Mini Review
Volume 14:05, 2023

Journal of Biometrics & Biostatistics

ISSN: 2155-6180 Open Access

Ethical Considerations in Biostatistics and Data Privacy

Zelina Pose*

Department of Biostatistics, Science and Technology of New York, New York, USA

Abstract

Researchers and practitioners in biostatistics must adhere to strict guidelines and regulations to maintain data privacy. This involves implementing various measures, such as data anonymization, encryption, and access controls, to prevent unauthorized access to sensitive information. Additionally, obtaining informed consent from study participants and ensuring secure data storage and transmission are crucial components of maintaining data privacy in biostatistics research.

Keywords: MFA • Data anonymization • Fingerprint scanning

Introduction

In the ever-evolving landscape of the digital world, identity verification has become a critical aspect of maintaining trust and ensuring security. As online interactions have grown exponentially, so has the risk of fraud, data breaches, and identity theft. In response, businesses, governments, and individuals are turning to advanced identity verification methods to safeguard sensitive information and establish trust in virtual interactions. This article explores the importance of identity verification and how it plays a pivotal role in maintaining the integrity of our digital society. Identity verification is essential for regulatory compliance, especially in sectors such as finance, healthcare, and e-commerce, where stringent Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations are in place. It also helps protect individuals from impersonation, safeguard their personal information, and maintain the integrity of digital platforms and services [1].

Literature Review

The rapid digital transformation has led to a surge in online transactions. From e-commerce purchases to digital banking, people are increasingly relying on the internet to manage their daily affairs. However, with convenience comes vulnerability. Fraudsters and cybercriminals exploit these digital channels to gain unauthorized access to personal information, leading to financial losses and reputational damage. Identity verification is essential in this context, as it allows businesses and individuals to confirm the identity of the parties involved, creating a foundation of trust for digital interactions. Identity verification is the process of authenticating a person's identity through various means, such as documents, biometrics, or behavioural analysis. Traditional methods, like usernames and passwords, have proven inadequate in deterring sophisticated cyber-attacks. Therefore, newer and more robust methods have emerged, including facial recognition, fingerprint scanning, and Multi Factor Authentication (MFA). These technologies not only enhance security but also provide a seamless user experience, reducing friction in the verification process [2,3].

***Address for Correspondence:** Zelina Pose, Department of Biostatistics, Science and Technology of New York, New York, USA, E-mail: pose145@edu.in*

***Copyright:** © 2023 Pose Z. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*

Received: 27 September, 2023, Manuscript No. Jbmbs-23-115654; **Editor assigned:** 29 September, 2023, Pre QC No. P-115654; **Reviewed:** 12 October, 2023, QC No. Q-115654; **Revised:** 17 October, 2023, Manuscript No. R-115654; **Published:** 26 October, 2023, DOI: 10.37421/2155-6180.2023.14.189

Biometric and its behavioural analysis

As technology continues to advance, identity verification will likely undergo further improvements. Artificial Intelligence (AI) and Machine Learning (ML) will play a significant role in enhancing verification accuracy and detecting fraudulent activities in real-time. Additionally, decentralized identity systems, based on block chain technology, may revolutionize the way we manage and verify identities, providing individuals with more control over their data. While identity verification strengthens security, it also raises concerns about privacy. Striking the right balance between robust identity verification and protecting personal data is essential. Privacy-enhancing technologies, such as zero-knowledge proofs, allow parties to verify each other's identity without sharing sensitive information, mitigating potential privacy risks. In the financial sector, identity verification is critical for customer on boarding and Know Your Customer (KYC) compliance. By verifying identities, banks and financial institutions can prevent money laundering, terrorist financing, and other illicit activities. Additionally, MFA adds an extra layer of protection to financial transactions, safeguarding customer funds. In the world of online shopping, trust is paramount. Identity verification ensures that both buyers and sellers are legitimate, reducing the risk of fraudulent transactions.

Discussion

Furthermore, it allows businesses to provide personalized services and prevent unauthorized access to user accounts. The healthcare industry holds a wealth of sensitive patient data. Identity verification helps protect this information, ensuring that only authorized personnel can access patient records. It also aids in the fight against medical identity theft, a growing concern in the digital age. Governments worldwide are increasingly digitizing public services. From filing taxes to accessing social benefits, identity verification is essential for ensuring that citizens' information is secure and that services are provided to the right. It appears that you are conducting a comprehensive analysis of trust in the digital world. Trust is a critical aspect of any digital scenario where people, things, and infrastructure connect with each other. Establishing and maintaining trust is essential for the successful operation of various digital systems and services. Let's break down the different aspects of your analysis. The digital world is susceptible to biometric, data breaches, and other malicious activities. Building trust in the digital environment requires robust biometric measures to safeguard sensitive information and systems [4-6].

Conclusion

Identity verification is an essential component of trust and security in today's digital world. It helps prevent fraud, ensures regulatory compliance, and protects individuals' identities and personal information. By employing various methods, such as document verification, biometric authentication,

and knowledge-based verification, identity verification systems establish the authenticity of individuals. The on-going challenges of maintaining security, privacy, and staying ahead of fraudsters require continuous advancements in technology and collaboration between stakeholders. With the increasing reliance on digital interactions, identity verification will continue to play a crucial role in establishing trust and ensuring secure online transactions and interactions.

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 Author declares there is no conflict of interest associated with this manuscript.

References

1. Chakraborty, Soumyajit, Siddhartha Mukherjee, Bhaswati Sadhukhan and Kazi Tanvi Yasmin. "Biometric voting system using Aadhar Card in India." *Int J Innov* 4 (2016).
2. Messerschmidt, Martin and Matus Pleva. "Biometric systems utilizing neural networks in the authentication for e-learning platforms." *ICETA* (2019): 518-523
3. Rosenthal, Jeffrey N., David J. Oberly and Amanda M. Noonan. "From fingerprints to facial recognition: Scanning developments in biometric technology." *J Robot Artif Intell Law* 5 (2022): 123-128.
4. Rui, Zhang and Zheng Yan. "A survey on biometric authentication: Toward secure and privacy-preserving identification." *IEEE access* 7 (2018): 5994-6009.
5. Van Rooy, Dirk and Jacques Bus. "Trust and privacy in the future internet—A research perspective." *Identity Inf Soc* 3 (2010): 397-404.
6. Jones, E. M., N. A. Sheehan, N. Masca and S. E. Wallace, et al. "Datashield–shared individual-level analysis without sharing the data: A biostatistical perspective." *Nor Epidemiol* 21 (2012).

How to cite this article: Pose, Zelina. “Ethical Considerations in Biostatistics and Data Privacy.” *J Biom Biosta* 14 (2023): 189.