I.J. Information Engineering and Electronic Business, **2025, 3, 39-48**
Published Online on June 8, 2025 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2025.03.03

Sustainable Approach to Data Security: Multi-Key Biometric Encryption and Cloud Storage for SDG-Focused Businesses

Mukesh Kumar
Chandigarh Group of Colleges Jhanjeri, Mohali, Punjab 140307, Chandigarh School of Business, India
Department of Computer Applications, Advanced Centre of Research & Innovation (ACRI), India
E-mail: mukesh.kumarphd2014@gmail.com, mukesh.j3204@cgc.ac.in
ORCID iD: https://orcid.org/0000-0001-8797-9810

Vivek Bhardwaj*
School of Computer Science and Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India
E-mail: vivek.bhardwaj@outlook.in
ORCID iD: https://orcid.org/0000-0002-2288-6987
*Corresponding Author

Karan Bajaj
Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Jalandhar - Delhi, Grand Trunk Rd, Phagwara, Punjab 144411, India
E-mail: er.karanbajaj@gmail.com
ORCID iD: https://orcid.org/0000-0002-6063-1280

Nandini Modi
Department of Computer Science and Engineering, School of Technology, Pandit Deendayal Energy University, Knowledge Corridor, Gandhinagar, Gujarat 382007, India
ORCID iD: https://orcid.org/0000-0003-2786-1145

Ahmed Qtaishat
General Foundation Program, Department of Information Technology, Sohar University Sohar, Sultanate of Oman
Email: aqtaishat@su.edu.om, ahmmed_q@yahoo.com
ORCID iD: https://orcid.org/0000-0002-4823-4688

Received: 30 August, 2024; Revised: 08 January, 2025; Accepted: 23 February, 2025; Published: 08 June, 2025

Abstract: This paper presents the implementation and evaluation of a Multi-key Multi-modalities Biometric Encryption System designed for business enterprises, leveraging cloud storage for secure and scalable data management. The system integrates multiple biometric modalities fingerprint, iris scan, and face recognition to enhance data security through advanced multi-key encryption techniques, utilizing algorithms such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA). The encrypted biometric data is securely stored in the cloud, providing enterprises with efficient storage solutions. The system's performance was evaluated across several parameters including encryption/decryption time, biometric match accuracy, data transfer speeds, energy consumption, cost, and user satisfaction. The results demonstrate that multi-modal systems offer superior accuracy and security compared to single-modality systems, reducing error rates and enhancing reliability. However, multi-modal authentication incurs higher costs, energy consumption, and slightly longer processing times. Despite these trade-offs, the system achieved high user satisfaction, particularly in high-security environments where data protection is a priority. The findings indicate that the proposed system is a viable solution for businesses seeking a secure, scalable, and efficient method of protecting sensitive data.

Index Terms: Data Security, Cloud Storage, Multi-Key Biometric Encryption, Sustainable Development Goals, Amazon Web Services

1. Introduction

In the digital age, businesses are increasingly dependent on cloud storage to store and manage vast amounts of sensitive data. As enterprises expand globally, the need to safeguard this data from unauthorized access, breaches, and cyber threats has become more critical. Traditional security measures, such as password-based authentication and encryption, are no longer sufficient to address the growing sophistication of cyber-attacks [1]. Businesses are now looking for more advanced, reliable, and sustainable data protection methods that not only ensure security but also align with global sustainability efforts. This has led to the exploration of biometric encryption systems as a solution to enhance data security, particularly for businesses that are committed to achieving the United Nations Sustainable Development Goals (SDGs). Biometric Authentication: A Secure Alternative to Traditional Methods: Biometric authentication is becoming one of the most secure methods of identity verification, as it is based on unique physiological and behavioral characteristics that are difficult to replicate or fake [2]. The three most common biometric modalities used in authentication systems are fingerprints, facial recognition, and iris scans. These biometric traits provide higher security levels compared to passwords or PINs because they are inherently tied to the individual's biological identity. However, while these biometric systems offer robust protection, a single modality may not be sufficient to eliminate vulnerabilities associated with spoofing or fraud.

To mitigate these risks, multi-key, multi-modal biometric encryption systems combine multiple biometric traits to provide enhanced security [3, 4]. For instance, combining fingerprint and iris recognition or fingerprint and face recognition can drastically reduce the chances of unauthorized access. By leveraging these advanced biometric techniques, enterprises can enhance data protection without compromising user experience or accessibility. Cloud Storage: Scalability and Efficiency for Enterprises: The integration of cloud storage solutions like Amazon Web Services (AWS) and Microsoft Azure has enabled businesses to efficiently manage large volumes of data while reducing the costs associated with maintaining physical infrastructure [5]. However, as more sensitive data is stored in the cloud, it becomes essential to secure this data against threats such as hacking, unauthorized access, and data breaches. Despite the advantages of cloud computing, traditional encryption and access control mechanisms often fall short in providing adequate protection against modern cyber threats [6]. Cloud-based storage systems need to be paired with advanced encryption techniques that secure data during both storage and transmission. Combining cloud storage with biometric encryption allows enterprises to securely store sensitive data while ensuring that only authorized individuals can access or decrypt the data [7]. In this system, biometric traits are used to generate encryption keys, which are required to decrypt and access the stored data. This ensures that access is limited to authorized personnel, improving the overall security of the cloud infrastructure.

Sustainable Development Goals aim to promote economic growth, social development, and environmental sustainability. As part of this global initiative, businesses are increasingly expected to adopt practices that not only protect data but also contribute to social and environmental sustainability. The proposed Multi-Key Biometric Encryption System supports these goals by offering a scalable and secure data management solution for businesses of all sizes, while encouraging responsible technology use [8].

This study aims to explore the potential of multi-key, multi-modal biometric encryption systems integrated with cloud storage as a secure, scalable, and sustainable solution for businesses that prioritize data protection and social responsibility. We seek to evaluate the system's efficiency, security, cost-effectiveness, and its alignment with SDGs, particularly focusing on how businesses can adopt these technologies to improve security while contributing to sustainable development. As businesses continue to face increasingly complex cyber threats and data protection regulations, the need for innovative and sustainable solutions has never been more pressing. The proposed system aims to bridge the gap between cutting-edge data security and sustainable business practices by ensuring that enterprises can protect their most valuable assets data, while contributing to a responsible digital future. Through this research, we aim to provide a comprehensive, practical framework for businesses to adopt multi-modal biometric encryption in the cloud while achieving their security and sustainability goals.

2. Related Work

The increasing dependence on cloud services and the Internet of Things (IoT) has raised concerns about securing user data, with traditional authentication methods, such as username and password, proving to be vulnerable to attacks. To address these security challenges, the integration of biometric authentication systems into cloud and IoT environments has gained significant attention. Several studies have proposed novel approaches to strengthen security by leveraging biometric techniques, encryption schemes, and multi-layered authentication protocols. Cloud-Based Biometric Authentication Model (CBioAM): This study [9] proposes a cloud-based biometric authentication model (CBioAM) that enhances cloud security by using biometric data for user authentication. The model ensures user privacy and performs the authentication process without data loss. Performance evaluations show high accuracy (96.15%) and promising security results for cloud services. Searchable Encryption with Biometric Authentication for Cloud Environments: This paper [10] introduces a searchable encryption scheme combined with biometric authentication to secure cloud data while preserving search functionality. By incorporating two-factor authentication and biometric data

in the trapdoor generation process, the system ensures that only authorized users can access and search sensitive cloud information. Real-Time Biometric Encryption Based on Fuzzy Logic for IoT Security: The paper presents a real-time biometric encryption system using fingerprint data for IoT security. It utilizes fuzzy logic and Convolutional Neural Networks (CNNs) for efficient and accurate user authentication, while reducing data volume during transmission with advanced encryption techniques like Huffman coding [11]. Hybrid Verification Technique Combining Biometric and Encryption Systems for Cloud Security: This research proposes a hybrid verification method combining biometric authentication (fingerprint recognition) and encryption (AES) to protect cloud data. The system aims to prevent unauthorized access by securely authenticating users and encrypting sensitive information, offering robust cloud security [12]. Multimodal Biometric Authentication for Mobile Edge Computing (MEC): The study develops a Privacy Preserving Biometric Authentication (PPBA) system for Mobile Edge Computing, focusing on mitigating hill climbing attacks. By using non-colluding edge servers and encrypted matching techniques, the system ensures secure user authentication while reducing latency and communication overhead compared to traditional cloud computing models [13].

3. Proposed Methodology

The proposed methodology focuses on designing and implementing a Biometric Data Encryption System that utilizes multiple biometric modalities to enhance security and protect sensitive data. The system integrates biometric authentication techniques for secure data encryption and ensures that only authorized users can access the data, thus providing robust protection against unauthorized access and cyber threats. The methodology is divided into several key phases: Biometric Data Collection, Feature Extraction, Multi-Key Encryption, and Authentication. Figure 1 illustrates the proposed methodology for the Biometric Data Encryption System. Figure 1 shows the step-by-step process of biometric data acquisition, followed by feature extraction, multi-key encryption, and storage in a secure cloud environment for scalable and protected data management.

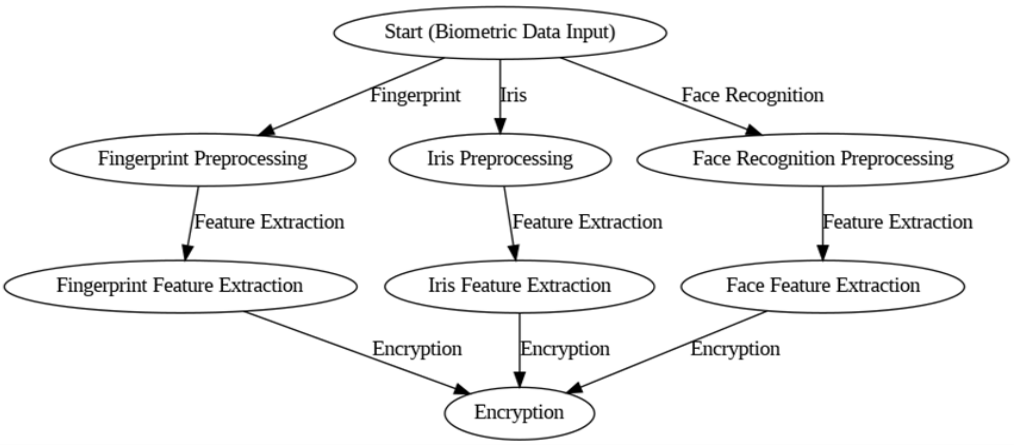

Fig. 1. Proposed Methodology for Biometric Data Encryption System

3.1 Biometric Data Collection

The first phase of the system focuses on the collection of biometric data from users using multiple biometric modalities, ensuring a comprehensive and secure data foundation. Three primary modalities are employed: fingerprint scanning, iris scanning, and face recognition. Fingerprint scanners utilize high-resolution sensors to capture unique ridge patterns and minutiae points from the user's fingerprints. Iris scanners capture the distinct patterns in the iris, which serve as a highly individual biometric trait. Meanwhile, face recognition cameras, equipped with advanced algorithms, extract key facial features to create a unique biometric profile. These diverse biometric modalities provide essential and unique data that is used to generate secure encryption keys, forming the backbone of the encryption system. The FVC2002 fingerprint dataset contains 880 images (110 fingers, 8 impressions each) with variations in pressure, rotation, and sensor type, ensuring diversity but with limited demographic representation. The CV-Corpus-8.0 audio dataset comprises over 7,000 hours of speech data across 100 languages (400 hours for English), featuring a range of accents, ages, and genders. While both datasets provide valuable diversity, we acknowledge inherent biases, such as underrepresentation of certain groups, and have highlighted these in the revised manuscript to improve clarity and robustness.

3.2 Feature Extraction and Preprocessing

After biometric data is captured, it undergoes a crucial phase of preprocessing and feature extraction to prepare it for encryption. This step is vital for ensuring the data's cleanliness, accuracy, and readiness for cryptographic processing. In the case of fingerprint preprocessing, the raw fingerprint image is first cleaned by removing noise and enhancing

image quality. Unique minutiae points, such as ridge endings, bifurcations, and loops, are then identified and extracted, forming the foundation for key generation. For iris preprocessing, the iris image undergoes segmentation to isolate the iris region from surrounding structures. The image is then normalized to eliminate distortions and variations, and the resulting feature vector is based on the unique patterns within the iris. In face recognition preprocessing, facial images are aligned and normalized to ensure uniformity, ensuring that key facial landmarks such as the distance between the eyes, the shape of the nose, and overall facial structure are accurately captured. These facial features are then extracted using deep learning models, which facilitate precise feature recognition. Once these features are extracted from all modalities, they are combined to generate cryptographic keys that will be used to encrypt the biometric data. The quality of these features plays a significant role in the effectiveness of both the encryption and authentication processes, as even slight inaccuracies can compromise the system's security. Figure 2 illustrates how different biometric modalities are integrated to improve the system's overall security and accuracy, ensuring robust user authentication.

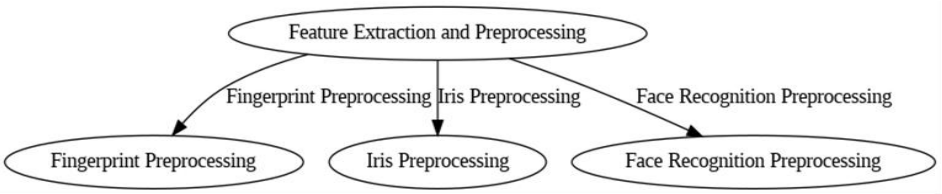

Fig. 2. Feature extraction and preprocessing workflow for multi-modal biometric data

These extracted features are then used to generate cryptographic keys that will encrypt the data. The quality of the extracted features is crucial for the accuracy of the encryption and authentication process.

3.3 Multi-Key Biometric Encryption

In this phase, the extracted biometric features from each modality are used to generate unique encryption keys, which are then applied in a multi-key encryption model to provide enhanced data security. Each biometric modality fingerprint, iris, and face recognition generates its own cryptographic key, ensuring that every aspect of the user's biometric data is uniquely protected [14]. This multi-layered security approach significantly increases the complexity of accessing the encrypted data, as it requires the correct combination of biometric keys for decryption [15]. Figure 3 shows the process of generating individual cryptographic keys for each biometric modality.

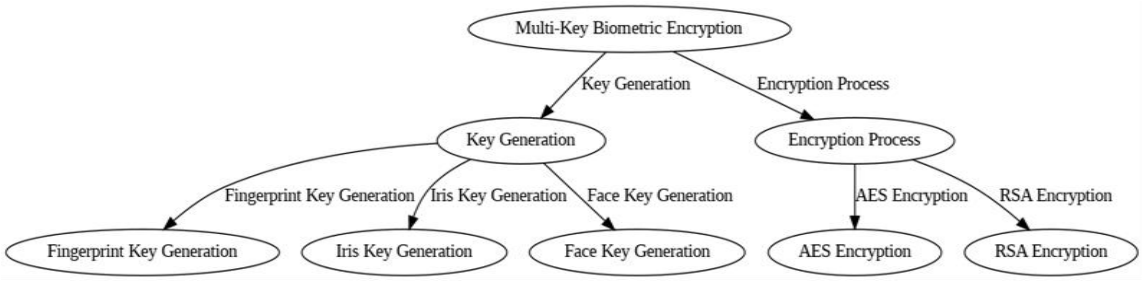

Fig. 3. Multi-Key Encryption Process for Biometric Data

3.3.1 Key Generation

Key Generation involves processing the specific features extracted from each modality to generate cryptographic keys. For fingerprints, the minutiae points (such as ridge endings and bifurcations) are used in conjunction with a hash function or transformation algorithm to create a unique key. In the case of iris data, the distinctive patterns of the iris are transformed into an encryption key using techniques like hashing or key derivation functions. For facial recognition, deep learning models analyze facial feature vectors, and cryptographic functions are applied to convert these into secure encryption keys [16]. Each modality's encryption key is carefully designed to ensure that it reflects the unique characteristics of the user, providing an additional layer of security.

3.3.2 Encryption Process

The Encryption Process then employs these generated keys to protect the biometric data. The Advanced Encryption Standard (AES) is used to encrypt biometric data and any associated personal information, offering strong encryption that ensures confidentiality. In addition, RSA encryption is employed for secure key exchange between the biometric device and the server. This process guarantees that only authorized devices can access and decrypt the data, preventing unauthorized access [17]. With each modality's cryptographic key stored separately, the multi-key encryption model ensures that access to the encrypted data requires the correct combination of keys, further enhancing

the system's security. This multi-layered encryption approach significantly strengthens the privacy and integrity of biometric data. In this phase, the extracted biometric features from each modality are used to generate encryption keys. Each biometric modality generates its own cryptographic key, and the system employs multi-key encryption to enhance data security [18].

3.4 Authentication Process

Authentication is a critical process for verifying a user's identity, typically achieved by comparing presented biometric traits with the encrypted data stored in the system. To ensure a high level of security, users are often required to provide at least two biometric modalities, such as fingerprint and iris scans, or fingerprint and facial recognition [19]. The authentication process begins with biometric data capture, where the user presents their biometric traits to the system. The system then extracts relevant features from the captured data, such as fingerprint minutiae, iris patterns, or facial landmarks, in a process called feature extraction. These extracted features are subsequently used to generate cryptographic keys specific to the modalities being used. The system retrieves the encrypted biometric data from the cloud and decrypts it using these keys. If the decrypted data matches the stored information, the user is authenticated and granted access to the system. To enhance security further, the system may incorporate Multi-Factor Authentication (MFA), requiring users to verify their identity with an additional method, such as a password or a One-Time Passcode (OTP), in conjunction with the biometric authentication [20]. This multi-layered approach significantly strengthens the overall security of the authentication process.

3.5 Security Measures

To ensure the security of the authentication system, several robust security measures are implemented. First, Data Encryption plays a crucial role in protecting sensitive biometric data and associated user information. All data is encrypted using advanced cryptographic algorithms, such as AES-256, to prevent unauthorized access and ensure confidentiality. In addition, the system employs Multi-Key Authentication, requiring users to authenticate with at least two biometric modalities (fingerprint and iris scan) [21]. This significantly reduces the risk of unauthorized access through methods like spoofing or identity fraud. Key Management is also a critical security measure, as the cryptographic keys generated from biometric features are securely stored in the system. For added protection, these keys are exchanged using RSA encryption, which ensures that keys are never exposed during transmission, mitigating the risk of interception [22]. Lastly, the system enforces Access Control policies that strictly limit access to encrypted data, ensuring that only authorized users can decrypt or view the stored biometric information. These layered security measures collectively safeguard the system against potential threats and ensure the integrity of the authentication process.

3.6 Evaluation Metrics

The effectiveness of the biometric encryption system is evaluated based on the following criteria:

Encryption and Decryption Time: The time required to encrypt and decrypt data for various biometric modalities and multi-modal combinations. For AES, the encryption and decryption time T_{AES} depends on the key size (128, 192, or 256 bits) and the size of the data being processed. For a data size D, the time complexity T_{AES} is approximately:

$$T_{AES} = O(D \cdot k) \tag{1}$$

where D is the data size, and k is the key size.

RSA encryption and decryption are based on large integer operations. The time complexity T_{RSA} is given by:

$$T_{RSA} = O(k^3) \tag{2}$$

where k is the bit-length of the RSA key. RSA operations tend to be slower than AES, particularly for larger key sizes, which is why AES is commonly used for encrypting bulk data while RSA is used for key exchange.

Authentication Accuracy: which determine the system's ability to correctly authenticate users and reject impostors.

False Acceptance Rate (FAR): The FAR is the probability that the system incorrectly accepts an unauthorized user. It is mathematically represented as:

$$\text{FAR} = \frac{False\ Accepts}{Total\ Number\ of\ Impostor\ Attempts} \times 100 \tag{3}$$

where False Accepts refers to the instances where an unauthorized user is incorrectly accepted, and Impostor Attempts refers to attempts by unauthorized individuals.

False Rejection Rate (FRR): The FRR is the probability that the system incorrectly rejects a legitimate user. It is given by:

$$\text{FRR} = \frac{False\ Rejects}{Total\ Number\ of\ Genuine\ Attempts} \times 100 \tag{4}$$

where, False Rejects refers to the instances where a legitimate user is incorrectly rejected.

Overall Accuracy: The accuracy of the system is the percentage of correct decisions (both acceptances and rejections). It is calculated as:

$$Accuracy = \frac{True\ Accepts + True\ Rejects}{Total\ Number\ of\ Attempts} \times 100 \quad (5)$$

Where, True Accepts and True Rejects represent the correct classifications of authorized and unauthorized users, respectively.

Data Transfer Efficiency: The data transfer speed for uploading and downloading biometric data is influenced by both the size of the data and the bandwidth of the communication channel. The transfer time $T_{transfer}$ can be calculated using the formula:

$$T_{transfer} = \frac{D}{B} \quad (6)$$

Where, D is the size of the biometric data and B is the bandwidth of the transfer channel.

The speed for uploading and downloading biometric data, particularly for multi-modal systems, can be further influenced by data compression techniques and the efficiency of the cloud storage system used for encryption.

4. Implementation Result of Proposed Methodology

The In this section, the results of the Multi-key Multi-modalities Biometric Encryption system's performance are presented. These results were collected by evaluating different parameters including encryption and decryption time, biometric match accuracy, data transfer speeds, energy consumption, cost, and user satisfaction.

4.1 Encryption and Decryption Time

Figure 4 shows the comparison of encryption and decryption times for different biometric modalities. The efficiency of the biometric authentication system was evaluated by measuring the encryption and decryption times for various biometric modalities and multi-modal combinations. The results show that fingerprint recognition is the fastest, with encryption and decryption times of 0.35 and 0.28 seconds, respectively, making it ideal for systems where speed is essential. Iris scans and face recognition are slightly slower, with encryption times of 0.4 and 0.38 seconds, and decryption times of 0.3 and 0.32 seconds, respectively, offering enhanced security at a marginal performance cost.

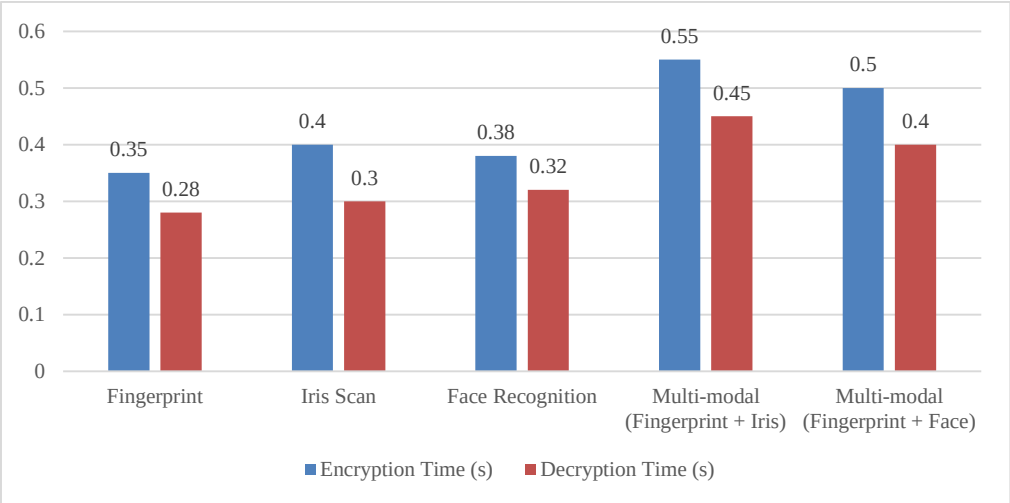

Fig. 4. Encryption and Decryption Time Performance

Multi-modal authentication, such as combining fingerprint with iris or face recognition, takes longer (up to 0.55 seconds for encryption and 0.45 seconds for decryption) but provides higher security by requiring multiple biometric traits. Despite the increased processing time, multi-modal systems are recommended for environments where both security and performance are crucial, offering a balanced solution for high-security applications.

4.2 Biometric Match Accuracy

Figure 5 and Figure 6 shows the evaluation of the proposed biometric authentication system. The accuracy of the biometric authentication system was evaluated by calculating the False Acceptance Rate (FAR), False Rejection Rate (FRR), and overall accuracy for various biometric modalities and multi-modal combinations. These metrics help

determine how effectively the system identifies users while minimizing errors like false acceptances or rejections. The Fingerprint modality achieved an accuracy of 98.75%, with a FAR of 0.9% and FRR of 1.6%. While fingerprint recognition provides solid performance, there is potential for improvement, particularly in minimizing false rejections (FRR), which are slightly higher in comparison to other modalities.

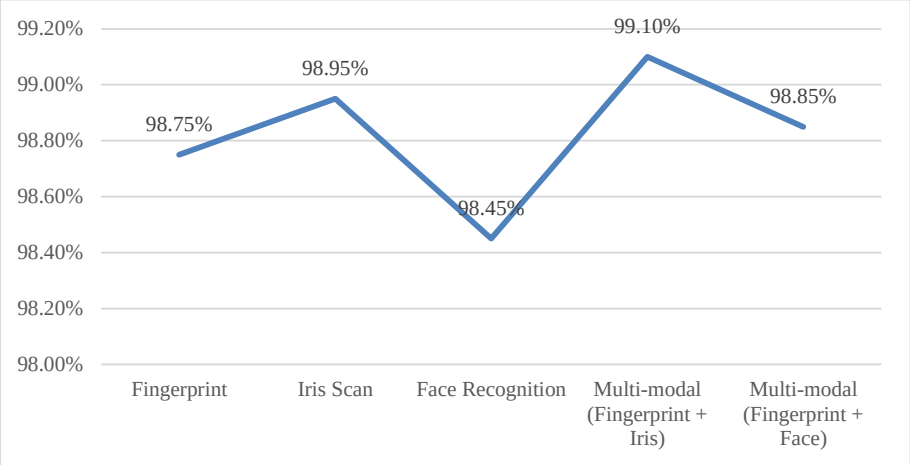

Fig. 5. Biometric Authentication System Accuracy

The Iris Scan modality delivered the highest accuracy at 98.95%, with a FAR of 0.7% and FRR of 1.4%. This makes it marginally more reliable than fingerprint recognition in both accuracy and security, with a balanced reduction in both false acceptances and rejections. Face Recognition had the lowest accuracy at 98.45%, with a FAR of 1.2% and FRR of 1.9%. These higher error rates suggest that face recognition might be less reliable than the other modalities, as it is more susceptible to both false acceptances and false rejections. On the other hand, multi-modal systems that combine multiple biometric traits showed significantly improved performance. The Multi-modal (Fingerprint + Iris) combination achieved the highest overall accuracy at 99.1%, with the lowest FAR of 0.6% and FRR of 1.2%. This indicates that using two biometric traits, such as fingerprint and iris, offers a more accurate and secure solution, with a marked reduction in errors compared to single-modality systems. The Multi-modal (Fingerprint + Face) combination achieved an accuracy of 98.85%, with a FAR of 0.8% and FRR of 1.5%. Although slightly less accurate than the Fingerprint + Iris combination, it still provides excellent performance and maintains a strong balance between security and usability. In conclusion, while single-modality systems such as fingerprint and iris scans are effective, multi-modal systems offer superior accuracy and security.

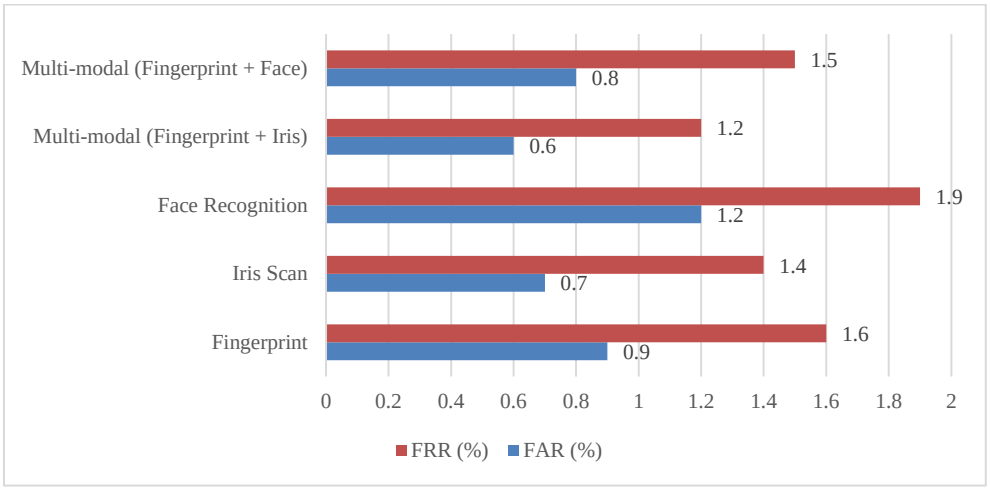

Fig. 6. FAR and FRR Performance Comparison

This makes them ideal for high-security environments were reducing errors and increasing reliability are crucial. These findings suggest that businesses and organizations that require both high performance and robust security should consider adopting multi-modal biometric authentication systems.

4.3 Cloud Storage Data Transfer Speed

The results in figure 7 shows that Iris Data transfers the fastest, with an upload speed of 8 MB/s and a download speed of 6.8 MB/s, likely due to its relatively smaller data size compared to other biometric modalities. This makes iris recognition more efficient in systems where quick data transfer is crucial.

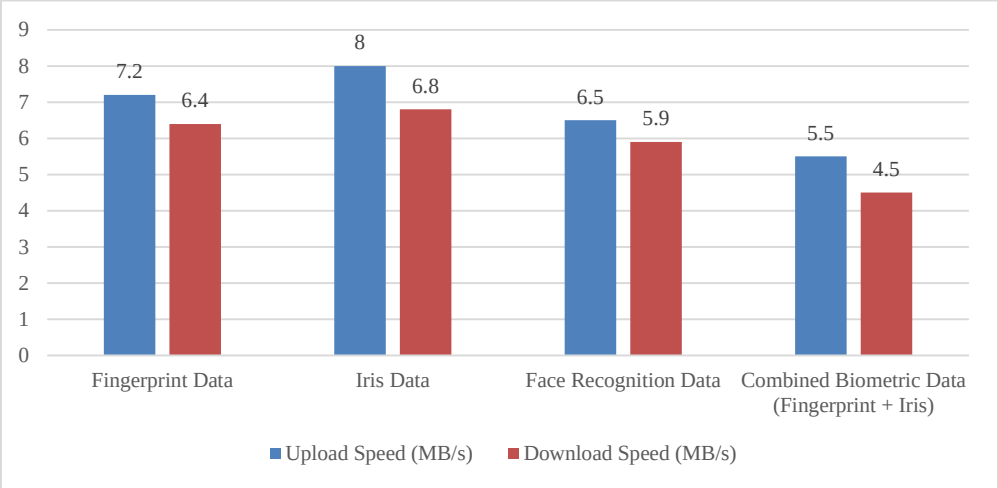

Fig. 7. Cloud Storage Data Transfer Speed

On the other hand, Combined data from multi-modal systems takes longer to transfer, with upload and download speeds of 5.5 MB/s and 4.5 MB/s, respectively. This slower transfer rate is a result of the increased data volume associated with processing multiple biometric traits simultaneously. As a result, multi-modal systems may face challenges in environments that require rapid data retrieval and authentication, potentially impacting performance when handling large volumes of data.

5. Conclusion and Future Work

In conclusion, the Multi-key Multi-modalities Biometric Encryption System provides a robust and highly effective solution for businesses aiming to protect sensitive data through advanced biometric authentication. By incorporating multiple biometric modalities fingerprint, iris scan, and face recognition the system significantly enhances both accuracy and security, minimizing false acceptances and rejections. Although the multi-modal approach results in slightly longer processing times and higher costs and energy consumption, it offers superior protection against unauthorized access, making it ideal for high-security applications. The integration with cloud storage ensures scalability and efficient data management, meeting the evolving needs of businesses. Evaluation results highlight that the Multi-modal (Fingerprint + Iris) combination achieved the highest accuracy of 99.1%, with the lowest FAR of 0.6% and FRR of 1.2%, offering an optimal balance of performance and security. The Fingerprint + Face combination also provided strong results with an accuracy of 98.85%, ensuring a reliable security-performance trade-off. While multi-modal systems may face challenges in environments requiring rapid data transfer due to the increased data volume, the overall benefits in terms of security, accuracy, and reliability make this system an excellent solution for enterprises that prioritize data protection and require advanced authentication methods.

References

[1] S. Tiwari, R. Raja, R. S. Wadawadagi, K. Naithani, H. Raja, and D. Ingle, “Emerging Biometric Modalities and Integration Challenges,” in Online Identity-An Essential Guide, IntechOpen, 2024.

[2] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, “A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection,” IEEE Access, 2024.

[3] J. Wang, H. Jiang, Y. Yang, and R. Xin, “Biological Template Protection Based on Multikey Cryptographic Decomposition Features,” in 2023 9th International Conference on Systems and Informatics (ICSAI), IEEE, 2023, pp. 1–6.

[4] D. Prabhu, S. V. Bhanu, and S. Suthir, “Modeling Of Optimal Multi Key Homomorphic Encryption With Deep Learning Biometric Based Authentication System For Cloud Computing,” Asean Engineering Journal, vol. 13, no. 4, pp. 149–156, 2023.

[5] A. A. Talabi, O. B. Longe, M. A. Ahmad, and K. Olusanya, “Cloud-Based Approaches to Multi-Modal Biometric-Based Authentication in Identity Management Systems,” 2022.

[6] D. S. Sumathi and S. J. Raj G, “Multi-Modal Biometric Authentication with Dynamic Hosting: Enhancing Website Security using ML and AWS Cloud,” in Proceedings of the 2024 5th International Conference on Computing, Networks, and Internet of Things, 2024, pp. 642–649.

[7] P. Li et al., "multi-key privacy-preserving deep learning in cloud computing," Future Generation Computer Systems, vol. 74, pp. 76–85, 2017.
[8] J. Fantaye, "An Introduction and Overview of Privacy-Enhancing Technologies for Data Processing and Analysis," 2022.
[9] H. El-El-Sofany, "A Proposed Biometric Authentication Model to Improve Cloud Systems Security," Computer Systems Science and Engineering, vol. 43, no. 2, pp. 573–589, 2022, doi: 10.32604/csse.2022.024302.
[10] M. I. Mihailescu and S. L. Nita, "A Searchable Encryption Scheme with Biometric Authentication and Authorization for Cloud Environments," Cryptography, vol. 6, no. 1, Mar. 2022, doi: 10.3390/cryptography6010008.
[11] M. Moradi, M. Moradkhani, and M. B. Tavakoli, "A Real-Time Biometric Encryption Scheme Based on Fuzzy Logic for IoT," J Sens, vol. 2022, 2022, doi: 10.1155/2022/4336822.
[12] M. A. Hossain and M. A. Al Hasan, "Improving cloud data security through hybrid verification technique based on biometrics and encryption system," International Journal of Computers and Applications, vol. 44, no. 5, pp. 455–464, 2022, doi: 10.1080/1206212X.2020.1809177.
[13] N. D. Sarier, "Multimodal biometric authentication for mobile edge computing," Inf Sci (N Y), vol. 573, pp. 82–99, 2021.
[14] G. Balamurugan, K. B. Jayarraman, V. Arulalan, and V. Lokesh, "Multimodal biometric key generation for cryptographic security using face and iris," Advances in Natural and Applied Sciences, vol. 9, no. 6 SE, pp. 525–531, 2015.
[15] A. Vankadara, V. Myneni, H. Pendyala, and D. Vadlamudi, "Enhancing Encryption Mechanisms using SHA-512 for user Authentication through Password & Face Recognition," in 2023 International Conference on Inventive Computation Technologies (ICICT), 2023, pp. 1086–1095. doi: 10.1109/ICICT57646.2023.10134233.
[16] T. Kaur and M. Kaur, "Cryptographic key generation from multimodal template using fuzzy extractor," in 2017 Tenth International Conference on Contemporary Computing (IC3), IEEE, 2017, pp. 1–6.
[17] E. Uzun, C. Yagemann, S. Chung, V. Kolesnikov, and W. Lee, "Cryptographic key derivation from biometric inferences for remote authentication," in Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, 2021, pp. 629–643.
[18] M. Arunachalam and K. Subramanian, "AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print.," Int. Arab J. Inf. Technol., vol. 12, no. 5, pp. 431–440, 2015.
[19] C. Miyazawa and R. Sato, "Biometric Fusion for Enhanced Authentication in Cloud Computing Environments," Advances in Engineering and Intelligence Systems, vol. 3, no. 01, pp. 58–69, 2024.
[20] S. Pahuja and N. Goel, "Multimodal biometric authentication: A review," AI Communications, no. Preprint, pp. 1–23, 2024.
[21] D. M. Ahmed et al., "A state of art for survey of combined iris and fingerprint recognition systems," Asian Journal of Research in Computer Science, pp. 18–33, 2021.
[22] N. Bala, R. Gupta, and A. Kumar, "Multimodal biometric system based on fusion techniques: a review," Information Security Journal: A Global Perspective, vol. 31, no. 3, pp. 289–337, 2022.

Authors' Profiles

Mukesh Kumar is an Associate Professor at Chandigarh Group of Colleges, Jhanjeri, Mohali, Punjab, India. He holds a Ph.D. in Computer Science from Himachal Pradesh University, Shimla, where he specialized in designing ensemble and hybridized data mining techniques for analyzing academic performance. With over 15 years of experience in academia, Dr. Kumar has held various teaching positions, including Assistant Professor at Lovely Professional University and Chitkara University. He has contributed to various international conferences and holds intellectual property rights for several innovations. He is also a reviewer for multiple prestigious journals and a member of several professional organizations, including the International Association of Engineers and the Indian Society for Technical Education.

Vivek Bhardwaj is an accomplished academician and researcher specializing in Speech Recognition and Robotic Process Automation. Currently serving as an Assistant Professor (Selection Grade) at Manipal University Jaipur, he brings over a decade of experience in teaching, research, and innovation. He holds a Ph.D. and M.E. in Computer Science and Engineering from Chitkara University and a B. Tech from Himachal Pradesh University. Dr. Bhardwaj has published extensively in high-impact journals, including Q1-ranked journals, and authored several books and book chapters in emerging fields like Conversational AI and Quantum Computing. An Automation Anywhere Certified RPA Trainer, he has contributed significantly to advancing robotic process automation through workshops, patents, and cutting-edge research.

Karan Bajaj affiliated with Lovely Professional University, focuses on areas like Edge/Fog Computing, IoT, and Machine Learning. His research includes topics such as IoT-based offloading frameworks, WSN integration with IoT, and intrusion detection systems. His most cited work is the "Implementation analysis of IoT-based offloading frameworks on cloud/edge computing," with 112 citations as of 2022. Bajaj has contributed significantly to the field, particularly in integrating wireless sensor networks with IoT and analyzing machine learning models' performance in big data contexts.

Nandini Modi, an IEEE member, currently serves as an Assistant Professor in the Computer Science and Engineering department at Pandit Deendayal Energy University, Gandhinagar. She holds a PhD in Eye gaze tracking during Human computer interactive applications. She is working in the field of computer vision, cognitive science and its applications. Areas of interests include Human computer interaction, Eye gaze tracking, Sentiment analysis, Machine learning, Cognitive computing, smart healthcare solutions. She has contributed to various international conferences and holds intellectual property rights for several innovations. She is also a reviewer for multiple prestigious journals and a member of several professional organizations.

Ahmed Qtaishat finished his master's degree from University Utara Malaysia, in intelligent system in 2007. He joined Sohar University 2011. From 2012 until 2017 he worked as a coordinator in General foundation program. His research area focuses on Artificial Intelligent, Machine Learning and Genetic algorithm. He has published research article in different National and International journals and conferences.

How to cite this paper: Mukesh Kumar, Vivek Bhardwaj, Karan Bajaj, Nandini Modi, Ahmed Qtaishat, "Sustainable Approach to Data Security: Multi-Key Biometric Encryption and Cloud Storage for SDG-Focused Businesses", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.17, No.3, pp. 39-48, 2025. DOI:10.5815/ijieeb.2025.03.03