National Research Journal of Information Technology & Information Science
Volume No: 13, (January) Year: 2026 (Special Issue)
PP: 132-138
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

SECURE AUTHENTICATION SYSTEM USING BIOMETRIC

Azhar

Dept. of Computer Science Engineering, Chandigarh University Mohali, Punjab, India

Joti Sharma

Dept. of Computer Science Engineering, Chandigarh University Mohali, Punjab, India

Himani

Dept. of Computer Science Engineering Chandigarh University Mohali, Punjab, India

Shiv Sharan Dixit

Dept. of Computer Science Engineering Chandigarh University Mohali, Punjab, India

Shubham Kumar

Dept. of Computer Science Engineering, Chandigarh University Mohali, Punjab, India

Arpit Negi

Dept. of Computer Science Engineering Chandigarh University Mohali, Punjab, India

ABSTRACT

In today's world of digital transformation, a secure and reliable authentication system is necessary to prevent unauthorized access and breaches in both actual and virtual data. Traditional authentication mechanisms like password-based and PIN-based systems are vulnerable to various forms of security threats such as phishing, credential leaks, or brute-force attacks. Biometric authentication for a good alternative authenticated verification mode is found to either contain unique physiological or behavioral distinct user characteristics fingerprints, face or iris recognition, or biometrics. This research undertakes an investigation into the effectiveness, security, and challenges of biometric authentication. It studies the space mapping of integration multimodal biometrics, encryption, and machine learning algorithms to enhance security and minimize spoof identity risks. The study also addresses the advantage-disadvantage argument of security versus privacy versus user transparency and considers all the topics of concern related to data storage, biometric spoofing, and ethics in these terms.

Keywords—Biometrics, Authentication, security, Encryption, Credentials, machine learning, PINs.

I. INTRODUCTION

Authentication by biological means has become an important technology in present-day security systems, being a strong alternative for credentials such as passwords, PINs, or security tokens. With digital services forming an integral part of our everyday life, authentication has to be secure and trusted to avert unauthorized access or data breaches. There is an increasing number of conventional methods being attacked by cyber threats, credential theft, phishing attacks, or brute-force attacks. On the contrary, biometric authentication verifies the identity of people by using unique physiological and behavioral characteristics such as fingerprints, facial recognition, iris scans, and voice patterns. These traits are difficult to replicate, and this makes biometrics one of the more secure and efficient solutions in digital security.

The increasing reliance on biometric authentication is credited mainly to its ability to offer a seamless experience that is quite user-friendly along with a high degree of security. In contrast with passwords that can easily be forgotten, stolen, or shared, biometric characteristics naturally belong to one individual and remain through outtime.

This technology has been widely applied to mobile devices, banking systems, healthcare security this advancement comes with various challenges. Constant advances in encryption methods, secure storage, and anti- spoofing solutions must be made to resolve issues such as privacy, data security, and disadvantages to authentication reliability.

Indeed, one of the biggest worries within biometric identification is whether the biometric data themselves will be kept safe. Biometric data, unlike passwords, cannot be easily reset after a breach. Once compromised, biometric data cannot be changed, making biometrical identification all the more harmful when breached. Thus, the secure storage of biometric templates via encryption, homomorphic computing, and blockchain-based decentralized identity management becomes indispensable in reducing risks. Moreover, the introduction of AI and machine learning into biometric systems increases their precision, flexibility, and defenses against spoofing attacks. AI model analysis of small changes in biometric data is a form of making these systems more reliable and effective. The integration of multimodal biometric authentication methods,

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

which combine two or more biometric traits in a manner that improves security or reduces the acceptance or rejection rate, is gaining popularity A system that uses facial recognition in conjunction with voice authentication thus creates a stronger deterrent mechanism since it becomes difficult for an intruder to bypass. In addition, integration is being made possible by advancements in biometric authentication aimed at continuous authentication, which means validating user identity at multiple points in time rather than just single login time instances. This is of great help for authentication purposes during money transfer, corporate security, and high governmental applications.

With these advancements come ethical and regulatory hurdles that biometric authentication must overcome to thrive on a large scale. Like other kinds of data, biometric data have privacy concerns associated with them, especially on the grounds of consent, misuse of data, and surveillance. Governments and private organizations have to put appropriate data protection laws, such as the General Data Protection Regulation (GDPR) or Biometric Information Privacy Act (BIPA), in place to provide responsible use of biometric data. In addition to this, researchers are working on privacy-preserving biometric authentication techniques like biometric hashing and federated systems learning to increase security without revealing pure biometric data.

Future biometric auths seem to be very promising, especially in the innovations that make them more secure, user-friendly, and widely applicable. The biometric authentication systems will greatly advance security frameworks when integrated with various emerging technologies, such as blockchain, quantum cryptography, and decentralized identity solutions. Exploring the current terrain of biometrics authentication, changes brought by technology, security- related challenges, and future trends is what this research has set out to do. The study will identify and address the key concerns while proposing innovative solutions to developing more secure and efficient authentication systems that will negate the threat posed by evolving cyber threats while ensuring user privacy and convenience

The integration of biometric authentication with emerging technologies such as artificial intelligence, edge computing, and federated learning has opened new research directions. AI-driven biometric systems can adapt to changes in user appearance, aging, and environmental conditions, improving long-term reliability. Edge computing has enabled on-device biometric processing, reducing dependency on cloud- based authentication and enhancing user privacy. Federated learning has been explored as a method to train biometric authentication models across multiple devices while preserving user data privacy.

Fingerprint recognition was the primary biometric application. It still continues to count as among the most widely-used authentication technique. With this, fingerprint identification works on minutiae-based matching and ridge pattern analysis alone. But researchers identified shortcomings of this system, such as denial of service under spoofing using artificial fingerprints. Thus, the mechanisms of detection to resist this intrusion with other corresponding measures are liveness detection and sweat pore analysis. Some machines learning and deep learning developments also allow for fingerprint verification that provides enhancement due to their features extraction and classification through neural networks. Moreover, the entrenched capacitive and ultrasonic fingerprint sensors in most mobile devices favor fingerprint usage security.

II. LITERATURE REVIEW

The field of biometric authentication has seen extensive research and development, leading to various innovative solutions aimed at enhancing security, usability, and robustness. Several studies have focused on improving recognition accuracy, reducing vulnerability to spoofing, and ensuring privacy protection. This section highlights the major contributions in biometric authentication and discusses existing solutions deployed in real-world applications.

The early biometric authentication systems relied mainly on fingerprint recognition due to its superior accuracy and user-friendliness. Amongst other advancements, the minutiae-based extraction techniques were refined by researchers, and attempts were made to use deep learning techniques to enhance performance. Jain et al. (2020) reported the use of deep neural networks (DNNs) for fingerprint classification, resulting in a considerable reduction in both false rejection and false acceptance rates. Fingerprint authentication techniques, however, are still vulnerable to spoofing attacks, thus incorporating liveness detection mechanisms.

The same evolution is seen in face recognition, wherein several new generation deep learning methods such as FaceNet and DeepFace have improved their accuracy in strenuous conditions. Parkhi et al. (2015) and Schroff et al. (2017), for example, showed that convolutional neural networks (CNNs) have been exploited for extracting deep feature representations for reliable authentication. However, contrasting findings were also reported by Deb et al. in 2019, mentioning that high-resolution photographs and video footage could be used in adversarial and presentation attacks against face recognition systems.3D face recognition schemes with depth-sensing capabilities were developed as a measure against these attacks in the name of improving robustness.

All research regarding iris and retina recognition has observed various types of high reliability and security. Daugman's (2004) famous research on iris recognition using Gabor wavelet-based feature extraction is still used as a reference for

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

researchers in the field. Recent work has sought to enhance the capability of iris recognition in and under different environmental factors. Mahalingam and Ricanek (2013) proposed approaches toward abating occluded or low-quality images of irises to optimize recognition rates in real-world applications.

Several advantages have been derived because of their continuous authentication capabilities. Machine learning techniques would model typing patterns for authentication (Killourhy and Maxion, 2009). In similar studies, Nixon et al. (2010) explored video-based motion capture to identify a subject at a distance using the person's gait. Recently, advances have been made in voice authentication, with systems using deep learning- based spectrogram models to improve the recognition accuracy of speakers, such as the work of Lei et al. (2014). On the other hand, behavioral biometrics still suffer from changes in behavior from individual users and require adaptive learning methods.

Multimodal biometric recognition, thus, is the remedy to the limitations of each biometric modality. The combination of more than one biometric trait such as fingerprint and face, or iris and voice leads to enhancement in security and reduction of false rejection rates. Ross et al. (2006) have noted that score and decision-level fusion techniques could mitigate the negative effects of spoofing attacks on biometric authentication. Researches are still ongoing on fusing biometric data with or without other biometrics for better security provisions through blockchain.

security.

The aspect of ensuring the security and privacy of biometric data has called for research in this regard, as techniques for biometric template protection. Cancellable biometrics were introduced by Ratha et al. (2001), whereby biometric templates could be transformed to be revoked when compromised. Other recent methods involve the use of homomorphic encryption and secure multiparty computation for privacy-preserving authentication systems. Kerschbaum et al. (2019) looked into biometric hashing mechanisms that allow secure authentication without disclosing raw biometric data.

Biometric authentication systems have been put to use in real-world applications across different scopes of life. An excellent example that fits this description is the biometric Aadhaar system of India. Basically, it conveys more than a billion people with a secure, integrated fingerprint and iris recognition for identity. It is used widely in banking operations, such as Apple Face ID, Samsung's ultrasonic fingerprint sensor, and many other banks. Their focus is to improve convenience for the user.

Overall, while significant advancements have been made in biometric authentication, challenges such as spoofing resistance, privacy protection, and adaptive learning remain key areas for future research. The integration of AI-driven techniques, federated learning, and decentralized identity management systems is expected to drive the next generation of biometric authentication solutions.

III. METHODOLOGY

A. Acquire and preprocess the biometric data High resolution sensors have used biometric acquisition such as fingerprints, face images, voice samples, and iris scans. Histogram equalization, Gaussian filtering, and adaptive thresholding are some preprocessing techniques that improve the quality of the original images. Face alignment is attained by advanced models like MTCNN and RetinaFace, while fingerprint images become clearer thanks to Gabor filtering and ridge thinning.

B. Feature Extraction & Representation Unique biometric features are extracted through deep learning as well as traditional methods. Fingerprint recognition that uses minutiae extraction, SIFT keypoints, and wavelets will be combined with facial recognition techniques employing various models such as FaceNet, ArcFace, or ResNet. Iris recognition employs Gabor wavelet transformation and pattern matching based on Hamming distance.

C. Authentication Model Development Machine- learning models such as CNNs, SVMs, and Siamese Networks classify biometric features. Distance metric learning like Euclidean or cosine similarity indicates that an authentication attempt was successful. A multimodal approach to security unites many biometric modalities.

D. Security Enhancements & Anti-Spoofing Cryptographic hash functions (SHA-3, Argon2) secure biometric templates. Liveness detection mechanisms like blink detection, pulse analysis, and 3D depth sensing prevent spoofing attacks. Privacy is preserved through secure enclave processing and homomorphic encryption.

E. System Deployment & Integration System Deployment & Integration System integration is based on a client-server model, allowing for on-device processing as well as cloud processing. Edge computing offers advantages of latencies, blockchain-based identity management assures data integrity with existing authentication infrastructures.

F. Performance Evaluation & Optimization Performance evaluation is based on the false acceptance rate (FAR), false rejection rate (FRR), and equal error rate (EER).

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

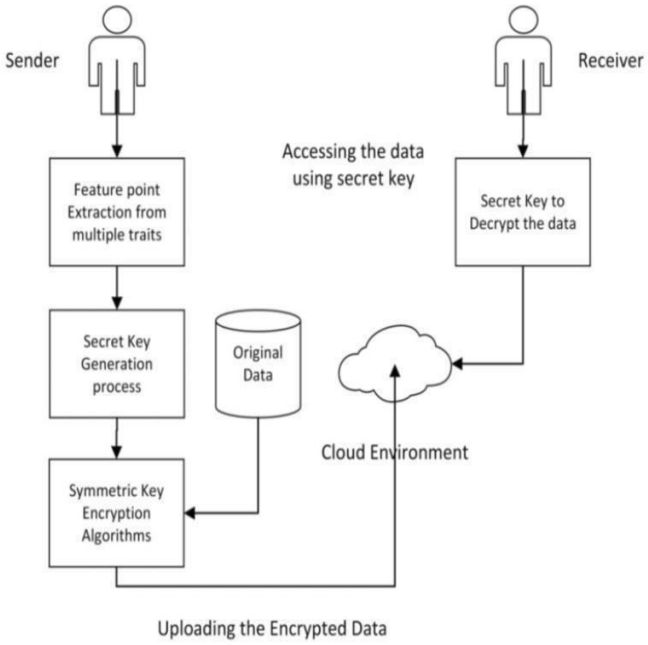

Fig.1 (Authentication system Framework)

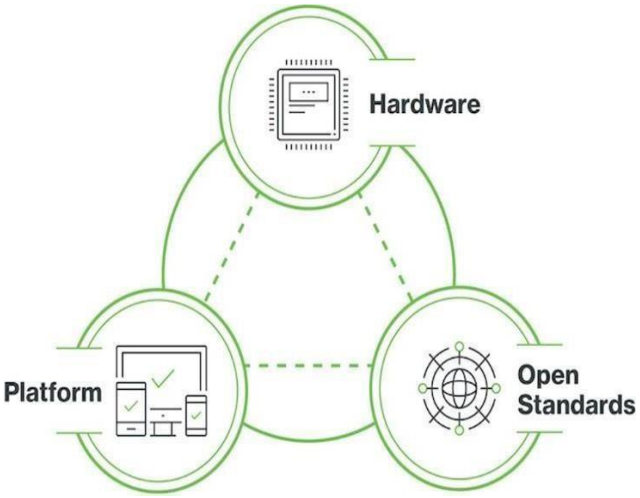

Fig.2 (Biometric Authentication Ecosystem)

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

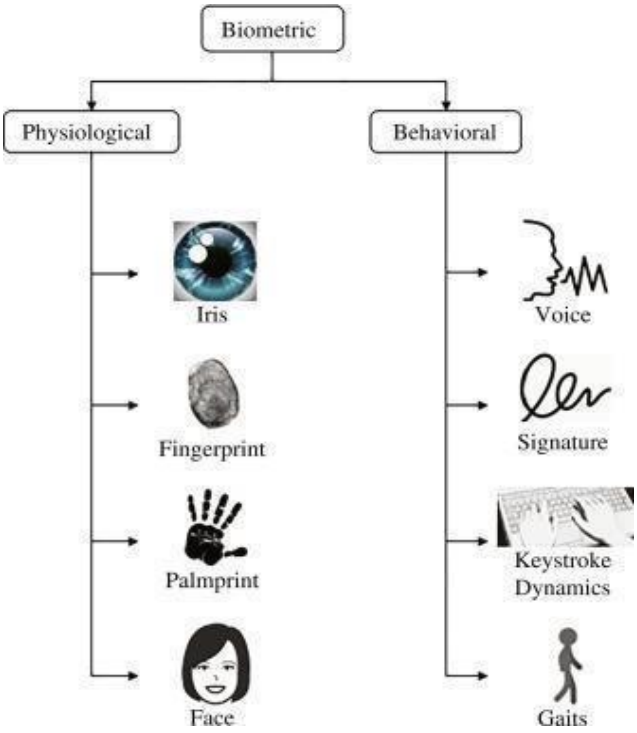

Fig.3 (Biometric Authentication Overview)

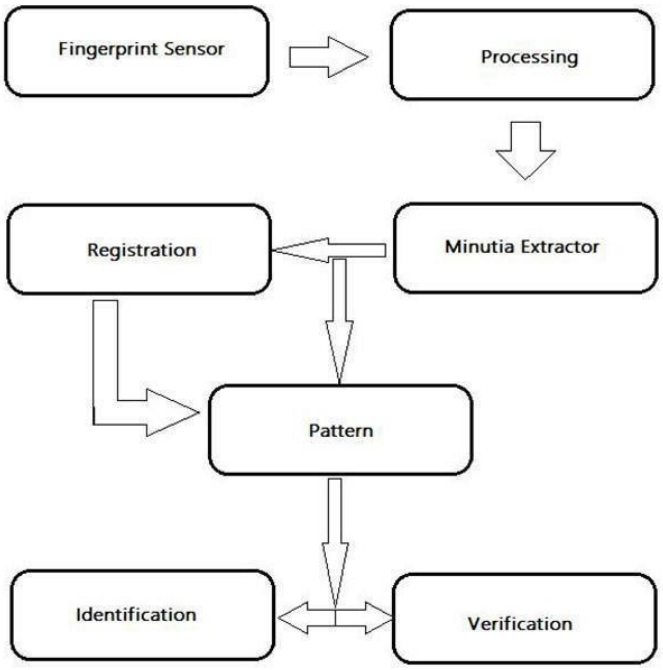

Fig. 4. (Biometric System Architecture)

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

IV. CONCLUSION AND FUTURE WORK

The biometric authentication system proposed here relied on advanced techniques of feature extraction, deep learning models, security measures against cryptography, and life detection to develop a countermeasure against spoofing and possible unauthorized access. This system covers multiple biometric modalities like fingerprints, facial recognition, and iris scanning to bring high reliability and reduced chances of false acceptance or rejection. Moreover, the techniques of cryptography will ensure the safety of biometric templates from issues related to privacy in biometric data protected storage, privacy in storage, and maya privacy in data transmission. Biometric authentication, however, is still challenged by adversarial attacks, errors in environment variation occurring in recognition systems, and ethical concerns regarding using biometric data. It is pertinent to present that fairness and lesser bias in biometric recognition systems are upholding, especially in diverse populations, and real-time processing efficiency requires optimization for end users' experiences and system scalability.

In the years to come, work in this area will focus on integrating more advanced deep learning architectures like transformer-based biometric recognition models for competitive performance in feature extraction and classification. The implementation of federated learning can ensure better privacy results for decentralized biometric authentication without any raw data ever being exposed. Nevertheless, the whole process of identity management can be further secured if combined with blockchain technologies, thus providing a decentralized, tamper-proof record for authentication that minimizes the risk of a data breach.

Adaptive biometric systems that will churn their user biometric templates all the more frequently over time in order to accommodate the natural variations due to ageing or environmental conditions are another area of promising research. Furthermore, the methods of fusion of multimodal authentication will be perfected to make the system stronger, including behavioral biometrics as keystroke dynamics and gait recognition, with traditional physiological biometrics.

Future implementations will also work toward the incorporation of biometric authentication into post- quantum cryptography in order to have a remedy for future. .

REFERENCES

1. Jain, A., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14(1),* 4-20.
2. Zhang, D., & Lu, G. (2003). Review of Shape Representation and Description Techniques. *Pattern Recognition, 37(1),* 1-19.
3. Daugman, J. (2004). How Iris Recognition Works. *IEEE Transactions on Circuits and Systems for Video Technology, 14(1),* 21-30.
4. Kumar, A., & Zhang, D. (2009). Personal Authentication Using Multibiometric Rank-Level Fusion. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 39(4),* 455-466.
5. Li, S. Z., & Jain, A. K. (Eds.). (2015).
6. *Handbook of Face Recognition.* Springer.
7. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21(2),* 120-126.
8. Uludag, U., Pankanti, S., Jain, A. K., & Prabhakar, S. (2004). Biometric Cryptosystems: Issues and Challenges. *Proceedings of the IEEE, 92(6),* 948-960.
9. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing Security and Privacy in Biometrics-Based Authentication Systems. *IBM Systems Journal, 40(3),* 614-634.
10. Nandakumar, K., Jain, A. K., & Pankanti, S. (2007).Fingerprint-Based Fuzzy Vault: Implementation and Performance. *IEEE Transactions on Information Forensics and Security, 2(4),* 744-757.
11. Bui, T., & Hatzinakos, D. (2008). Biometric Authentication with Multimodal Fusion Using Wavelet-Based Image Processing. *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 37(5),* 1347-
12. 1355.
13. J. J. G. Preibush, "Identity and Access Management: Business Performance through Connected Intelligence," Wiley, 2021.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

14. Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2008). A Survey of Iris Recognition Accuracy. *ACM Computing Surveys (CSUR), 41(3),* 1-42.

15. Scheirer, W. J., Rocha, A., Sapkota, A., & Boult, T. E. (2013). Toward Open-Set Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 35(7),* 1757-1772.

16. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep Residual Learning for Image Recognition. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* 770-778.

17. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio,

18. Y. (2014). Generative Adversarial Nets. *Advances in Neural Information Processing Systems (NeurIPS),* 2672-2680.

19. Abate, A. F., Nappi, M., Riccio, D., & Sabatino, G. (2007). 2D and 3D Face Recognition: A Survey. *Pattern Recognition Letters, 28(14),* 1885-1906.

20. Viola, P., & Jones, M. (2001). Rapid Object Detection Using a Boosted Cascade of Simple Features. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* 511-518.

21. Li, Y., Xue, Y., & Li, X. (2020). *A survey*

22. *on secure user authentication schemes for mobile cloud computing.* Future Generation Computer Systems, 101, 251-264.

23. Bojinov, H., Bursztein, E., Boyen, X., & Boneh, D. (2012). *Kamouflage: Loss-resistant password management.* European Symposium on Research in Computer Security, 286-302.

24. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," *IEEE Symposium on Security and Privacy*, 2012.

25. DeepFace. (2014). A System for Face Recognition Using Deep Learning. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* 1701-1708.

26. Bonneau, J. and C. Herley. and Van Oorschot, P. C., and Stajano, F. (2012). The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. IEEE Symposium on Security and Privacy (SP), 2012, 553-567.

27. Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The Tangled Web of Password Reuse. Network and Distributed System Security Symposium (NDSS), 2014, 1-15.

28. Kumar, A., & Zhang, D. (2009). Personal Authentication Using Multibiometric Rank-Level Fusion. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 39(4), 455-466.

29. Abuhamad, M., & Abu-Dalo, A., & Abusnaina, A., & Mohaisen, D. (2020). Sensor- Based Continuous Authentication for Extended Reality Head-Mounted Displays. Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2020, 1825-1839.