Mini Review
Volume 14:2, 2023

Journal of Biometrics & Biostatistics

ISSN: 2155-6180 Open Access

Unlocking the Future: Exploring Biometric Applications for Enhanced Security and Convenience

Blemingo Biming*

Department of Biostatistics, University of Dhaka, Dhaka, Bangladesh

Abstract

As technology continues to advance, the realm of biometric applications has emerged as a promising avenue for revolutionizing security and convenience in various industries. Biometrics, the science of measuring and analyzing unique biological characteristics, provides a robust means of identifying and authenticating individuals. This paper delves into the vast landscape of biometric applications, exploring their potential to enhance security and convenience across different sectors.

Keywords: Technology • Biometric system • Revolutionizing

Introduction

The paper delves into the different biometric modalities and their applications in enhancing security, including access control, identity verification, law enforcement, and financial transactions. It also explores how biometrics can improve convenience in areas like mobile devices, transportation, healthcare, and education. Advantages of biometric systems, such as enhanced security, improved user experience, and scalability, are discuss alongside challenges like privacy concerns, vulnerability to attacks, and legal issues. The research paper presents future trends in biometrics, such as multi-modal biometrics, artificial intelligence, wearable devices, and integration with the Internet of Things (IoT). Ethical considerations, including data protection, inclusivity, and transparency, are also examined to ensure responsible biometric implementation. The paper includes real-world case studies showcasing the use of facial recognition in airports, fingerprint authentication in mobile banking, and voice recognition in healthcare [1,2].

Literature Review

Additionally, multimodal biometrics, which combine multiple biometric modalities like fingerprints and iris scans, further enhance security and reduce the risk of false positives or negatives. With the ubiquity of smartphones and tablets, biometrics have become integral to mobile device security. Fingerprint sensors, facial recognition, and iris scanning technologies allow users to unlock their devices and authorize secure transactions conveniently and securely. Biometric authentication adds an extra layer of protection, reducing reliance on passcodes that can be forgotten or easily hacked. Moreover, biometric data remains encrypted and stored securely on the device, mitigating privacy concerns. The healthcare sector is increasingly adopting biometric applications to enhance patient identification, secure medical records, and improve healthcare delivery. Biometrics facilitates accurate patient identification, reducing medical errors and preventing fraud. Hospitals and clinics utilize biometric systems to link patients with their medical records securely, ensuring accurate diagnosis and treatment. Biometrics also enable healthcare professionals to access critical information quickly, enhancing efficiency and patient care. By capturing and comparing unique biometric traits, such as fingerprints or facial features, individuals can be reliably identified, preventing identity theft and fraud. Biometric verification processes are faster and more accurate than traditional methods, reducing the chances of errors or unauthorized access [3].

Challenges and biometrics developments

While biometric applications offer significant advantages, there are important considerations and challenges to address. Privacy concerns arise as biometric data is highly personal and sensitive. Safeguarding this data through robust encryption and secure storage systems is crucial. Additionally, ensuring the accuracy and reliability of biometric systems is vital, as false positives or false negatives can have serious consequences. Regular maintenance, updating algorithms, and addressing bias in the systems are ongoing challenges. Ethical considerations must also be addressed, including obtaining informed consent for biometric data collection and usage, as well as addressing potential biases in the technology. Striking the right balance between security, convenience, and privacy remains a key challenge in implementing biometric applications. Biometrics have significantly transformed the travel and immigration industry. Biometric passports, also known as e-passports, incorporate an individual's facial biometrics and fingerprints, making them more secure and tamper-resistant. These passports streamline border control processes by automating identity verification, reducing queues, and enhancing overall security. Immigration authorities also use biometric systems to verify the identity of travelers, ensuring accurate and reliable identification [4-6].

Discussion

These systems offer a higher level of security compared to traditional methods like PINs or signatures, reducing the risk of fraud and unauthorized access to accounts. Biometrics also simplify the authentication process, allowing users to complete transactions swiftly, whether in-person or online. As biometric technologies advance, we can expect to see wider adoption of biometric payment systems, fostering a more secure and seamless financial ecosystem. In the field of education, biometrics find applications in areas such as attendance management and exam integrity. Biometric attendance systems streamline the process of tracking student attendance, eliminating the need for manual record-keeping and reducing errors. These systems use biometric traits like fingerprints or facial features to uniquely identify students, ensuring accurate attendance records. Biometrics also contribute to maintaining exam integrity by verifying the identity of students during examinations, minimizing the risk of cheating or impersonation. By leveraging biometric applications, educational institutions can enhance efficiency, improve accountability, and uphold academic integrity.

Conclusion

The paper emphasizes the potential of biometric technology in shaping a safer and more convenient future while highlighting the need to strike a balance

Address for Correspondence: *Blemingo Biming, Department of Biostatistics, University of Dhaka, Dhaka, Bangladesh, E-mail: biming46@edu.in*

Received: 27 March, 2023, Manuscript No. Jbmbs-23-101646; **Editor assigned**: 29 March, 2023, Pre QC No. P-101646; **Reviewed:** 12 April, 2023, QC No. Q-101646; **Revised:** 17 April, 2023, Manuscript No. R-101646; **Published:** 25 April, 2023, DOI: 10.37421/2155-6180.2023.14.155

between security and privacy. These applications offer enhanced security, convenience, and accuracy, transforming the way we authenticate and interact with systems and services. However, addressing privacy concerns, ensuring accuracy, and maintaining ethical standards are crucial as biometric technologies continue to evolve. As we embrace these innovations, biometrics will play an increasingly central role in shaping a future where security, convenience, and personalization go hand in hand. Biometric authentication has gained traction in the financial industry, revolutionizing transactions and enhancing security. Biometric payment systems enable individuals to make secure and convenient payments using their unique physiological traits, such as fingerprints or facial features.

Acknowledgement

We thank the anonymous reviewers for their constructive criticisms of the manuscript. The support from ROMA (Research Optimization and recovery in the Manufacturing industry), of the Research Council of Norway is highly appreciated by the authors.

Conflict of Interest

The authors declare that there was no conflict of interest in the present study.

References

1. Ghubaish, Ali, Tara Salman, Maede Zolanvari and Devrim Unal, et al. "Recent advances in the Internet-of-Medical-Things (IoMT) systems security." *IEEE Internet Things J* (2020): 8707-8718.
2. Akhtar, Zahid, Abdenour Hadid, Mark S. Nixon and Massimo Tistarelli, et al. "Biometrics: In search of identity and security (Q & A)." *IEEE MultiMedia* 25 (2018): 22-35.
3. Razdan, Sahshanu and Sachin Sharma. "Internet of Medical Things (IoMT): Overview, emerging technologies, and case studies." *IETE Tech. Rev* 39 (2022): 775-788.
4. Hasan, Mohammad Kamrul, Shayla Islam, Imran Memon and Ahmad F. Ismail, et al. "A novel resource oriented DMA framework for internet of medical things devices in 5G network." *IEEE Trans Industr Inform* 18 (2022): 8895-8904.
5. Kumar, Prabhat, Govind P. Gupta and Rakesh Tripathi. "A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks." *J Ambient Intell Humaniz Comput* 12 (2021): 9555-9572.
6. Gao, Junqi, Jiazeng Wang, Linjie Zhang and Qiang Yu, et al. "Magnetic signature analysis for smart security system based on TMR magnetic sensor array." *IEEE Sens J* 19 (2019): 3149-3155.

How to cite this article: Biming, Blemingo. "Unlocking the Future: Exploring Biometric Applications for Enhanced Security and Convenience." *J Biom Biosta* 14 (2023): 155.