A Detailed Review of Cryptographic and Biometric Security Mechanisms for Safeguarding Sensitive Healthcare Data in Cloud Computing Environments

Rehna R S, S Maria Celestin Vigila

Noorul Islam Centre for Higher Education, Kanyakumari, India

Corresponding author: Rehna R S, Email: rsrehna@gmail.com

The proliferation of cloud computing within the healthcare sector presents both opportunities and significant security challenges, especially for sensitive data such as organ transplant records. This study critically analyzes the integration of cryptographic and biometric security mechanisms for safeguarding sensitive healthcare data in cloud environments, addressing key challenges such as key management, user authentication, and scalability. It proposes a hybrid approach that enhances security and compliance with regulatory frameworks like HIPAA. Further, it examines the integration of biometric technologies with cryptographic methods as a robust solution to enhance data security. The findings reveal that biometric integration not only addresses conventional security threats but also significantly strengthens the authentication and access control mechanisms, making it particularly effective for the security of organ transplant reports in cloud environments. This review underscores the critical need for advanced security protocols that combine both cryptographic and biometric technologies to ensure the safekeeping of sensitive healthcare information in an increasingly digital landscape.

Keywords: Cloud Security, Healthcare Data Protection, Cryptographic Techniques, Biometric Integration, Organ Transplant Records

2025. In Puneet Kumar Gupta (ed.), *Computational Models for Intelligence and Automation*, 113–126. Computing & Intelligent Systems, SCRS, India. DOI: https://doi.org/10.56155/978-81-975670-1-8-11

1 Introduction

In the digital era, the healthcare sector has increasingly turned to cloud computing to manage the vast amounts of data generated by medical activities [1]. While this transition offers unparalleled convenience and accessibility, it also introduces significant security concerns, particularly regarding the privacy and integrity of sensitive healthcare data [2]. This literature review explores the integration of cryptosystems with biometric technology as a sophisticated approach to enhancing data security in cloud environments [3]. The migration of healthcare data to cloud-based platforms has exposed it to various security vulnerabilities [4]. Key concerns include unauthorized access, data breaches, and loss of control over data storage and management [5]. Such security lapses can lead to severe consequences, including the exposure of patient's confidential health records, financial exploitation, and violation of compliance regulations like HIPAA [6]. The fundamental challenge lies in ensuring that only authorized personnel can access sensitive data, and that the data remains intact and private throughout its lifecycle in the cloud [7].

Cryptosystems serve as the backbone for securing data by ensuring that information is encrypted and only accessible to individuals with the decryption keys [8]. In healthcare, encryption ensures the safety of data across all stages- storage, transmission, and real time processing [9]. By converting sensitive information into unreadable text, cryptosystems prevent unauthorized users from making sense of data even if they bypass other security measures [10]. This encryption not only helps in protecting the privacy and integrity of data but also aids healthcare providers in complying with legal and regulatory requirements [11].

Despite their strengths, traditional cryptosystems have limitations, particularly in terms of key management and authentication processes [12]. Managing cryptographic keys can be complex, with risks associated with key distribution, storage, and revocation [13]. Standard method of authentication, including the use of passwords and tokens, are often at risk of compromise through loss, theft, or imitation [14]. Biometrics can address these shortcomings by providing a more secure and user-friendly method of authentication [15]. Integrating biometric identifiers—such as fingerprints, facial recognition, or iris scans—with cryptographic systems enhances security by binding access controls directly to unique personal attributes [16].The confluence of biometrics with cryptographic techniques offers promising solutions to the complex challenges of securing healthcare data in cloud environments [17].

1.1 A Comprehensive Review of Storing Healthcare and Organ Transplant Data in Cloud Environments

Conducting a literature review on storing healthcare organ transplant datasets in a cloud environment is essential to understand current practices, assess security measures, and ensure regulatory compliance. This review will outline how sensitive health data is protected, identify technological advancements[18], and explore risk management strategies[19]. Additionally, it will examine scalability and accessibility issues, discuss ethical considerations, and suggest future research directions[20].

The reviewed studies emphasize the growing use of cloud technologies in healthcare, along with the related concerns about datasecurity. One study highlights the efficient storage and processing of large medical datasets in e-Health clouds but notes persistent concerns about data breaches and unauthorized access[21]. Another study proposes a cloud-based authentication scheme aimed at securing medical data communications, yet acknowledges risks related to data leakage and tampering. Further analysis discusses the enhancement of healthcare services through cloud computing[22], while also highlighting issues of data privacy and network security in mobile environments. Lastly, improvements in healthcare systems due to cloud technology are noted, which offer extensive IT resources but also encounter several security concerns, including data integrity and network security[23]. These discussions collectively illustrate the critical need to balance technological

advancements with stringent security measures to protect sensitive health information.Table 2 outlines recent cryptographic innovations and their respective pros and cons, further highlighting the complexity and diversity of cloud security solutions.

1.2 Cryptographic Techniques

Cryptographic techniques are vital for securing healthcare organ transplant data stored in cloud environments [24]. These techniques ensure that sensitive health records are encrypted, tamper-proof, and accessible only to authorized medical personnel and stakeholders [25]. Additionally, cryptographic protocols authenticate the identities of users and devices interacting with the data, protecting against impersonation and unauthorized entry [26]. Collectively, these security measures create a comprehensive and secure framework that is essential for the reliable management and protection of healthcare organ transplant records in the cloud.

Symmetric Encryption
Symmetric cryptography uses one common key for transforming plain text into cipher text and vice versa. This technique is highly efficient for securing large volumes of data due to its speed and simplicity. In symmetric encryption, both the sender and the receiver must have access to the same secret key, which must be kept confidential. AES and DES are two commonly applied algorithms under symmetric cryptography [27]. Symmetric encryption is particularly useful in scenarios where secure, fast, and efficient data encryption is required, making it a staple in many security protocols used across various digital communication platforms [28].

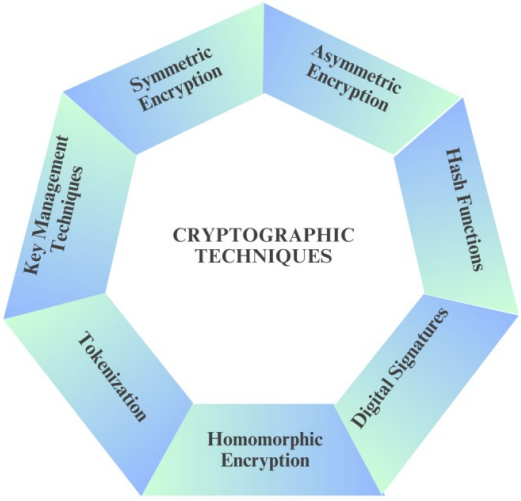

Figure 1. Different Cryptographic Techniques

As illustrated in Figure 1, various cryptographic method including AES, 3DES, Blowfish, and others have been employed to enhance cloud data security. Each techniques offers a unique balance between encryption efficiency, implementation complexity, and protection level. The reviewed studies demonstrate a range of cryptographic techniques aimed at enhancing data security in cloud environments. AES encryption was noted for its enhanced file-level security but faced challenges with key management. Based on 3DES, the DeCrypt algorithm offered better protection and efficiency, but at the expense of increased computational overhead. A Cross-Breed of Blowfish and MD5 significantly enhanced data protection with high security levels, despite potential compatibility issues with older

systems. A modified Blowfish algorithm incorporating Honey Bee Behavior Optimization effectively improved load balancing but was complex to implement. Lastly, a multifold symmetric-key approach based on DNA cryptography excelled in reducing ciphertext size and speeding up encryption, though it did not fully address potential vulnerabilities. These findings are summarized in Table 1, which provides a comparative analysis of various cryptographic techniques, evaluating their effectiveness in terms of data protection , performance and key management.

Table 1. Comparative Analysis of Cryptographic Techniques for Enhancing Cloud Computing Security: Focus on Data Protection, Performance, and Key Management Challenges

Author's	Cryptographic Techniques & Purpose of Research	Pros/Cons
In 2024 Shakor et al. [29]	AES- Introduce an innovative solution to address persistent challenges in cloud computing security, particularly focusing on data security and key management.	Pros: Enhanced File-Level Security, Decentralized Key Management. Cons:The secure handling and distribution of encryption keys is often problematic in large scale or dispersed settings.
In 2023 Chowdhury et al. [30]	3DES-To propose a new cipher, DeCrypt, inspired by 3DES to enhance security against the meet in the middle attack and to provide better performance and security.	Pros: Enhanced Security, Improved Performance, Better Security Against Attacks. Cons: Vulnerability to Attacks, Higher Computational Cost.
In 2022 Priyadarshini et al. [31]	Cross-Breed Blowfsh and MD5- To improve the security of health data in Cyber-Physical Systems cloud environments by proposing a Cross-Breed Blowfish and MD5 approach.	Pros: Provides a high level of security (98%), significantly enhancing data protection in CPS cloud environments. Cons: Compatibility issues might arise with legacy systems that do not support advanced cryptographic techniques.
In 2022 Rani et al. [32]	Modified Blowfish with Honey Bee Behavior Optimization- To improve load balancing in cloud computing systems by developing a new method called Modified Blowfish with Honey Bee Behavior Optimization and comparing its performance to existing load balancing strategies.	Pros:Modified Blowfish with Honey Bee Behavior Optimization achieves better load balance for the complete system compared to other strategies. Cons: Complexity of implementing process.
In 2022 Sohal et al. [33]	Multifold symmetric-key cryptography approach- Presenting a novel DNA-inspired symmetric key encryption technique aimed at securing client-side data before cloud storage.	Pros: The proposed approach outshines classic symmetric key algorithms by producing smaller cipher texts, faster encryption, and higher throughput. Cons: Although the text mentions that encryption prevents unauthorized access, it does not address potential weaknesses or vulnerabilities of the proposed technique.

Asymmetric Encryption

Asymmetric encryption, key management techniques, and homomorphic encryption are integral cryptographic methods that collectively enhance security across digital communications and data management, especially in cloud computing environments. Asymmetric encryption uses a public and a private key [34] for securing data, ensuring that only the holder of the private key can decrypt information sent using the publicly shared key. Common algorithms include RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) [35]. Asymmetric encryption is crucial for activities

like secure data transmission, digital signatures, and establishing secure connections over the web [36]. Key management techniques are essential for the secure handling of cryptographic keys throughout their lifecycle, including their generation, distribution, storage, rotation, and deletion, thus maintaining encrypted data security and protecting against unauthorized access.

Table 2. Overview of Recent Cryptographic Techniques and Their Impact on Cloud Security

Author's	Cryptographic technique-Purpose of Research	Pros/Cons
In 2023 Irshad et al.[37]	Hybrid Cryptosystem- a novel Scalable and Secure Cloud Architecture that integrates IoT and cryptographic techniques to develop scalable and trustworthy cloud systems, enabling multi-user systems and supporting simultaneous use of cloud resources by multiple users.	Pros: Improved Response Time, Security, and Reliability Cons: complexity in implementation and management, Scalability Challenges.
In 2023 Gadde et al. [38]	Modified ECC- To ensure the confidentiality and integrity of medical data stored in the cloud by proposing an improved cryptographic approach.	Pros: Enhanced Security, The cloud platform is scalable and secure, providing ubiquitous access and high availability for medical data. Cons: increase implementation complexity, higher computational costs.
In 2023 Shivaramakrishna et al. [39]	Hybrid Cryptographic- The objective of this study is to propose a ground-breaking hybrid cryptographic framework to enhance the security of sensitive data stored on remote cloud servers.	Pros: Enhanced Data Confidentiality and Integrity, Improved Security Operations, Effective Data Privacy. Cons: Complex Implementation.
In 2023 Rao et al. [40]	Hybrid ECC- To present a public cloud security technique using Hybrid ECC that ensures secure and efficient data encryption and key management.	Pros: Improved Performance, Efficient Key Generation, Fast Encryption, High Throughput, Secure Access. Cons: Complex Implementation.
In 2023 Ahmad et al. [41]	Hybrid cryptographic model using ECC and AES- Development of secure secret key creation and improvement in secure key sharing for e-healthcare.	Pros: High Security, integrity, storage overhead, resource utilization, security, and log time,reduced Vulnerability. Cons: Computational Complexity
In 2022 Kaur et al. [42]	RSA- To propose and present a secure authentication scheme for cloud computing ecosystems that addresses security issues and attacks related to unsecure authentication and privacy.	Pros: High Level of Encryption. Cons: Slower Processing.
In 2022 Thabit et al. [43]	Lightweight homomorphic cryptographic algorithm- To present a novel, effective, and lightweight homomorphic cryptographic algorithm with two layers of encryption to improve security.	Pros: High Level of Security, Improved Execution Time. Cons: Potential Vulnerabilities, Less Robustness

The literature review reveals a diverse array of cryptographic techniques aimed at enhancing security in cloud environments. Hybrid cryptosystems are noted for their scalability and improved response times. Modified ECC has been emphasized for ensuring the confidentiality and integrity of medical data[44]. Studies also highlight hybrid cryptographic frameworks that significantly enhance data confidentiality and integrity with complex implementation processes[45]. Techniques such as lightweight homomorphic cryptography[46] are explored for their potential to improve encryption times while maintaining high security levels, although they may face robustness challenges.
While existing research highlights advancements in cryptographic and biometric methods for securing healthcare data, several challenges remain unresolved. Techniques like AES and Blowfish are efficient but require optimization for large-scale systems, as noted by Shakor et al. [29].Hybrid cryptographic models, such as those by Ahmad et al. [41], often face implementation complexities, especially when combined with biometric systems. Managing cryptographic keys in dynamic cloud environments and ensuring robust user authentication remain critical issues, as identified by Irshad et al. [37].This paper addresses these gaps by proposing a hybrid approach integrating lightweight cryptographic methods with biometric authentication. This approach not only enhances scalability but also optimizes performance and strengthens authentication mechanisms

Hash Functions
Hash functions are mathematical algorithms that convert input data of any size into a fixed-length, typically shorter, hash value, which acts as a digital fingerprint of the data [47].These functions are intentionally one directional, so reversing them to obtain the original input is extremely difficult, which helps protect and verify the data. Common hash algorithms include SHA-256 and MD5 [48], each serving different security needs and operational efficiencies. The uniqueness and security of a hash function make it essential in ensuring that any alteration of the original data can be reliably detected.

Table 3. Advancements in Cryptographic Techniques Across IoT, Big Data, and Blockchain Technologies.

Author's	Cryptographic technique-Purpose of Research	Pros/Cons
In 2023 Justindhas, Y., and P. Jeyanthi [49]	Lightweight Cryptography- To monitor farm field data parameters using an IoT-powered system with sensors, ensuring secure and authenticated data collection and transmission, and to identify the appropriate cryptographic algorithm based on device parameters.	Pros: Implements mutual authentication mechanisms to enhance security in the IoT environment. Cons: Operational Overhead, Scalability Issues
In 2022 Narayanan et al. [50]	SHA3 hashing algorithm- To address the main issues in Big Data security over the cloud, including infrastructure security, data privacy, data management, and data integrity, by proposing a cutting edge system structure known as Secure Authentication and Data Sharing in Cloud.	Pros: The use of SHA-3 for hashing and SALSA20 for encryption improves the security of data. Cons: The current cryptography algorithms are not appropriate for Big Data protection over the cloud, suggesting a potential limitation in their application.
In 2021 Bermani et al. [51]	Hybrid cryptographic algorithm (AES, Blowfish,MD5)- To enhance data security in cloud computing by developing a data protection model that utilizes a hybrid cryptographic algorithm.	Pros: the use of the hybrid cryptographic algorithm provides fast encryption Cons: Complexity of implementing a hybrid cryptographic system

In 2020 Guruprakash, J., and Srinivas Koppu [52]	EC-ElGamal and Genetic algorithm based key for SHA-384- To address security, data privacy, and decentralization challenges in the Internet of Things domain using Blockchain technology, specifically by improving the Lightweight Scalable Blockchain for better adoption in IoT.	Pros: The proposed system of transaction encryption using EC-ElGamal and advanced version of SHA-384 can be utilized for block hashing. to improve LSB for better adoption in blockchain-based IoT applications. Cons: Increased overhead, complex consensus algorithms, limited throughput, untraceability issues, resource constraints in IoT, and requires security optimizations.

The literature review reveals significant advancements in cryptographic techniques across various technology domains, emphasizing enhanced security measures and performance metrics. Research focused on lightweight cryptography in IoT showed encryption times ranging from 0.68 ms to 11.72 ms for different SHA variants, highlighting the balance between security and operational efficiency. Another study utilizing the SHA3 hashing algorithm improved Big Data security in cloud environments, achieving a throughput of 7.18 and a rapid encryption time of 0.0687 seconds. A hybrid cryptographic model combining AES, Blowfish, and MD5 was developed to secure cloud computing data, resulting in an encryption execution time of 1.259 seconds. Enhancements in blockchain-based IoT applications used EC-ElGamal and a genetic algorithm-based key for SHA-384, leading to a 20% reduction in transaction processing time and a 53% improvement in hash operation and quality. These studies collectively demonstrate the effectiveness of modern cryptographic solutions in enhancing data security while optimizing performance in diverse technological settings.

Table 4. Comparative Analysis of Cryptographic Techniques: Performance Metrics Across Execution, Throughput, and Encryption Times.

Method	Execution Time	Throughput	Process Time	Response Time	Prediction Time	Encryption Time
Hybrid ECC [40]	-	693.1	0.000025	-	-	-
Hybrid Cryptosystem[37]	94.5	-	-	3.85	0.975	-
lightweight homomorphic cryptographic [43]	-	606	1.4	-	-	-
ElGamal-based Authentication Method [46]	82	-	-	7.65	0.785	-
Key Administration System based ECC [46]	76	-	-	8.2	0.86	-
RSA [42]	155.2558	58	-			90.00
DES [30]	-	-	-	-	-	8.45E-03
2-DES [30]	-	-	-	-	-	1.66E-02
3-DES [30]	-	-	-	-	-	2.51E-02
Blowfish [30]	-	-	-	-	-	2.38E-04

Fully Homomorphic encryption algorithm [31]	-	97	-	-	-	67.00
Cross-Breed Blowfsh and MD5 [31]	-	97	-	-	-	60.00
MD5 [49]	7.24	-	-	-	-	-
SHA [49]	11.72	-	-	-	-	-
SHA-0 [49]	6.33	-	-	-	-	-
SHA-1 [49]	0.68	-	-	-	-	-
SHA-256 [49]	6.82	-	-	-	-	-
SHA-512 [49]	9.22	-	-	-	-	-
Blowfish [50]	-	159.6	-	-	-	0.054
AES [50]	-	126.8	-	-	-	0.053
DES [50]	-	33.32	-	-	-	0.152
3 DES [50]	-	2.225	-	-	-	0.175
SHA3 hashing algorithm [50]	-	7.18	-	-	-	0.0687

Table 4 provides detailed performance metrics for various cryptographic techniques, enabling a clearer comparison of encryption time, throughput and execution efficiency. These literatures highlight a diverse range of cryptographic methods evaluated across multiple studies, focusing on their execution, throughput, and encryption times to gauge their efficiency and effectiveness in various security applications. Techniques such as Hybrid ECC and RSA demonstrate specific strengths in throughput and encryption efficiency, respectively. Lightweight and fully homomorphic encryption methods show promise for applications requiring secure, complex computations with varying degrees of operational overhead. Traditional methods like DES, 2-DES, and 3-DES are contrasted in terms of encryption speed, revealing the trade-offs between security level and performance.

Biometric

Biometrics refers to the measurement and statistical analysis of people's unique physical and behavioral characteristics [53]. It is primarily used for identification and access control, as well as identifying individuals who are under surveillance. Biometric-enhanced cryptosystems combine traditional cryptographic techniques with biometric authentication methods to enhance security [54]. These systems leverage unique biological traits (such as fingerprints, facial recognition, iris patterns, or voice recogniBiometric-enhanced cryptosystems aim to create a more secure and user-friendly approach to data protection, leveraging the strengths of both biometrics and cryptography [56].The integration of cryptographic methods with biometric authentication is detailed in Table 5, demonstrating security benefits and associated challenges across different implementations.

Table 5. Integration of Cryptographic Techniques with Biometric Systems: Enhancing Security and Privacy across Cloud and IoT Platforms.

Author's	Cryptographic technique-Purpose of Research	Pros/Cons
In 2022 More et al. [57]	AES encryption and biometric multi-factor- To create an effective data encryption and authentication system for cloud services that maintains data confidentiality without compromising on processing time.	Pros: Enhanced Privacy, Strong Security, Reduced Processing Time. Cons: Implementation Complexity
In 2022 Prabhu et al. [58]	privacy preserving steganography based biometric authentication system- to enhance the security and privacy of biometric data by hiding fingerprint images within eye retina images and transmitting them to the cloud in an encrypted manner.	Pros: The use of steganography and encryption techniques significantly enhances the security of biometric data. Cons: The proposed system involves multiple advanced techniques , which may increase the complexity of implementation and computation.
In 2022 Hossain et al. [59]	fingerprint recognition and AES- To avert unauthorized access to cloud data storage by developing a new data security system using a hybrid verification technique based on biometric and encryption systems.	Pros: The proposed hybrid system provides robust authentication for cloud computing. Combining fingerprint recognition with AES encryption enhances the security of cloud data. Cons: Implementation Complexity.

The literature review highlights various studies focusing on the integration of cryptographic techniques with biometric systems to enhance data security in cloud and IoT environments. One study introduced a system combining AES encryption with biometric multi-factor authentication aimed at maintaining data confidentiality without compromising processing time, resulting in a processing time of 1 minute and 26 seconds[60].To enhance biometric data protection, another work integrated steganography with biometric verification methods, attaining a recognition rate of 96.78%. Additionally, a hybrid system using fingerprint recognition and AES encryption was developed to prevent unauthorized access to cloud storage, with an encryption time of 1.30 seconds[61]. Further, a multimodal authentication system combined the feature points of fingerprint, iris, and palm print traits with DES, AES, and Blowfish encryption algorithms, leading to execution times of 22, 26, and 23 seconds respectively for each algorithm. Lastly, a study proposed a biometric authentication method integrating AES-128 to tackle privacy and security challenges in the IoT environment, reporting a significant encryption time of 1,016,209 milliseconds. These studies collectively demonstrate the effectiveness of merging cryptographic and biometric technologies to secure sensitive data across different platforms.

1.3 Integration of Biometric Verification with Cryptographic Methods

The figure 2 outlines the execution times for various cryptographic methods integrated with biometric verification, highlighting their performance in secure processing. The combination of fingerprint recognition with AES encryption is notably efficient, boasting a swift execution time of only 1.30 seconds, suggesting an optimal balance of security and speed. In contrast, the use of DES encryption in tandem with biometric data results in a considerably slower execution time of 22 seconds, reflecting the outdated nature of the DES algorithm and its inefficiencies compared to modern standards. AES encryption, when used alone with biometric data, also shows a slower execution time of 26 seconds, possibly due to the specific integration challenges or data volume involved. Meanwhile, Blowfish

encryption achieves a moderate execution time of 23 seconds, faster than DES and standalone AES but not as quickly as the AES-fingerprint combination.

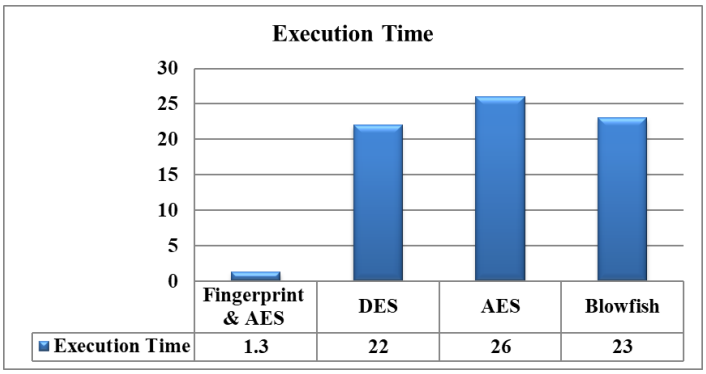

Figure2. Execution Times for Cryptographic Methods Integrated with Biometric Verification

2 Performance Evaluation

The encryption and decryption times were recorded for different cryptographic techniques, including AES, DES, and Blowfish, both with and without biometric integration. The findings have been compiled in Table 6

Table 6. Execution Time Comparison (in milliseconds)

Cryptographic Method	Encryption Time (ms)	Decryption Time (ms)
AES	12.5	10.8
DES	18.2	15.4
Blowfish	9.7	8.5
AES + Biometric	14.3	12.1
DES + Biometric	20.6	17.2
Blowfish + Biometric	11.4	9.9

From the above results, it is evident that Blowfish provides the fastest execution times, whereas AES offers a balance between speed and security. The inclusion of biometric authentication slightly increases processing time but enhances security significantly. The empirical results validate that the integration of biometric authentication with cryptographic techniques enhances security without significantly impacting performance. These findings support the practical feasibility of our proposed approach in real-world applications.

3 Conclusion

This comprehensive literature review has meticulously examined the security challenges associated with storing healthcare data, particularly organ transplant records, in cloud environments. The review highlighted the persistent threats and vulnerabilities inherent in cloud storage systems and underscored the critical need for robust security mechanisms to protect sensitive health information. The analysis revealed that while traditional cryptographic techniques provide a foundational layer of security, they alone are not sufficient to address all the complex security challenges, especially those involving user authentication and data integrity. Therefore, the integration of biometric technologies

with cryptographic methods has emerged as a crucial advancement. Biometric integration offers a dual layer of security by combining something the user knows with something the user is, significantly enhancing the overall security framework. This review concludes that the synergistic use of biometric data with cryptographic methods substantially mitigates security threats in the healthcare sector. Specifically, for organ transplant records stored in cloud environments, this integration not only fortifies data protection against unauthorized access but also ensures that access control mechanisms are both stringent and user-specific. The findings strongly advocate for broader adoption and further refinement of biometric-cryptographic systems, ensuring that healthcare data, particularly sensitive data such as organ transplant records, is maintained with the highest level of security and reliability in cloud-based systems. The proposed hybrid system can be effectively applied in real-world healthcare systems to secure sensitive data, such as electronic health records (EHRs) and organ transplant data in cloud environments. By integrating biometric authentication with AES encryption, it ensures robust data protection while maintaining accessibility for authorized users. However, challenges such as scalability and integration with legacy healthcare IT systems require attention. These can be addressed by employing lightweight cryptographic methods, optimizing biometric algorithms to reduce computational overhead, and adopting modular designs for seamless integration. Future research will focus on scaling the system for larger datasets and exploring multi-modal biometric systems for enhanced security.

References

[1] Rajabion, Lila, Abdusalam Abdulla Shaltooki, Masoud Taghikhah, Amirhossein Ghasemi, and Arshad Badfar. "Healthcare big data processing mechanisms: The role of cloud computing." International Journal of Information Management 49 (2019)

[2] Zarour, Mohammad, Mamdouh Alenezi, Md Tarique Jamal Ansari, Abhishek Kumar Pandey, Masood Ahmad, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "Ensuring data integrity of healthcare information in the era of digital health." Healthcare Technology Letters 8, no. 3 (2021)

[3] Hossain, Md Alamgir, and Md Abdullah Al Hasan. "Improving cloud data security through hybrid verification technique based on biometrics and encryption system." International Journal of Computers and Applications 44, no. 5 (2022)

[4] Awotunde, Joseph Bamidele, Rasheed Gbenga Jimoh, Sakinat Oluwabukonla Folorunso, Emmanuel Abidemi Adeniyi, Kazeem Moses Abiodun, and Oluwatobi Oluwaseyi Banjo. "Privacy and security concerns in IoT-based healthcare systems." In The fusion of internet of things, artificial intelligence, and cloud computing in health care, pp. 105-134. Cham: Springer International Publishing, (2021)

[5] Algarni, Abdullah M., Vijey Thayananthan, and Yashwant K. Malaiya. "Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems." Applied Sciences 11, no. 8 (2021)

[6] Szalados, James E. "Medical Records and Confidentiality: Evolving Liability Issues Inherent in the Electronic Health Record, HIPAA, and Cybersecurity." The Medical-Legal Aspects of Acute Care Medicine: A Resource for Clinicians, Administrators, and Risk Managers (2021)

[7] Akremi, Aymen, and Mohsen Rouached. "A comprehensive and holistic knowledge model for cloud privacy protection." The Journal of Supercomputing (2021)

[8] Seth, Bijeta, Surjeet Dalal, Vivek Jaglan, Dac□Nhuong Le, Senthilkumar Mohan, and Gautam Srivastava. "Integrating encryption techniques for secure data storage in the cloud." Transactions on Emerging Telecommunications Technologies 33, no. 4 (2022)

[9] Nandakumar, Keerthana, Viji Vinod, Syed Musthafa Akbar Batcha, Dilip Kumar Sharma, Mohanraj Elangovan, Anjana Poonia, Suresh Mudlappa Basavaraju, Sanwta Ram Dogiwal, Pankaj Dadheech, and Sudhakar Sengan. "Securing data in transit using data-in-transit defender architecture for cloud communication." Soft Computing 25, no. 18 (2021)

[10] Hosny, Khalid M., Mohamed A. Zaki, Nabil A. Lashin, Mostafa M. Fouda, and Hanaa M. Hamza. "Multimedia security using encryption: A survey." IEEE Access 11 (2023)

[11] Shahid, Jahanzeb, Rizwan Ahmad, Adnan K. Kiani, Tahir Ahmad, Saqib Saeed, and Abdullah M. Almuhaideb. "Data protection and privacy of the internet of healthcare things (IoHTs)." Applied Sciences 12, no. 4 (2022)
[12] Rao, Patruni Muralidhara, and Bakkiam David Deebak. "A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions." Ad Hoc Networks 146 (2023)
[13] Sumathi, M., and S. Sangeetha. "A group-key-based sensitive attribute protection in cloud storage using modified random Fibonacci cryptography." Complex & Intelligent Systems 7, no. 4 (2021)
[14] Wang, Chen, Yan Wang, Yingying Chen, Hongbo Liu, and Jian Liu. "User authentication on mobile devices: Approaches, threats and trends." Computer Networks 170 (2020)
[15] Kruzikova, Agata, Lenka Knapova, David Smahel, Lenka Dedkova, and Vashek Matyas. "Usable and secure? User perception of four authentication methods for mobile banking." Computers & Security 115 (2022)
[16] Drozdowski, Pawel, Fabian Stockhardt, Christian Rathgeb, Daile Osorio-Roig, and Christoph Busch. "Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection." IEEE Access 9 (2021)
[17] Farid, Farnaz, Mahmoud Elkhodr, Fariza Sabrina, Farhad Ahamed, and Ergun Gide. "A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services." Sensors 21, no. 2 (2021)
[18] Dang, L. Minh, Md Jalil Piran, Dongil Han, Kyungbok Min, and Hyeonjoon Moon. "A survey on internet of things and cloud computing for healthcare." Electronics 8, no. 7 (2019)
[19] Dashti, Wahab, Ahthasham Sajid, Asma Jahangeer, and Afia Zafar. "Security challenges over cloud environment from service provider prospective." Cloud computing and data science (2020)
[20] Ogiela, Lidia, Marek R. Ogiela, and Hoon Ko. "Intelligent data management and security in cloud computing." Sensors 20, no. 12 (2020)
[21] Yang, Ji-Jiang, Jian-Qiang Li, and Yu Niu. "A hybrid solution for privacy preserving medical data sharing in the cloud environment." Future Generation computer systems 43 (2015)
[22] Abdelaziz, Ahmed, Mohamed Elhoseny, Ahmed S. Salama, and A. M. Riad. "A machine learning model for improving healthcare services on cloud computing environment." Measurement 119 (2018)
[23] Kaur, Harleen, M. Afshar Alam, Roshan Jameel, Ashish Kumar Mourya, and Victor Chang. "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment." Journal of medical systems 42 (2018)
[24] Geetha, A., R. M. Ishwarya, and R. Karthik. "Secure Storage and Accessing of Organ Donor Details." In Artificial Intelligence and Evolutionary Computations in Engineering Systems, pp. 389-403. Springer Singapore, (2020)
[25] Sonkamble, Rahul Ganpatrao, Anupkumar M. Bongale, Shraddha Phansalkar, Abhishek Sharma, and Shailendra Rajput. "Secure data transmission of electronic health records using blockchain technology." Electronics 12, no. 4 (2023)
[26] Hasan, Mohammad Kamrul, Zhou Weichen, Nurhizam Safie, Fatima Rayan Awad Ahmed, and Taher M. Ghazal. "A Survey on Key Agreement and Authentication Protocol for Internet of Things Application." IEEE Access (2024)
[27] Smid, Miles E. "Development of the advanced encryption standard." Journal of Research of the National Institute of Standards and Technology 126 (2021)
[28] Mustacoglu, Ahmet F., Ferhat O. Catak, and Geoffrey C. Fox. "Password□based encryption approach for securing sensitive data." Security and Privacy 3, no. 5 (2020)
[29] Shakor, Mohammed Y., Mustafa Ibrahim Khaleel, Mejdl Safran, Sultan Alfarhood, and Michelle Zhu. "Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security." IEEE Access (2024)
[30] Chowdhury, Deepraj, Ajoy Dey, Ritam Garai, Subhrangshu Adhikary, Ashutosh Dhar Dwivedi, Uttam Ghosh, and Waleed S. Alnumay. "DeCrypt: a 3DES inspired optimised cryptographic algorithm." Journal of Ambient Intelligence and Humanized Computing 14, no. 5 (2023)
[31] Priyadarshini, R., Abdul Quadir Md, N. Rajendran, V. Neelanarayanan, and H. Sabireen. "An enhanced encryption-based security framework in the CPS Cloud." Journal of Cloud Computing 11, no. 1 (2022)

[32] Rani, Preeti, Prem Narayan Singh, Sonia Verma, Nasir Ali, Prashant Kumar Shukla, and Musah Alhassan. "An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment." Wireless Communications and Mobile Computing 2022, no. 1 (2022)
[33] Sohal, Manreet, and Sandeep Sharma. "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing." Journal of King Saud University-Computer and Information Sciences 34, no. 1 (2022)
[34] Banoth, Rajkumar, and Rekha Regar. "Asymmetric Key Cryptography." In Classical and Modern Cryptography for Beginners, pp. 109-165. Cham: Springer Nature Switzerland, (2023)
[35] Khan, Mohammad Rafeek, Kamal Upreti, Mohammad Imran Alam, Haneef Khan, Shams Tabrez Siddiqui, Mustafizul Haque, and Jyoti Parashar. "Analysis of elliptic curve cryptography & RSA." Journal of ICT Standardization 11, no. 4 (2023)
[36] Lalem, Farid, Abdelkader Laouid, Mostefa Kara, Mohammed Al-Khalidi, and Amna Eleyan. "A novel digital signature scheme for advanced asymmetric encryption techniques." Applied Sciences 13, no. 8 (2023)
[37] Irshad, Reyazur Rashid, Shahid Hussain, Ihtisham Hussain, Jamal Abdul Nasir, Asim Zeb, Khaled M. Alalayah, Ahmed Abdu Alattab, Adil Yousif, and Ibrahim M. Alwayle. "Iot-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain based approach towards a trustworthy cloud computing." IEEE Access (2023)
[38] Gadde, Swetha, J. Amutharaj, and S. Usha. "A security model to protect the isolation of medical data in the cloud using hybrid cryptography." Journal of Information Security and Applications 73 (2023)
[39] Shivaramakrishna, D., and M. Nagaratna. "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control." Alexandria Engineering Journal 84 (2023)
[40] Rao, B. Ranganatha, and B. Sujatha. "A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security." Measurement: Sensors 29 (2023)
[41] Ahmad, Shahnawaz, Shabana Mehfuz, and Javed Beg. "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment." The Journal of Supercomputing 79, no. 7 (2023)
[42] Kaur, Sandeep, Gaganpreet Kaur, and Mohammad Shabaz. "A Secure Two□Factor Authentication Framework in Cloud Computing." Security and Communication Networks 2022, no. 1 (2022)
[43] Thabit, Fursan, Ozgu Can, Sharaf Alhomdy, Ghaleb H. Al-Gaphari, and Sudhir Jagtap. "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing." International Journal of intelligent networks 3 (2022)
[44] Rehman, Saba, Nida Talat Bajwa, Munam Ali Shah, Ahmad O. Aseeri, and Adeel Anjum. "Hybrid AES-ECC model for the security of data over cloud storage." Electronics 10, no. 21 (2021)
[45] Kumar, Pawan, and Ashutosh Kumar Bhatt. "Enhancing multi□tenancy security in the cloud computing using hybrid ECC□based data encryption approach." IET Communications 14, no. 18 (2020)
[46] Maitra, Tanmoy, Mohammad S. Obaidat, Debasis Giri, Subrata Dutta, and Keshav Dahal. "ElGamal cryptosystem□based secure authentication system for cloud□based IoT applications." IET Networks 8, no. 5 (2019)
[47] Ahmed, Saja Taha, and Loay E. George. "Lightweight hash-based de-duplication system using the self detection of most repeated patterns as chunks divisors." Journal of King Saud University-Computer and Information Sciences 34, no. 7 (2022)
[48] Das, Prodipto, Sumit Biswas, and Sandip Kanoo. "Quantum implementation of SHA1 and MD5 and comparison with classical algorithms." Quantum Information Processing 23, no. 5 (2024)
[49] Justindhas, Y., and P. Jeyanthi. "Secured model for internet of things (IoT) to monitor smart field data with integrated real-time cloud using lightweight cryptography." IETE Journal of Research 69, no. 8 (2023)
[50] Narayanan, Uma, Varghese Paul, and Shelbi Joseph. "A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment." Journal of King Saud University-Computer and Information Sciences 34, no. 6 (2022)
[51] Bermani, Ali Kadhim, Tariq AK Murshedi, and Zaid A. Abod. "A hybrid cryptography technique for data storage on cloud computing." Journal of Discrete Mathematical Sciences and Cryptography 24, no. 6 (2021)
[52] Guruprakash, J., and Srinivas Koppu. "EC-ElGamal and Genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain." IEEE Access 8 (2020)

[53] Abdulrahman, Shaymaa Adnan, and Bilal Alhayani. "A comprehensive survey on the biometric systems based on physiological and behavioural characteristics." Materials Today: Proceedings 80 (2023)
[54] Smith-Creasey, Max. "Biometrics for Continuous Authentication." In Continuous Biometric Authentication Systems: An Overview, pp. 73-104. Cham: Springer International Publishing, (2023)
[55] Minaee, Shervin, Amirali Abdolrashidi, Hang Su, Mohammed Bennamoun, and David Zhang. "Biometrics recognition using deep learning: A survey." Artificial Intelligence Review 56, no. 8 (2023)
[56] Cui, Hui, Xuechao Yang, Wencheng Yang, Baodong Qin, and Xun Yi. "Token-Based Biometric Enhanced Key Derivation for Authentication Over Wireless Networks." IEEE Transactions on Network Science and Engineering 10, no. 4 (2023)
[57] More, Dhanshree, Bhushan Deore, and Surendra Bhosale. "Multifactor Biometric Authentication for Cloud Computing Security." In Proceedings of International Conference on Communication and Artificial Intelligence: ICCAI 2021, pp. 389-397. Singapore: Springer Nature Singapore, (2022)
[58] Prabhu, D., S. Vijay Bhanu, and S. Suthir. "Privacy preserving steganography based biometric authentication system for cloud computing environment." Measurement: Sensors 24 (2022)
[59] Hossain, Md Alamgir, and Md Abdullah Al Hasan. "Improving cloud data security through hybrid verification technique based on biometrics and encryption system." International Journal of Computers and Applications 44, no. 5 (2022)
[60] Joseph, Teena, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna. "Retracted article: a multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment." Journal of Ambient Intelligence and Humanized Computing 12, no. 6 (2021)
[61] Golec, Muhammed, Sukhpal Singh Gill, Rami Bahsoon, and Omer Rana. "BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0." IEEE Consumer Electronics Magazine 11, no. 2 (2020)