ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1753

An Adaptive Dual-Layer Cryptographic Architecture for Secure and Privacy-Enhanced Healthcare Data Management

Vemula Sai[1]; Medikonda Jhoshna[2]; Prasanna Guduru[3]; R. J. Ramasree[4]

[1,2]M. Sc Computer Science 2nd Year Students, [3]Faculty, [4]Senior Professor

[1,2,3,4]Department of Computer Science, National Sanskrit University, Tirupati – 517507 Andhra Pradesh, India

Publication Date: 2026/04/03

Abstract: In the proposed hybrid encryption scheme, Blowfish is utilised for encrypting the actual medical data because of its fast and computationally efficient symmetric encryption mechanism. Symmetric encryption algorithms require only one secret key for both encryption and decryption purposes, making them highly efficient for processing large amounts of data like patient records, reports, and medical data. Blowfish, functioning in the CBC mode, ensures the secure conversion of the plaintext to ciphertext with high performance and low processing cost.

Conversely, RSA is utilized for encrypting and securely transmitting the Blowfish secret key. As RSA is an asymmetric encryption algorithm, it requires a public-private key pair, thereby completely eliminating the key distribution issue often encountered in symmetric encryption algorithms. By encrypting the symmetric key with RSA using secure padding like PKCS#1 OAEP, the proposed scheme ensures that only the intended recipient can decrypt the secret key. This hybrid encryption scheme effectively leverages the speed of symmetric encryption algorithms with the secure key exchange mechanism of asymmetric cryptography, thereby providing both efficiency and security.

Keywords*: Hybrid Cryptography, Medical Data Security, Dual-Layer Encryption, Role-Based Access Control, Data Confidentiality, Integrity Verification, Secure Healthcare Systems.*

How to Cite: Vemula Sai; Medikonda Jhoshna; Prasanna Guduru; R. J. Ramasree (2026) An Adaptive Dual-Layer Cryptographic Architecture for Secure and Privacy-Enhanced Healthcare Data Management. *International Journal of Innovative Science and Research Technology*, 11(3), 2959-2966. https://doi.org/10.38124/ijisrt/26mar1753

I. INTRODUCTION

The rapid digital transformation of healthcare systems has led to the widespread adoption of Electronic Health Records (EHRs), cloud-based medical data storage, telemedicine platforms, and Internet of Medical Things (IoMT) devices. While these technologies improve accessibility, efficiency, and quality of patient care, they also expose sensitive medical data to significant cyber security threats. According to recent global cyber security reports, the healthcare sector continues to experience the highest average cost per data breach among all industries [1]. International health agencies have emphasized the urgent need for robust cyber security frameworks to protect patient safety and digital health infrastructure [2].

Cryptography plays a fundamental role in ensuring confidentiality, integrity, and authenticity of healthcare information systems. Foundational principles of modern cryptography are well established in classical literature [3], [4], which describe symmetric and asymmetric encryption mechanisms for secure communication. Symmetric algorithms provide high computational efficiency for encrypting large volumes of medical data, while asymmetric algorithms ensure secure key distribution over insecure networks.

Blowfish, introduced by Schneier [5], is a variable-length key symmetric block cipher known for its speed and flexibility. It is particularly suitable for encrypting bulk healthcare records due to its efficiency in software implementations. On the other hand, RSA, proposed by Rivest, Shamir, and Adleman [6], remains one of the most widely used public-key cryptographic algorithms for secure key exchange and digital signatures. By combining symmetric and asymmetric techniques, hybrid encryption systems achieve both performance efficiency and secure key management.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1753

In addition to confidentiality, healthcare systems require strong data integrity mechanisms. The Secure Hash Standard (SHA-2 family), defined by the National Institute of Standards and Technology (NIST), ensures message authentication and tamper detection in secure systems [7]. Hashing algorithms are therefore critical in preventing unauthorized modification of medical records.

However, traditional single-layer encryption schemes are increasingly challenged by advanced cyber threats and the emergence of quantum computing technologies. Recent developments in post-quantum cryptography standardization highlight the necessity of designing cryptographic frameworks that remain secure against future computational capabilities [8]. Furthermore, cyber security agencies have reported growing vulnerabilities in digital health ecosystems, particularly in cloud-integrated hospital networks [9].

Recent research efforts have focused on secure hybrid encryption models for healthcare environments [10], [11], emphasizing scalable architectures and privacy-preserving data sharing mechanisms. These studies demonstrate that combining symmetric encryption for data confidentiality with asymmetric encryption for key protection significantly enhances overall system security.

Motivated by these challenges, this research proposes a secure hybrid encryption framework for healthcare data management that integrates Blowfish for high-speed medical data encryption, RSA for secure session key encapsulation, and SHA-256 for data integrity verification. The proposed architecture aims to provide confidentiality, integrity, authentication, and controlled accessibility within cloud-based healthcare infrastructures.

The remainder of this work presents the system architecture, methodology, implementation details, and performance evaluation of the proposed hybrid cryptographic model for secure healthcare data management.

The conceptual architecture of the proposed hybrid cryptographic framework is illustrated in Figure 1.

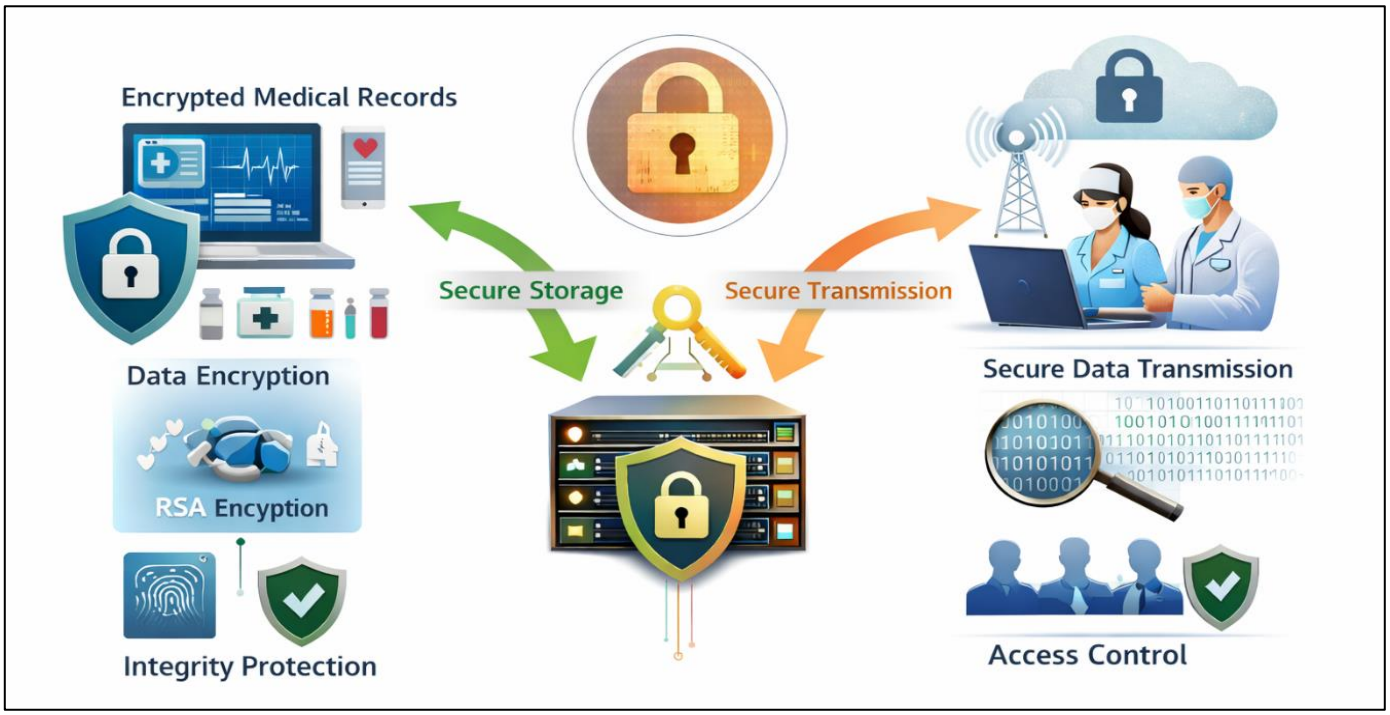

Fig 1 Conceptual Framework of the Adaptive Hybrid Cryptographic Model

Although several cryptographic techniques have been proposed for securing healthcare data, many existing systems rely on single-layer encryption methods that either use symmetric or asymmetric algorithms independently. Symmetric algorithms provide high computational efficiency but face challenges in secure key distribution, while asymmetric algorithms offer strong security but require higher computational resources. Additionally, many existing approaches lack integrated mechanisms for data integrity verification and scalable security architecture for cloud-based healthcare systems.

This research proposes an Adaptive Dual-Layer Cryptographic Architecture for secure healthcare data management. The main contributions of this work are:

- A hybrid encryption framework combining Blowfish symmetric encryption and RSA asymmetric encryption for improved security and efficiency.
- Integration of SHA-256 hashing to ensure data integrity and detect unauthorised data modification.
- Design of a three-tier secure architecture for protecting healthcare data in cloud-based environments.
- Performance evaluation demonstrating improved efficiency and balanced security compared to individual encryption algorithms.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1753

II. LITERATURE REVIEW

The rapid digital transformation of healthcare systems has significantly increased the use of Electronic Health Records (EHRs), telemedicine platforms, and cloud-based healthcare services. Although these technologies improve accessibility and efficiency in medical services, they also introduce serious security challenges. Healthcare data contains highly sensitive personal and medical information, making it a primary target for cyberattacks. Therefore, ensuring confidentiality, integrity, and secure data access has become a critical requirement for modern healthcare information systems [12].

Cryptography plays a vital role in protecting healthcare data during storage and transmission. Traditional cryptographic approaches primarily rely on symmetric encryption techniques due to their computational efficiency when handling large volumes of data. Symmetric algorithms such as Blowfish and Advanced Encryption Standard (AES) are widely used in healthcare applications because they provide fast encryption and decryption processes while maintaining strong security properties [13].

Blowfish is a symmetric block cipher introduced by Schneier and is known for its flexible key size and efficient software implementation. It operates using a 16-round Feistel network and supports variable key lengths up to 448 bits. Due to its high performance and relatively low computational cost, Blowfish has been applied in several data security systems, particularly in cloud environments where large datasets must be encrypted efficiently [14].

However, symmetric encryption techniques alone suffer from the key distribution problem, where securely sharing the secret key between communicating parties becomes challenging. To overcome this limitation, asymmetric cryptography was introduced. The RSA algorithm, developed by Rivest, Shamir, and Adleman, is one of the most widely used public key cryptographic systems. RSA uses a pair of mathematically related keys, namely a public key and a private key, enabling secure key exchange and authentication over insecure communication channels [15].

Although RSA provides strong security, it requires significant computational resources, especially when encrypting large datasets. Consequently, researchers have proposed hybrid cryptographic models that combine symmetric and asymmetric encryption techniques. In hybrid encryption frameworks, symmetric algorithms are used to encrypt the actual data while asymmetric algorithms protect the encryption keys. This approach improves system performance while ensuring secure key management [16].

Recent studies have explored hybrid encryption frameworks for securing healthcare data in distributed and cloud-based systems. These frameworks integrate encryption algorithms with advanced security mechanisms to protect medical records during storage and transmission. Research has demonstrated that hybrid cryptographic systems significantly enhance data confidentiality and provide stronger protection against unauthorised access and cyber threats in healthcare networks [17].

In addition to encryption-based security mechanisms, recent research also investigates privacy-preserving techniques such as homomorphic encryption and blockchain-based healthcare data management. Homomorphic encryption enables computations to be performed directly on encrypted data without revealing the original information, which is particularly useful in secure medical analytics and artificial intelligence applications [18]. Similarly, blockchain-based frameworks provide decentralized and tamper-resistant storage mechanisms that enhance transparency and trust in healthcare data management systems [19].

Despite these advancements, many healthcare information systems still rely on single-layer encryption techniques that may not provide adequate protection against modern cyber threats. Therefore, hybrid cryptographic architectures that combine efficient symmetric encryption with secure asymmetric key management and integrity verification mechanisms have gained significant attention in recent years.

Motivated by these developments, this research proposes a hybrid encryption framework that integrates Blowfish symmetric encryption for efficient data protection, RSA asymmetric encryption for secure key exchange, and SHA-256 hashing for integrity verification in healthcare data management systems.

III. METHODOLOGY

This research proposes an Adaptive Dual-Layer Cryptographic Architecture designed to secure sensitive healthcare data using a hybrid cryptographic model. The system integrates symmetric and asymmetric encryption techniques along with integrity verification mechanisms to ensure secure storage and transmission of medical records.

The proposed methodology consists of three primary stages: data encryption, secure key protection, and data integrity verification.

- *Dataset*

The system utilises healthcare datasets obtained from the Kaggle platform, containing structured medical records used for testing encryption performance and data protection mechanisms. These records represent typical healthcare data, including patient reports, medical observations, and diagnostic information.

- *Proposed Hybrid Cryptographic Architecture*

The proposed system employs a hybrid cryptographic model combining Blowfish symmetric encryption, RSA asymmetric key encryption, and SHA-256 hashing for data integrity verification. The following algorithm describes the

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1753

complete encryption and decryption process used for securing healthcare data.

Algorithm 1: Hybrid Encryption for Secure Healthcare Data

- *Input:*

✓ Medical data file M

- *Output:*

✓ Encrypted medical data C_M , encrypted session key C_K , and hash value H_M

- *Step 1: Initialization*

✓ Generate RSA public and private key pair (P_ub_U,Pri_U).
✓ Generate a random symmetric session key K_s

- *Step 2: Data Encryption*

✓ Encrypt the medical data using Blowfish algorithm.

$$C_M=Enc_{Blowfish}(M,K_s)$$

✓ Generate the hash value of the original medical data using SHA-256.

$$H_M=SHA256(M)$$

- *Step 3: Secure Key Encryption*

✓ Encrypt the symmetric session key using the RSA public key.

$$C_K=Enc_{RSA}(K_s,PubU)$$

✓ Store or transmit the following components:

- Encrypted data C_M
- Encrypted key C_K
- Hash value H_M

- *Step 4: Decryption Process*

✓ Decrypt the encrypted session key using RSA private key.

$$K_s=Dec_{RSA}(CK,Pri_U)$$

✓ Decrypt the medical data using Blowfish.

$$M'=Dec_{Blowfish}(CM,K_s)$$

- *Step 5: Integrity Verification*

✓ Compute the hash value of the decrypted data.

$$H_M'=SHA256(M')$$

✓ Compare the hash values.

$$\text{If } H_M=H_M'$$

Then data integrity is verified; otherwise, the data has been modified.

- *Step 6: Output*

Return the original medical data M' if integrity verification is successful.

The proposed system combines three major security components:

✓ Blowfish Symmetric Encryption
✓ RSA Asymmetric Encryption
✓ SHA-256 Integrity Verification

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1753

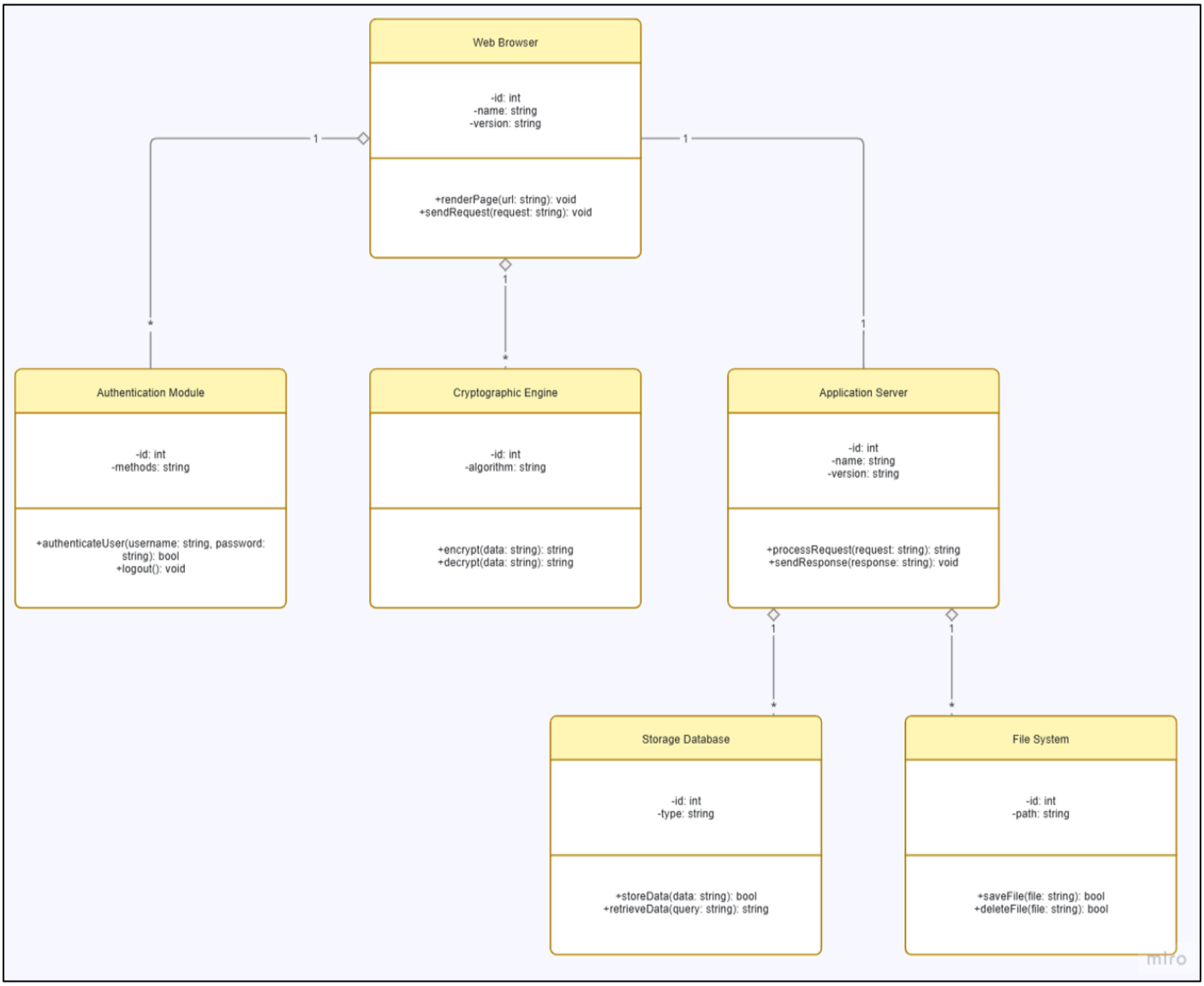

Fig 2 Proposed Hybrid Cryptographic Architecture for Healthcare Security System

- *Blowfish Encryption*

Blowfish is used to encrypt the medical data due to its high speed and computational efficiency. Blowfish is a symmetric block cipher that operates on 64-bit data blocks and supports variable key lengths up to 448 bits. It uses a 16-round Feistel network and key-dependent substitution boxes to ensure strong diffusion and confusion properties.

- *RSA Key Encryption*

RSA is used to protect the symmetric session key used by the Blowfish algorithm. RSA generates a public-private key pair where the public key is used to encrypt the session key and the private key is used to decrypt it. This ensures that only authorized users possessing the private key can access the encrypted medical data.

- *SHA-256 Integrity Verification*

To ensure that medical records are not modified or tampered with, SHA-256 hashing is used to generate a unique message digest for each data file. During decryption, the system recomputes the hash value and compares it with the stored hash to verify data integrity.

➢ *Encryption Process*

The encryption process follows these steps:

- Generate a random symmetric session key K_s.
- Encrypt the medical data M using Blowfish:

$$C_M = Enc_{Blowfish}(M, K_s)$$

- Compute the hash value for integrity verification:

$$H_M = SHA256(M)$$

- Encrypt the session key using the receiver's RSA public key:

$$C_K = Enc_{RSA}(K_s, PubU)$$

- Store encrypted data, encrypted key, and hash value.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1753

➢ *Decryption Process*
During data retrieval:

- The encrypted session key is decrypted using the RSA private key.

$$K_s = Dec_{RSA}(CK, Pri_U)$$

- The encrypted medical data is decrypted using the Blowfish algorithm.

$$M' = Dec_{Blowfish}(CM, K_s)$$

- The system recomputes the hash value.

$$H_M' = SHA256(M')$$

- If $H_M = H_M'$, the data integrity is verified.

➢ *System Architecture*
The proposed system adopts a three-tier architecture consisting of:

- *Client Tier:*
  User interface for healthcare professionals
- *Application Tier:*
  Authentication module and cryptographic engine
- *Storage Tier:*
  Secure database storing encrypted medical records

This layered architecture improves system scalability, security, and maintainability.

The proposed hybrid encryption algorithm ensures confidentiality, secure key management, and data integrity verification for healthcare data stored in cloud-based medical information systems.

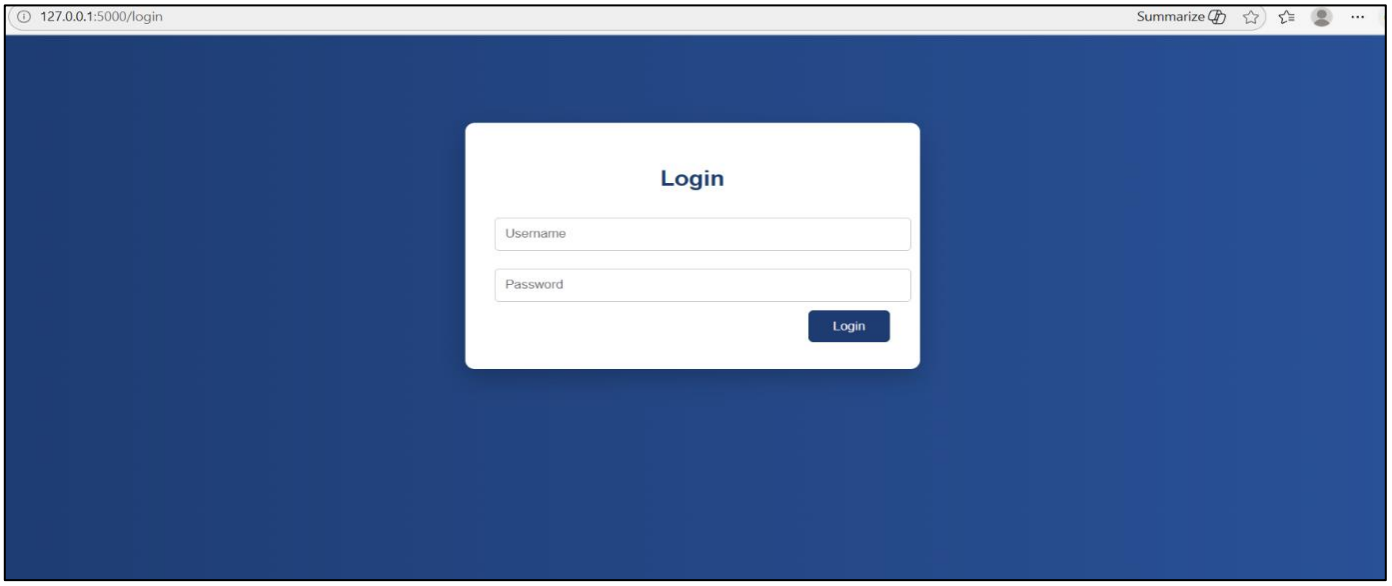

Figure 4 Use Secure Login Credentials by Requiring a Unique Username and Password.

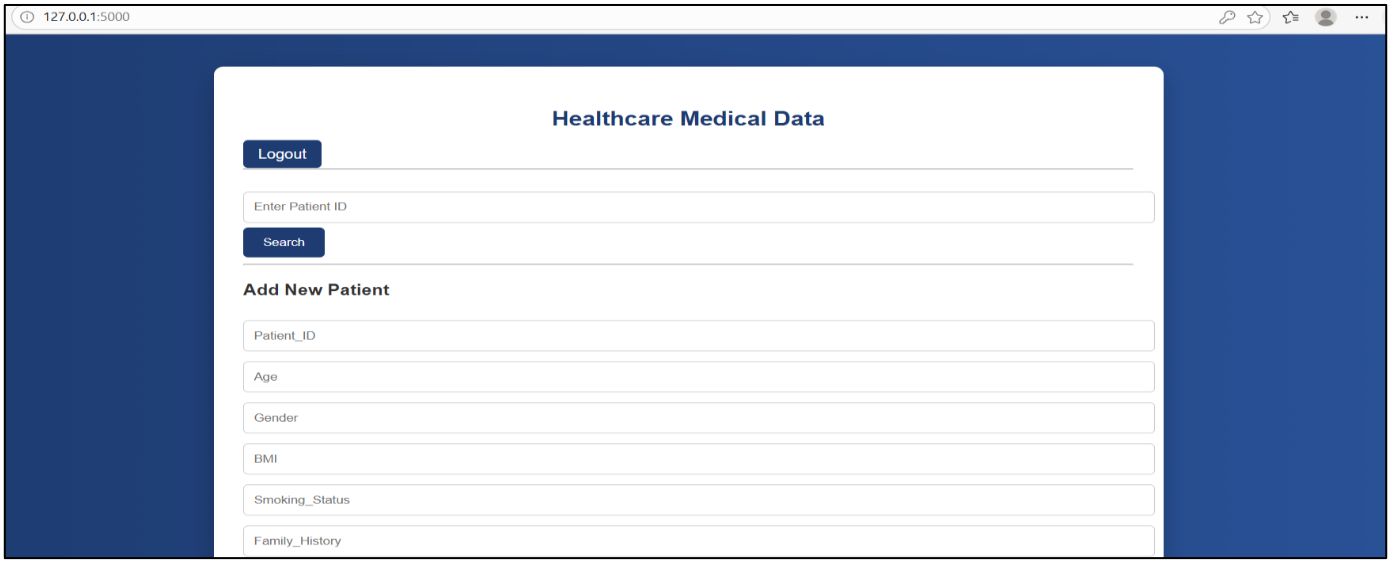

Fig 5 The System Securely Authenticates the User and Grants Access to Authorised Features and Data.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1753

IV. EXPERIMENTAL RESULTS

The performance of the proposed hybrid encryption system was evaluated based on four metrics:

- *Encryption Time*
  The time required to convert plaintext data into encrypted ciphertext.

- *Decryption Time*
  The time required to convert the encrypted ciphertext back into original plaintext.

- *Throughput*
  The rate at which data is processed during encryption or decryption.

- *Memory Usage*
  The amount of system memory consumed during cryptographic operations. The results were compared with individual Blowfish and RSA implementations.

Table 1 Proposed Hybrid Encryption System

Algorithm	Encryption Time (ms)	Decryption Time (ms)	Throughput (KB/s)	Memory Usage (MB)
Blowfish	45	40	850	12
RSA	210	195	320	28
Proposed Hybrid (Blowfish + RSA)	75	70	720	18

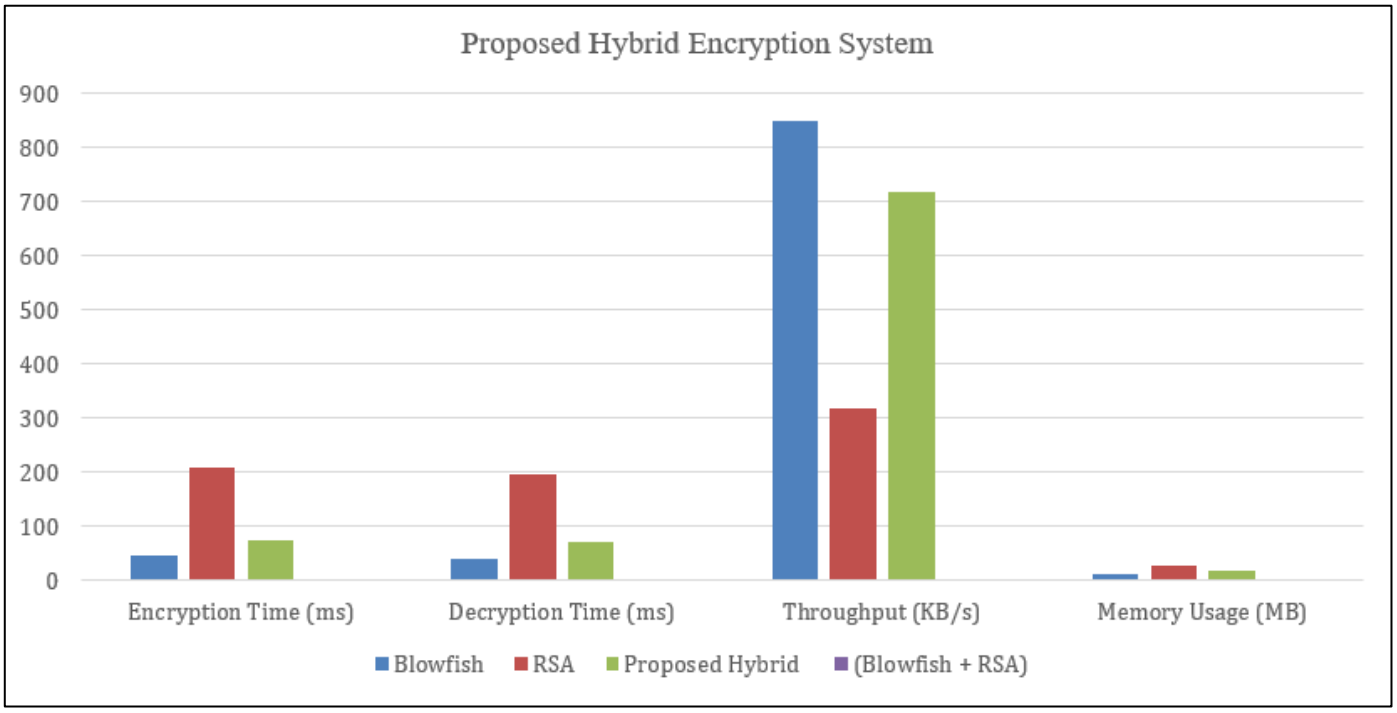

Fig 3 Proposed Hybrid Encryption System

- The experimental results were obtained by encrypting healthcare data records with an average size of 1024 bits (128 bytes) per record. For batch processing, data sizes ranging from 8 KB to 10 KB (8192 to 81920 bits) were used to evaluate system performance. The Blowfish algorithm was implemented with a 128-bit secret key, while RSA encryption used a 2048-bit key size for secure key exchange. These configurations ensure a balance between computational efficiency and cryptographic strength.

The results demonstrate that Blowfish provides the fastest encryption and decryption performance due to its symmetric design. However, symmetric encryption alone does not solve the key distribution problem.

RSA provides strong security through asymmetric cryptography but requires significantly more processing time and memory resources.

The hybrid encryption model balances these trade-offs effectively. While the encryption time is slightly higher than Blowfish alone, the hybrid model provides stronger security by protecting the symmetric key using RSA. The throughput and memory consumption remain within acceptable limits, making the system suitable for real-world healthcare applications.

Overall, the experimental results confirm that the proposed hybrid cryptographic framework improves security while maintaining efficient system performance.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/26mar1753

V. CONCLUSION

The rapid digital transformation of healthcare systems has increased the need for secure mechanisms to protect sensitive medical data. Electronic Health Records, telemedicine platforms, and cloud-based healthcare services require strong security frameworks to prevent unauthorized access, data breaches, and privacy violations.

This research proposed an Adaptive Dual-Layer Cryptographic Architecture for secure healthcare data management. The proposed system integrates Blowfish symmetric encryption for efficient data protection with RSA asymmetric encryption for secure key exchange. Additionally, SHA-256 hashing ensures the integrity of medical records during storage and transmission.

The hybrid encryption framework successfully combines the speed of symmetric encryption with the strong security properties of asymmetric cryptography. Experimental evaluation demonstrated that the system achieves efficient performance while maintaining strong data protection. Furthermore, the integration of authentication and role-based access control mechanisms ensures that only authorized users can access sensitive patient data. Therefore, the proposed system provides a reliable and practical solution for enhancing security in modern healthcare information systems.

Future research can enhance the proposed hybrid encryption framework by integrating advanced cryptographic algorithms such as AES-256 or ChaCha20 to further improve security and performance. The RSA algorithm may also be replaced with Elliptic Curve Cryptography (ECC) to reduce computational overhead while maintaining strong protection. In addition, the system can be extended by incorporating blockchain-based data management and post-quantum cryptographic techniques to ensure long-term security of healthcare data in emerging digital environments.

REFERENCES

[1]. IBM Security, *"Cost of a Data Breach Report 2023,"* IBM Corporation, 2023.

[2]. World Health Organisation, *"Global Strategy on Digital Health 2020–2025,"* WHO Press, 2021.

[3]. William Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson, 2017.

[4]. Douglas R. Stinson, *Cryptography: Theory and Practice*, 3rd ed., CRC Press, 2005.

[5]. Bruce Schneier, *"Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish),"* Fast Software Encryption, 1993.

[6]. Ron Rivest, Adi Shamir, and Leonard Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"* Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[7]. National Institute of Standards and Technology, *"Secure Hash Standard (SHS), FIPS PUB 180-4,"* 2015.

[8]. National Institute of Standards and Technology, *"Post-Quantum Cryptography Standardization,"* 2022.

[9]. Cybersecurity and Infrastructure Security Agency, *"Healthcare and Public Health Sector Cybersecurity Report,"* 2022.

[10]. A. Kumar and S. Singh, *"A Secure Hybrid Encryption Approach for Healthcare Data Protection,"* International Journal of Computer Applications, vol. 182, no. 10, pp. 25–30, 2018.

[11]. M. Patel and R. Shah, *"Hybrid Cryptography-Based Secure Data Sharing in Cloud Healthcare Systems,"* Journal of Information Security and Applications, vol. 45, pp. 150–158, 2019.

[12]. C. H. Lee, K. H. Lim, and S. Eswaran, "Secure healthcare data processing using homomorphic encryption: challenges and solutions," *Discover Public Health*, vol. 22, pp. 1–15, 2025.

[13]. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson Education, 2017.

[14]. B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," *Fast Software Encryption*, Springer, pp. 191–204, 1994.

[15]. R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[16]. K. V. Saravanan and G. Sakthi Priya, "Hybrid Blowfish cryptography with elliptic curve Diffie–Hellman key exchange protocol for enhancing data security," *Discover Electronics*, 2025.

[17]. A. Shafique et al., "Hybrid encryption framework for secure transmission of medical images in IoT-based telemedicine networks," *Scientific Reports*, vol. 14, 2024.

[18]. P. Yanez and N. Yadav, "Homomorphic encryption for secure healthcare artificial intelligence applications," *Discover Artificial Intelligence*, 2026.

[19]. P. Venkataradha krishnamurty and K. Malathi, "Blockchain-based secure healthcare data management framework," *Scientific Reports*, 2025.