** 19-Sep-2023, Manuscript No. JITSE-23-27747 (R); **Published:** 26-Sep-2023, DOI: 10.35248/2165-7866.23.13.354

Citation: Steve C (2023) Improving and Protecting the Cyber Threats with Biometric Technology. J Inform Tech Softw Eng. 13:354.

These regulations should encompass data protection, consent, and accountability, ensuring that both public and private entities adhere to best practices. Developers and organizations should provide transparency in their use of biometric data, including how it is collected, stored, and shared. Robust encryption measures must be in place to protect biometric data from unauthorized access. Data breaches can have severe consequences, and security should be a paramount concern [12]. Developers should address issues of bias and inaccuracy in biometric technology by investing in research and development to improve accuracy and inclusivity. Diverse datasets that represent various demographics should be used in the training of these systems.

CONCLUSION

Biometric technology offers tremendous advantages in terms of security and convenience, but it also presents ethical and privacy concerns that demand our attention. Striking a balance between harnessing the potential of biometrics and safeguarding individual privacy and civil liberties is a complex challenge that requires collaboration between governments, businesses, and the public. With the right regulations and responsible usage, biometric technology can be a valuable tool in our digital age.

REFERENCES

1. Yadav S, Singh A. Biometric traits based authentication system for Indian voting system. Int J Comput Appl. 0975-8887;65(15): 150-175.
2. Al-Waisy AS, Qahwaji R, Ipson S, Al-Fahdawi S, Nagem TAM. A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal Appl. 2017;21(3):783-802.
3. Birch I, Raymond L, Christou A, Fernando M.A, Harrison N, Paul F. The identification of individuals by observational gait analysis using closed circuit television footage. Sci Justice 2013;53(3): 339-342.
4. Black SM, Mallett X, Rynn C, Duffield N. Forensic hand image comparison as an aid for paedophile investigations. Police Prof. 2009;184:21-24.
5. Bendjenna H, Zarour N, Charrel PJ. Eliciting requirements for an inter-company cooperative information system. J Syst Inf Technol. 2010;12(4):303-335.
6. Grefen PWPJ, Mehandjiev N, Kouvas G, Weichhart G, Eshuis R. Dynamic business network process management in instant virtual enterprises. Comput Ind. 2009;60(2):86-103.
7. Faundez-Zanuy M, Elizondo DA, Ferrer-Ballester MA, Travieso-González CM. Authentication of individuals using hand geometry biometrics: a neural network approach. Neural Process Lett. 2007;26(3):201-216.
8. Zhang A, Gertych A, Tsao S, liu BJ, Huang HK. Bone age assessment for young children from new born-7 year old using carpal bones. J Comput Med Imaging Graph. 2007;31(4-5):299-310.
9. Chandra A, Calderon T. Challenges and constraints to the diffusion of biometrics in information systems. Commun ACM. 2005;34(12): 101-106.
10. Deane F, Barrelle K, Henderson R, Mahar D. Perceived acceptability of biometric security systems. Comput Secur. 1995;14(3):225-231.
11. Zhu X, He W, Du Y, Zhang K, Lu Y. Interocular symmetry of fixation, optic disc, and corneal astigmatism in bilateral high myopia: the shanghai high myopia study. Transl Vis Sci Technol. 2019;8(1): 22.
12. Falavarjani K.G, Modarres M, Joshaghani M, Azadi P, Afshar AE, Hodjat P. Interocular differences of the Pentacam measurements in normal subjects. Clin Exp Optom. 2010;93(1):26-30.