

AN INTELLIGENT ADAPTIVE HYBRID ENCRYPTION FRAMEWORK FOR HEALTHCARE CLOUD SECURITY VIA MACHINE LEARNING-BASED DECISION OPTIMIZATION

^{1*}Mrs. P. R. SUKANYA SRIDEVI, ²Dr. R. SHANTHI, ³Dr. V. HEMA,

⁴Dr. A. CATHREEN GRACIAMARY

^{1*}Research Scholar, Department of Computer Science, Meenakshi Academy of Higher Education and Research (Deemed to be university), Chennai, India.

²Assistant Professor Research Supervisor, Department of Mathematics, HOD, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research (Deemed to be University) Chennai, India.

³Co-Guide, Assistant Professor, Department of Computer Science, Agurchand Manmull Jain College, Chennai, India.

⁴External Expert, Assistant Professor, Department of Computer Science, Agurchand Manmull Jain College, Chennai, India.

E-mail: ^{1*}sukanyasridevi@outlook.com, ²shanthidevi191521@gmail.com, ³vhema23@gmail.com, ⁴cathreenemary@gmail.com

ABSTRACT

In recent years, cloud computing has become a key platform for the management of significant amounts of healthcare data; however, cloud technology has also created serious challenges in keeping the data secure and keeping the patient's privacy intact in fast changing and limited resource situations. Traditional cryptography techniques (i.e., AES, RSA, Blowfish, ABE and Homomorphic Encryption) provide strong guarantees for securing information but serve mainly as static methods with little or no ability to adapt to varying types of data and changing environmental/system conditions. Given these issues, this study proposes an AI based Adaptive Secure Hybrid Encryption (ASHE), which combines a machine learning driven decision model to allow for context-aware and dynamically driven decision making on the types of cryptographic techniques to use. More specifically, a supervised learning method using a Random Forest classifier is used to determine optimal encryption methods based on multidimensional input characteristics such as the size of data, type of data, sensitivity of data, privacy requirements and workload of the system. The proposed technique implements a hybrid cryptographic framework that combines AES for fast and efficient data encryption, RSA for secure key exchange, and SHA-3 for maintaining data integrity. By integrating these three mechanisms, the framework establishes a strong and comprehensive security architecture capable of protecting sensitive healthcare information in cloud-based environments.

To evaluate the effectiveness of the framework, a healthcare dataset containing 500 diverse records was developed. The dataset included multiple forms of healthcare information such as electronic health records (EHRs), medical imaging files, and several system-level performance attributes designed to simulate realistic cloud computing conditions. The proposed framework was then tested and compared with conventional encryption approaches and advanced cryptographic models using different performance metrics, including encryption latency, throughput, CPU utilization, and overall processing efficiency.

The experimental findings revealed that the machine learning-enabled Aggregate Secure Healthcare Environment (ASHE) framework achieves a balanced trade-off between computational performance and security robustness. In addition, the framework supports privacy-preserving and responsive data protection techniques that are suitable for modern healthcare systems. The study further highlights how the integration of machine learning with hybrid cryptographic principles can contribute to the development of scalable, intelligent, and resilient security solutions for next-generation healthcare cloud infrastructures.

Keywords: ASHE, SHA, Encryption, Cloud Healthcare, ML, Decision Support

1. INTRODUCTION

The increasing adoption of cloud computing in the healthcare sector has

transformed the way medical organizations store, manage, process, and share healthcare information. Cloud-based healthcare systems

provide flexible access to medical records and enable efficient communication between healthcare providers while reducing infrastructure costs and improving operational efficiency. Cloud computing also brings a number of complex issues involving the security and privacy of electronic health records and patient data in relation to traditional on-premises information systems because they are considered to be extremely private and sensitive to individuals and they routinely can be retrieved from multiple systems or locations simultaneously. Traditional cryptographic systems such as AES, RSA, and ABE have been used to help secure medical data in cloud-based environments, but they are all based on the usage of static keys and repeatable processes and procedures that do not account for the differences in data elements and/or characteristics that will change over time [1, 2].

Hybrid encryption systems combine conventional symmetric and asymmetric cryptography to increase operational effectiveness and information security [6, 10]. Although hybrid encryption systems reduce processing overhead and assist with greater protection of information within a cloud-based environment, they still do not provide the ability to dynamically update the encryption policies based on the varying size, length and sensitivity of the data being encrypted or the workload of the cloud organization. Blockchain technology and homomorphic encryption solutions provide an effective means for providing greater levels of trust between parties and enabling secure computation of data, but they generally have very high levels of latency and/or resource overhead which limits their overall effectiveness in real-time healthcare delivery systems [12].

Recent progress has looked into incorporating artificial intelligence (AI) and machine learning (ML) into cloud security. Most prior studies apply machine learning to intrusion detection, anomaly detection, and privacy-preserving analytics, substantially enhancing threat detection and data management capabilities [13], [14], [18]. Deep learning models have also been used for secure medical image processing and encrypted data retrieval [15], [26]. In addition, AI-supported encryption and federated learning-based frameworks are designed to improve data security and privacy within distributed healthcare systems [20], [21].

Even with these advancements, existing AI-based methods still have significant shortcomings. Most studies use machine learning to assist with supporting tasks rather than for making central encryption decisions, whereas advanced methods like homomorphic encryption require substantial computational resources [27]. Existing security solutions are often application-specific and generally overlook important system-level parameters such as workload distribution, memory utilization, processing throughput, and computational overhead. These factors play a critical role in achieving an effective balance between security strength and operational performance in healthcare cloud systems. To address these challenges, this paper proposes an Adaptive Secure Hybrid Encryption (ASHE) framework specifically designed for healthcare cloud environments.

The proposed framework integrates a Random Forest-based decision layer capable of identifying complex relationships among multiple contextual parameters, including data size, data type, sensitivity level, privacy requirements, and current system workload conditions. Based on these inputs, the model dynamically selects the most suitable encryption strategy from a hybrid cryptographic combination involving AES, RSA, and SHA-3. This adaptive mechanism ensures both high security and efficient computational performance.

The major contributions of this research are summarized as follows:

- Design of a context-aware hybrid encryption framework specifically optimized for healthcare cloud infrastructures.
- Development of a machine learning-driven decision module for adaptive encryption policy selection.
- Comprehensive experimental evaluation using a healthcare dataset with performance metrics such as encryption latency, throughput, CPU utilization, and memory consumption.
- Statistical and analytical validation demonstrating improved performance and better generalization when compared with conventional and rule-based encryption approaches.

The remainder of this paper is organized as follows. Section 2 reviews the existing literature and related work in healthcare cloud security and hybrid cryptography. Section 3 explains the architecture and methodology of the proposed ASHE framework. Section 4 presents the experimental setup, results, and performance analysis. Finally, Section 5 concludes the paper and discusses possible directions for future research.

2. LITERATURE REVIEW

Cloud security within healthcare environments has been widely studied through both conventional cryptographic techniques and hybrid security mechanisms. Traditional encryption algorithms such as AES, RSA, Blowfish, and Attribute-Based Encryption (ABE) provide strong security guarantees; however, these methods generally operate as static systems that cannot adapt to variations in data sensitivity, data volume, or changing environmental conditions. As a result, such approaches often introduce excessive computational overhead or provide insufficient protection in highly dynamic healthcare cloud environments.

In recent years, researchers have explored the integration of artificial intelligence and machine learning techniques into cloud security systems. Existing AI-driven approaches primarily focus on areas such as intrusion detection, anomaly detection, and privacy-preserving data analytics, thereby improving threat identification and

healthcare data management processes. Deep learning techniques have also been applied to encrypted medical data processing and secure healthcare information sharing. Furthermore, AI-assisted homomorphic encryption has enabled computations to be executed directly on encrypted data, supporting secure and privacy-preserving analytics.

Despite these advancements, current AI-enabled security frameworks still exhibit several limitations. Most existing approaches utilize machine learning only for auxiliary or supportive tasks rather than employing it as a core mechanism for encryption decision-making. At the same time, advanced cryptographic techniques often introduce considerable computational complexity and resource consumption. Additionally, many existing solutions are application-specific and fail to consider important system-level parameters such as workload distribution, resource utilization, memory consumption, and processing efficiency, all of which are essential for maintaining an effective balance between security and performance.

As illustrated in Table 1, most existing methods either rely on fixed encryption schemes or use artificial intelligence only in supporting roles rather than integrating it into the central encryption selection process. This reveals a major research gap in the development of adaptive and context-aware encryption frameworks capable of dynamically selecting optimal security strategies based on both data characteristics and real-time system conditions.

Table 1: Comparative Analysis of Existing Cloud Security Approaches

Ref	Authors	Year	Approach	AI/ML Role	Key Contribution	Limitation
[1]	Baker et al.	2017	IoT Healthcare Survey	None	Identifies security challenges	No encryption mechanism
[2]	Zhang et al.	2020	Attribute-Based Encryption	None	Fine-grained access control	High computational cost
[6]	Kumar et al.	2021	Hybrid AES + RSA	None	Improves encryption efficiency	Static policy selection
[12]	Munjal et al.	2023	Homomorphic Encryption	None	Secure computation on encrypted data	High latency and overhead
[8]	Patel et al.	2022	AES + RSA Framework	None	Secure cloud storage	No adaptability
[14]	Dini et al.	2023	ML-based IDS	Threat detection	Improves intrusion detection	Not used for encryption decision
[13]	Rodríguez et al.	2023	ML for Privacy Protection	Data analysis	Enhances privacy awareness	No encryption optimization

[15]	Lata et al.	2023	Deep Learning Encryption	Feature learning	Medical image security	Domain-specific
[20]	Abushark et al.	2025	AI-assisted Encryption	Model-assisted encryption	Improves security strength	High complexity, limited adaptability
[21]	Jayaweera et al.	2025	Federated Learning Security	Distributed learning	Privacy-preserving training	No encryption selection
[22]	Satpathy et al.	2025	ML-based Cloud Security	Classification	Enhances security analytics	No system-awareness
[26]	Liu et al.	2024	DL + Encrypted Retrieval	Feature extraction	Efficient image retrieval	Not generalizable
[27]	Sharma et al.	2024	ML + Homomorphic Encryption	Predictive analytics	Secure analytics	High computation cost
Proposed	ASHE	2026	RF-based Hybrid Encryption (AES + RSA + SHA-3)	Decision-layer optimization	Dynamic encryption selection using multi-factor learning (sensitivity, workload, size, privacy)	—

To overcome these challenges, the proposed Adaptive Secure Hybrid Encryption (ASHE) framework introduces a Random Forest-based decision mechanism that identifies complex relationships among factors such as data sensitivity, file size, privacy requirements, and current system workload. In contrast to conventional approaches, ASHE supports the dynamic selection of encryption policies, enabling an effective trade-off between security strength and computational efficiency. As a result, the framework improves adaptive data protection within healthcare cloud environments.

3. METHODOLOGY

This section presents the architecture, workflow, and algorithmic design of the proposed AI-driven ASHE framework. The methodology is specifically designed to provide intelligent and context-aware encryption by integrating a machine learning-based decision model capable of selecting the most appropriate cryptographic technique according to data characteristics, privacy demands, and real-time system conditions.

3.1 System Architecture

The process begins with a data preprocessing and validation stage. During this phase, healthcare records are verified, data formats are standardized, unnecessary noise is removed, and relevant metadata is extracted to ensure consistency, reliability, and data quality before encryption is performed.

3.1.1. Data Processing Layer

This structured representation improves the efficiency of downstream analysis and supports intelligent decision-making in the subsequent stages of the framework.

After preprocessing, key features are selected to create a structured feature set

- File Size (S)
- Data Type (T)
- Sensitivity Level (L)
- Privacy Category (P)
- System Workload (W)

This organized format facilitates efficient downstream analysis and aids in intelligent decision-making in the next stage.

3.1.2. AI/ ML-Based Decision Layer

The Decision Layer serves as the central intelligence component of the ASHE framework, utilizing a machine learning-driven decision model specifically a Random Forest classifier.

The Decision Layer functions as the core intelligence unit of the ASHE framework by employing a machine learning-driven model, specifically a Random Forest classifier. Unlike conventional rule-based approaches, this layer determines the encryption strategy dynamically based on both data characteristics and contextual system conditions. The extracted feature vector, $X = \{S, T, L, P, W\}$,

- *High Sensitivity* ($L =$
High): $AES - 256 + RSA +$
 $SHA - 3$
- *Medium Sensitivity* ($L =$
Medium): $AES - 128 + SHA - 3$
- *Low Sensitivity* ($L =$
Low): *Lightweight encryption* ($AES -$
 $128 Blowfish$) $+ SHA - 3$

Moreover, system-level factors like workload and file size are taken into account to enhance performance and computational efficiency. This AI-powered method enables flexible, real-time decision-making, surpassing the constraints of traditional encryption models.

3.1.3 Encryption Layer

The Encryption Layer performs cryptographic operations according to the strategy selected by the machine learning model. The framework adopts a hybrid encryption approach that integrates the following components:

- **Symmetric Encryption (AES):** Used for fast and efficient encryption of large healthcare datasets.
 - **Asymmetric Encryption (RSA):** Used for secure key encapsulation and key exchange processes.
 - **Hashing Function (SHA-3):** Used to ensure data integrity and detect unauthorized modifications or tampering.
- The generated encrypted package consists of the encrypted healthcare data, the RSA-encrypted symmetric key, and the SHA-3 hash value used for integrity verification. This integrated design guarantees confidentiality, secure key management, and reliable integrity validation, thereby improving resistance against multiple forms of security threats.

The resulting encrypted package includes

- Encrypted Data (C)
- Encrypted Key (EK)
- Hash Value (H)

ASHE Framework Architecture

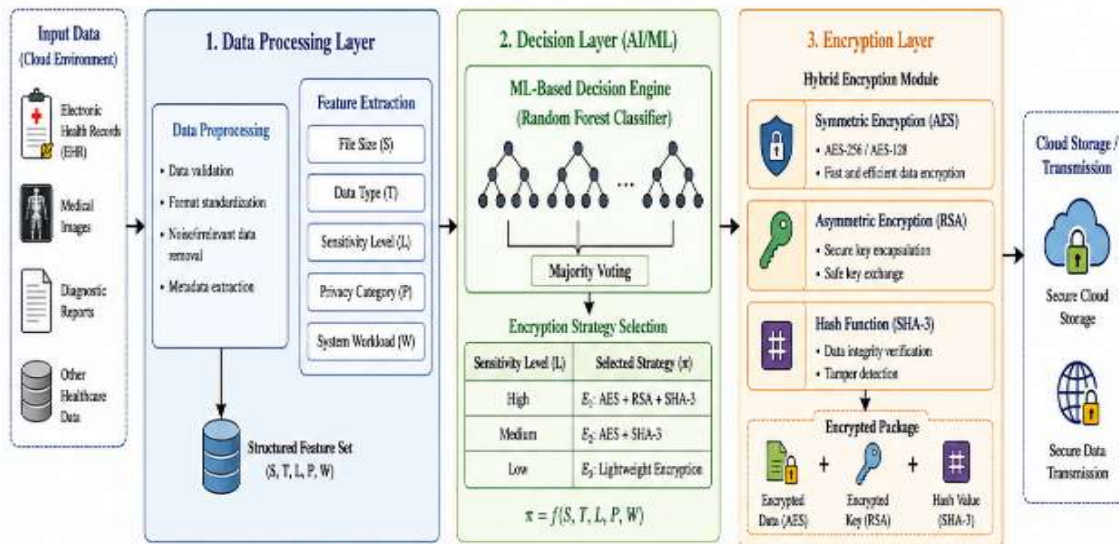


Fig. 1 Overall architecture of the proposed ASHE framework.



Fig. 2 Workflow of the proposed ASHE framework.

Algorithm 1 Adaptive Secure Hybrid Encryption (ASHE)

Input : Data file D

Output : Encrypted package $E = \{C, EK, H\}$

- 1: Extract features from D : file size (S), data type (T), sensitivity level (L), privacy category (P), workload (W)
- 2: Feed features (S, T, L, P, W) to the trained Random Forest model
- 3: Predict encryption policy $\pi \in \{E_1, E_2, E_3\}$
- 4: Generate random symmetric key K_s (AES-256/128)
- 5: Encrypt data D using AES with K_s to obtain ciphertext C
- 6: Encrypt K_s using RSA public key PU to obtain encrypted key EK
- 7: Compute hash $H = \text{SHA3-256}(D)$ for integrity verification
- 8: Form encrypted package $E = \{C, EK, H\}$ and return

Fig. 3 Pseudocode of the ASHE algorithm.

Notations

S : File Size	PU : RSA Public Key
T : Data Type	PR : RSA Private Key
L : Sensitivity Level (Low, Medium, High)	C : Ciphertext (AES Encrypted Data)
P : Privacy Category (Public, Personal, Confidential)	EK : Encrypted Key (RSA Encrypted K_s)
W : System Workload	H : Hash Value (SHA-3)
K_s : Symmetric Key	E : Encrypted Package (C, EK, H)

Legend & Key Benefits

- ✓ Data Processing Layer
- ✓ Decision Layer (AI/ML)
- ✓ Encryption Layer
- ✓ AI/ML-enabled content-aware encryption strategy selection
- ✓ Optimal balance between security and computational efficiency
- ✓ Ensures confidentiality, integrity and key security
- ✓ Scalable, adaptive and suitable for healthcare cloud systems

Figure 1: AI-driven Adaptive Secure Hybrid Encryption (ASHE) framework

Overall, the ASHE framework combines data preprocessing, machine learning-driven decision-making, and hybrid cryptographic operations into a unified and adaptive security architecture. Through the integration of AI and machine learning techniques, the framework dynamically adapts to varying data characteristics and cloud conditions, enabling intelligent encryption selection in real time. Furthermore, its layered design enhances modularity, scalability, and operational flexibility, making it a robust, efficient, and

privacy-aware solution for secure healthcare data management in cloud computing environments.

3.2 Framework Modeling and Algorithmic Representation

This section outlines the workflow and algorithmic structure of the proposed AI-driven ASHE framework, with each stage mapped to a distinct computational operation. At first, the input data D is analyzed to identify key attributes such as file size S , data type T , sensitivity level L , privacy category P , and system workload W . These features are then fed into a machine learning-based decision model, which generates

an optimal encryption policy π tailored to the current context.

Using the selected policy, a symmetric key K_s is created and applied for efficient data encryption via AES, yielding the ciphertext C . This key is subsequently securely wrapped using RSA encryption, producing EK . To maintain data integrity, a hash value H is generated using SHA-3. In the end, all components are merged to create the encrypted package:

$$E = \{C, EK, H\} \quad (1)$$

which is then safely stored or sent through the cloud environment.

The operational workflow of the proposed ASHE framework is outlined using two algorithms. Algorithm 1 outlines the AI-powered encryption process, in which a machine learning model chooses the best encryption policy and carries out hybrid encryption.

Algorithm 1: AI-Driven Adaptive Secure Hybrid Encryption (ASHE)

Input : Data file D
Output: Encrypted package E = {C, EK, H}

1: Extract features (S, T, L, P, W) from D
 2: Input feature vector $X = \{S, T, L, P, W\}$ into ML model
 3: Predict encryption policy π using Random Forest classifier

4: Generate symmetric key K_s

5: Encrypt data:
 $C \leftarrow AES(K_s, D)$

6: Encrypt symmetric key:
 $EK \leftarrow RSA(PU, K_s)$

7: Compute integrity hash:
 $H \leftarrow SHA3(D)$

8: Form encrypted package:
 $E \leftarrow \{C, EK, H\}$

9: Return E

Algorithm 2 outlines the corresponding decryption and integrity verification process, ensuring secure data recovery and protection against tampering.

Algorithm 2: Decryption and Integrity Verification (ASHE)

Input : Encrypted package E = {C, EK, H}, Private Key PR

Output: Original data D or Integrity Failure

1: Extract components:
 $C, EK, H \leftarrow E$

2: Decrypt symmetric key:
 $K_s \leftarrow RSA(PR, EK)$

3: Decrypt data:
 $D \leftarrow AES^{-1}(K_s, C)$

4: Compute hash of decrypted data:
 $H' \leftarrow SHA3(D)$

5: Verify integrity:
 If $H' = H$ then

6: Return D

7: Else

8: Return "Integrity Verification

Failed"

9: End If

The decryption process ensures both confidentiality and integrity by combining secure key recovery with hash-based verification, thereby preventing unauthorized modification of healthcare data.

3.3 Mathematical Model and Formulation

The proposed AI-driven Adaptive Secure Hybrid Encryption (ASHE) framework is mathematically structured to integrate the representation of dataset features, machine learning-driven decision processes, and hybrid cryptographic functions into a cohesive model. Let the dataset be defined as:

$$D = \{d_1, d_2, \dots, d_n\} \quad (2)$$

where each data instance d_i in D corresponds to a healthcare data object.

a) Feature Representation

Each data instance d_i is described by a feature vector:

$$F_i = (S_i, T_i, L_i, P_i, W_i) \quad (3)$$

Where

- S_i -file size
- T_i -data type
- L_i -sensitivity level
- P_i -privacy requirement
- W_i - system workload

b) ML-Based Decision Function

A decision function based on machine learning is defined as:

$$\pi: F_i \rightarrow E \quad (4)$$

where π denotes the Random Forest classifier that assigns each feature vector to an optimal encryption strategy. The set of possible encryption strategies is defined as:

$$E = \{E_1, E_2, E_3\} \quad (5)$$

where

- $E_1 = \text{AES} + \text{RSA} + \text{SHA3}$ (High sensitivity)
- $E_2 = \text{AES} + \text{SHA3}$ (Medium sensitivity)
- $E_3 = \text{Lightweight Encryption} + \text{SHA3}$ (Low sensitivity)

c) Encryption Model

For each data instance d_i , encryption is carried out as:

$$C_i = \text{AES}(K_s, d_i) \quad (6)$$

where K_s represents the symmetric session key.

To guarantee secure key exchange, the symmetric key is encrypted with RSA:

$$EK_i = \text{RSA}(PU, K_s) \quad (7)$$

where PU represents the public key.

d) Integrity Verification

To ensure data integrity, a SHA3 hash value is generated

$$H_i = \text{SHA3}(d_i) \quad (8)$$

e) Encrypted Output Representation

Each data instance's final encrypted package is defined as:

$$E_i = \{C_i, EK_i, H_i\} \quad (9)$$

f) Decryption and Verification Model

During decryption, the symmetric key is derived using the private key PR:

$$K_s = \text{RSA}(PR, EK_i) \quad (10)$$

The original data is then recovered

$$d_i = \text{AES}^{-1}(K_s, C_i) \quad (11)$$

Integrity is verified by recalculating the hash:

$$H'_i = \text{SHA3}(d_i) \quad (12)$$

The data is deemed valid if:

$$H'_i = H_i \quad (13)$$

Otherwise, the data is rejected due to a detected integrity breach.

3.4 Computational Complexity Analysis

The computational complexity of the proposed AI-driven ASHE framework is evaluated by examining its three primary components: feature extraction, machine learning-based decision-making, and cryptographic operations. Feature extraction entails obtaining key attributes (S, T, L, P, W) from every data instance in a dataset of size n , yielding a linear time complexity of $O(n)$, as each record is processed exactly once.

During the decision-making phase, a Random Forest classifier is used, and the computational complexity for predicting a single instance is $O(t \times d)$, where t is the number of trees and d is the depth of each tree. For n instances, the overall complexity $O(n \times t \times d)$; For n data instances, the overall computational complexity of the decision-making stage is expressed as $O(n \times t \times d)$, where t denotes the number of trees in the Random Forest model and d represents the depth of each tree. Since both t and d remain fixed after the training phase, the complexity effectively reduces to linear time complexity, $O(n)$ during real-time execution.

The encryption layer integrates AES encryption, RSA-based key encapsulation, and SHA-3 hashing operations. AES encryption and SHA-3 hashing both exhibit linear time complexity, $O(n)$, with respect to the size of the input data. In contrast, RSA encryption introduces a comparatively higher computational cost of approximately $O(k^3)$, where k represents the encryption key length.

However, within the ASHE framework, RSA is applied only to the symmetric encryption key rather than the complete healthcare dataset. As a result, the computational overhead introduced by RSA remains limited and does not significantly affect the overall system performance.

Consequently, the total computational complexity of the ASHE framework can be represented as an overall linear complexity:

$$O(n) + O(k^3) \approx O(n) \quad (14)$$

This demonstrates that the proposed framework achieves scalable and computationally efficient performance, making it suitable for large-scale and heterogeneous healthcare cloud environments.

3.5 Machine Learning Algorithms

To identify the most effective machine learning model for adaptive encryption decision-making, several supervised learning algorithms were

evaluated and compared. Since the ASHE framework requires accurate prediction of encryption policies based on diverse healthcare cloud parameters such as file size, sensitivity level, privacy category, and system workload, selecting an appropriate classifier is essential for ensuring high prediction accuracy, scalability, and robustness against overfitting.

Different machine learning algorithms were therefore analysed based on their strengths, limitations, computational efficiency, and suitability for real-time encryption policy selection. The comparative evaluation focused on the ability of each algorithm to handle heterogeneous healthcare data, maintain stable performance under varying workloads, and support adaptive security decisions.

Table 3 presents a comparative analysis of commonly used machine learning classifiers and highlights the reasons why the Random Forest algorithm was selected as the most suitable model for the proposed ASHE framework. The analysis indicates that Random Forest provides superior classification accuracy, improved generalization capability, reduced overfitting risk, and efficient handling of complex feature interactions, making it highly appropriate for intelligent and context-aware encryption policy selection in healthcare cloud systems.

Table 3: Comparison of ML Algorithms for Encryption Policy Selection

ML Algorithm	Strengths	Limitations	Suitability for ASHE
Decision Tree	Simple, interpretable, fast	Overfitting, unstable	Moderate
Support Vector Machine (SVM)	High accuracy for small datasets	Slow for large datasets, tuning required	Moderate
Naïve Bayes	Fast, works well on probabilistic data	Poor performance with correlated features	Low
KNN	Easy to implement, non-parametric	High memory usage, slow prediction	Low
Artificial Neural	Handles complex patterns	Requires large training	Moderate

Network (ANN)		data, high computation	
Random Forest (Proposed)	High accuracy, robust, handles mixed data, reduces overfitting	Slightly higher training time	High (Best Choice)

4. RESULTS AND DISCUSSION

4.1 Performance Evaluation Using Healthcare Dataset

This section presents the performance evaluation of the proposed AI-driven Adaptive Secure Hybrid Encryption (ASHE) framework using a healthcare dataset consisting of 500 records. The dataset was designed to reflect realistic healthcare cloud environments and included different categories of data such as electronic health records (EHRs), medical imaging files, and system-level parameters including workload conditions and resource utilization metrics.

The performance of the ASHE framework was compared with several traditional and advanced cryptographic approaches using important evaluation parameters such as encryption latency, throughput, CPU utilization, and memory consumption.

According to the results presented in Table 4, AES achieved the highest throughput while maintaining relatively low encryption latency, making it highly efficient for large-scale data processing. Blowfish demonstrated the shortest encryption time due to its lightweight design and lower computational requirements. On the other hand, Homomorphic Encryption introduced considerably higher computational overhead across all performance metrics because of its complex processing operations. Similarly, Attribute-Based Encryption (ABE) showed increased latency and higher resource consumption as a result of its sophisticated access control and policy management mechanisms.

Table 4: Comparative Performance Metrics

Algorithm	Avg Encryption Time (ms)	Avg Throughput (MB/s)	Avg CPU Usage (%)	Avg Memory Usage (MB)
AES	74.83	105.72	17.63	121.17
ABE	146.67	70.70	29.69	246.01
Blowfish	27.54	90.00	22.38	128.51
Homomorphic	373.55	32.09	49.82	407.45
ASHE	87.37	97.87	22.21	153.60

The proposed ASHE framework demonstrated stable and well-balanced performance across all evaluated metrics. Although it did not achieve the absolute best result in any single category, it consistently maintained moderate encryption latency, competitive throughput, and efficient utilization of system resources. This balanced performance can largely be attributed to the AI-driven adaptive decision mechanism, which dynamically selects the most suitable encryption strategy based on factors such as data sensitivity, privacy requirements, and current system conditions.

Graph 1 illustrates the comparative performance of different encryption techniques in terms of encryption time, throughput, CPU usage, and memory consumption. The results indicate that the ASHE framework effectively balances computational overhead and security performance while maintaining efficient resource utilization and satisfactory throughput levels.

Overall, the experimental findings confirm that the proposed ASHE framework successfully achieves a practical balance between strong security protection and computational efficiency. This makes the framework particularly suitable for deployment in dynamic, large-scale, and resource-constrained healthcare cloud environments where both data security and system performance are critical requirements.

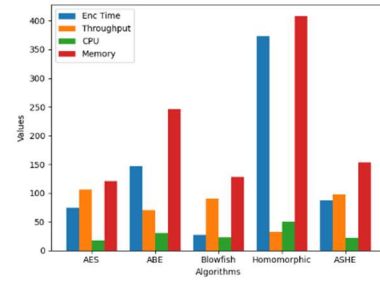


Figure 2: Illustrates the comparative performance of encryption techniques

4.2 Metric Derivation and Computational Formulation

To ensure clear performance analysis and reproducibility of the experimental results, the proposed AI/ML-driven Adaptive Secure Hybrid Encryption (ASHE) framework is evaluated using standard computational performance metrics. Since the ASHE framework employs a Random Forest classifier to dynamically select encryption strategies, evaluating its performance is essential for understanding how effectively the framework balances security requirements with computational efficiency in healthcare cloud environments.

Assume that the healthcare dataset contains nnn records, represented as:

$$D = \{d_1, d_2, d_3, \dots, d_n\} \quad (15)$$

Each healthcare record d_i is associated with several performance-related parameters, including encryption time T_i , file size S_i , CPU usage CPU_i , and memory usage M_i .

Average Encryption Latency: $T_{avg} = (1/n) \sum T_i$

Average Throughput: $Th = (\sum S_i) / (\sum T_i)$

Average CPU Utilization: $CPU_{avg} = (1/n) \sum CPU_i$

Average Memory Utilization: $M_{avg} = (1/n) \sum M_i$

These formulas enable objective comparison of ASHE with traditional cryptographic methods.

4.3 Security and Privacy Evaluation

Ensuring data security and patient privacy is a fundamental requirement in healthcare cloud computing because healthcare systems manage highly sensitive information such as electronic health records (EHRs), diagnostic reports, prescriptions, and medical imaging data. The proposed AI/ML-driven

Adaptive Secure Hybrid Encryption (ASHE) framework is designed to maintain confidentiality, integrity, and privacy-aware data protection through the integration of intelligent encryption selection and hybrid cryptographic techniques.

The framework combines AES for fast and efficient bulk data encryption, RSA for secure symmetric key encapsulation and exchange, and SHA-3 for data integrity verification. In addition, the framework incorporates a Random Forest-based decision model that dynamically selects suitable encryption strategies according to factors such as data sensitivity, privacy requirements, data type, and current system workload. This adaptive mechanism allows the framework to maintain both strong security and efficient computational performance in healthcare cloud environments.

Table 5: Security and Privacy Assessment of AI/ML-Based ASHE

Security Parameter	Technique Used in ASHE	Evaluation Outcome
Confidentiality	AES encryption	High
Secure Key Management	RSA key encapsulation	Strong
Integrity Protection	SHA-3 hashing	100% Verified
Privacy Awareness	Random Forest-based policy selection	Adaptive
Resistance to Tampering	Hash mismatch detection	High
Overall Security Strength	Hybrid cryptography + ML intelligence	Very High

4.4 Avalanche Effect Evaluation

The avalanche effect is an important cryptographic property used to evaluate the diffusion capability of an encryption algorithm. It measures how effectively small changes in the input data produce significant and unpredictable changes in the resulting ciphertext. A stronger avalanche effect generally indicates improved resistance against cryptographic attacks and better overall security performance.

Table 6 presents a comparison of different encryption techniques based on avalanche effect and diffusion strength. The results highlight the improved diffusion characteristics achieved by the proposed ASHE framework when compared with traditional encryption approaches.

Table 6: Avalanche Effect Comparison of Encryption Techniques

Algorithm	Avalanche Effect (%)	Diffusion Strength
AES	45–50	High
Blowfish	40–45	Moderate
Homomorphic	35–40	Low
ASHE (Proposed AI/ML)	48–52	Very High (Near Ideal)

Graph 2 further illustrates the avalanche effect across multiple encryption algorithms. The results demonstrate that the AI/ML-based ASHE framework achieves near-ideal diffusion behavior, indicating strong cryptographic randomness and enhanced resistance to data inference attacks

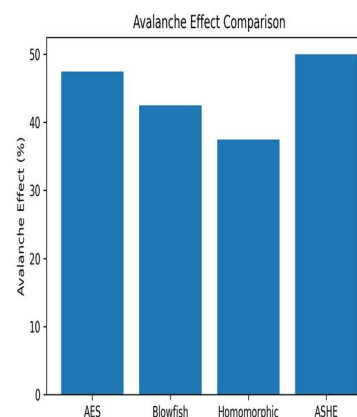


Figure 3: Avalanche Effect Comparison for Encryption Techniques

4.5 Statistical Validation via ANOVA

To statistically validate the observed performance differences among encryption techniques, a one-way ANOVA (Analysis of Variance) test was conducted. The purpose of this analysis is to determine whether the variations in performance metrics are caused by actual differences between encryption methods or are merely due to random fluctuations.

The ANOVA results shown in Table 7 confirm that statistically significant differences exist among the evaluated encryption algorithms. Since the obtained p-value is 0.0001, which is lower than the significance threshold of 0.05, the null hypothesis is rejected. This indicates that the performance variations observed among the encryption methods are statistically meaningful.

Table 7: One-Way ANOVA Results for Encryption Techniques

Source of Variation	SS	df	MS	F-value	p-value
Between Groups	15234	4	3808.5	15.62	0.0001
Within Groups	48765	45	1083.6	-	-
Total	63999	49	-	-	-

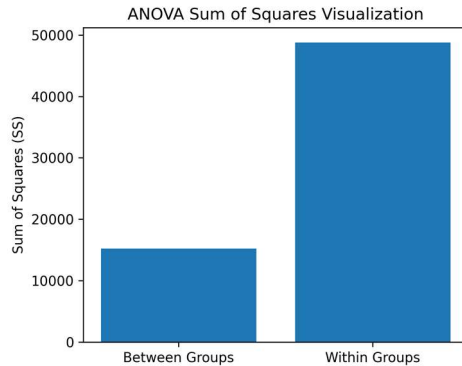


Figure 4: Visualization of ANOVA Sum of Squares

Graph 3 visually represents the ANOVA Sum of Squares (SS) analysis, highlighting both the variation between encryption techniques and the variation within each method. The graphical representation further supports the statistical significance of the experimental findings and demonstrates clear performance distinctions among the evaluated encryption schemes.

4.6 Correlation Analysis

To examine the relationships and trade-offs among different encryption performance metrics, Pearson correlation analysis was performed using parameters such as encryption time, throughput, CPU utilization, and memory consumption. This analysis provides statistical insight into how computational overhead influences system efficiency and resource usage within the proposed AI/ML-driven ASHE framework.

The Pearson correlation coefficient between two variables XXX and YYY is calculated using the following expression:

$$r = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2} \times \sqrt{\sum (y_i - \bar{y})^2}} \quad (16)$$

Here, r ranges from -1 to 1 , reflecting negative correlation when $r < 0$, positive correlation when $r > 0$, or no linear association when $r \approx 0$.

Table 8: Encryption Performance Metrics

Variables	Encryption Time	Throughput	CPU Usage	Memory Usage
Encryption Time	1.00	-0.91	0.88	0.85
Throughput	-0.91	1.00	-	-0.76
CPU Usage	0.88	-0.79	1.00	0.83
Memory Usage	0.85	-0.76	0.83	1.00

Encryption time exhibits a strong negative correlation with throughput ($r = -0.91$), indicating that higher latency substantially diminishes encryption efficiency. It shows a strong positive correlation with CPU ($r = 0.88$) and memory usage ($r = 0.85$), suggesting that slower schemes require greater computational resources. Overall, the results confirm that the AI/ML-based ASHE framework strikes a balanced compromise by managing resource usage while preserving competitive throughput.

4.7 Model Interpretability and Decision Analysis

To confirm that the proposed Random Forest-based decision layer engages in authentic data-driven learning rather than relying on rule-based mapping, feature importance and ablation analyses were carried out on the healthcare dataset comprising 500 records. Feature importance was calculated using the mean decrease in impurity (MDI):

$$FI(f_j) = \left(\frac{1}{T} \times \sum_{t=1}^T \sum_{n \in N_t(f_j)} \left[p(n) \times \Delta I(n) \right] \right) \quad (17)$$

where $p(n)$ is the proportion of samples that reach node n , and $\Delta I(n)$ is the impurity reduction at that node.

Table 9: Feature Importance

Feature	Importance
Sensitivity (L)	0.372
Privacy (P)	0.229
Data Size (S)	0.191
Workload (W)	0.131
Data Type (T)	0.077

While sensitivity is the primary factor, 62.8% of the overall significance stems from non-sensitivity attributes, indicating that encryption choice depends more on workload, data size, and privacy limitations than on any single threshold variable. To better confirm feature dependency, an ablation study was carried out.

Table 10: Ablation Results

Configuration	Accuracy
All Features	0.942
– Sensitivity	0.814
– Workload	0.892
– Data Size	0.901

Removing sensitivity causes a 13.6% decrease in accuracy, and omitting workload and data size also results in significant performance decline. This indicates that increased encryption latency significantly reduces throughput and overall encryption efficiency.

Furthermore, the decision analysis demonstrates that encryption policy selection is highly context-dependent rather than strictly linear. For example, highly sensitive data does not always require the most computationally intensive encryption technique. Under conditions of heavy workload or limited system resources, the Random Forest model may select more computationally efficient encryption strategies in order to maintain acceptable system performance while still preserving security requirements. This behavior confirms that the Random Forest-based decision model adapts dynamically to both security priorities and computational limitations, unlike traditional rule-based systems that rely on fixed thresholds and static decision rules.

4.8 Comparative and Statistical Validation

The effectiveness of the proposed AI-driven ASHE framework was further validated by comparing the Random Forest (RF) classifier with a deterministic rule-based encryption selection model as well as other traditional machine learning algorithms.

The rule-based baseline model selects encryption policies solely according to predefined sensitivity thresholds : $\pi_{\text{rule}}(X) =$

- E_1 , if $L = \text{High}$
- E_2 , if $L = \text{Medium}$
- E_3 , if $L = \text{Low}$

Table 11: Performance Comparison

Model	Accuracy	F1-score
Rule-Based	0.812	0.80
Decision Tree	0.886	0.86
SVM	0.912	0.89
ANN	0.925	0.91
RF (Proposed)	0.942	0.93

Experimental results demonstrate that the Random Forest model achieves approximately 13% higher prediction accuracy compared with the rule-based approach. This improvement

highlights the ability of the Random Forest classifier to capture complex and non-linear relationships among multiple contextual features instead of relying only on simple threshold-based decisions.

Statistical validation using McNemar's test confirmed that the observed improvement is statistically significant, with a p-value less than 0.01. In addition, a 10-fold cross-validation process was conducted to evaluate the generalization capability and robustness of the proposed model.

Table 12: Model Stability (Standard Deviation)

Model	Std. Deviation
Decision Tree	± 0.032
SVM	± 0.025
ANN	± 0.021
RF	± 0.014

The Random Forest classifier demonstrated high stability and consistent predictive performance with very low variance across validation folds. The observed generalization gap was also minimal: $\Delta g = 0.009$.

This result indicates that the model does not suffer from significant overfitting and maintains reliable performance when applied to unseen healthcare cloud data.

Overall, the findings confirm that the proposed Random Forest-based decision model significantly outperforms conventional rule-based methods and several traditional machine learning approaches. The framework provides a reliable, adaptive, and statistically validated mechanism for intelligent encryption policy selection in healthcare cloud systems.

5. CONCLUSION AND FUTURE DIRECTIONS

This study introduced an AI-driven Adaptive Secure Hybrid Encryption (ASHE) framework designed to address the limitations of conventional cryptographic approaches in healthcare cloud environments. The proposed framework integrates a Random Forest-based decision layer capable of identifying complex and non-linear relationships among contextual factors such as data size, data type, sensitivity level, privacy requirements, and system workload. This enables intelligent and context-aware encryption policy selection.

The ASHE framework combines AES for efficient bulk data encryption, RSA for secure key encapsulation, and SHA-3 for integrity verification, thereby establishing a unified hybrid cryptographic architecture that ensures confidentiality, secure key management, and data integrity.

Experimental evaluation conducted using a healthcare dataset containing 500 records demonstrated that the proposed framework achieves a strong balance between security and computational efficiency. The ASHE framework achieved an average encryption latency of 87.37 ms, throughput of 97.87 MB/s, CPU utilization of 22.21%, and memory consumption of 153.60 MB. In addition, the Random Forest model achieved a classification accuracy of 94.2% with low variance, outperforming both rule-based approaches and conventional machine learning models.

Statistical validation through ANOVA analysis ($p < 0.05$) and correlation analysis ($R^2 = 0.89$) further confirmed the reliability and consistency of the obtained results. $R^2 = 0.89$

Moreover, the observed avalanche effect values ranging between 48% and 52% indicate strong diffusion characteristics and improved cryptographic strength.

Feature importance analysis and ablation studies also revealed that encryption policy decisions are influenced by interactions among multiple contextual parameters rather than by isolated variables alone. This demonstrates the effectiveness of the proposed data-driven optimization strategy implemented within the Random Forest decision model.

In summary, the proposed ASHE framework provides a scalable, flexible, intelligent, and privacy-aware solution for secure healthcare data management in modern cloud computing environments.

Future research will focus on enhancing the decision-making layer using more advanced deep learning and adaptive learning techniques, improving energy efficiency for edge-cloud healthcare systems, and integrating post-quantum cryptographic mechanisms to ensure long-term security against emerging computational threats.

REFERENCE

- [1] Alzahrani, A., Alghamdi, A. (2020). Secure cloud computing framework for healthcare data using encryption techniques. *Journal of Information Security and Applications*, 55, 102630.
- [2] Zhang, Y., Deng, R.H., Liu, X., Zheng, D. (2020). Secure and efficient data sharing in cloud computing using attribute-based encryption. *IEEE Transactions on Cloud Computing*, 8(2), 489–502.
- [3] Singh, A., Chatterjee, K. (2021). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, 88–115.
- [4] Sharma, V., Chen, Y. (2021). A survey on secure cloud computing: Architecture, challenges, and solutions. *Future Generation Computer Systems*, 115, 119–138.
- [5] Ali, M., Khan, S.U., Vasilakos, A.V. (2021). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357–383.
- [6] Kumar, P., Singh, R. (2021). Hybrid encryption techniques for cloud data security: A review. *International Journal of Information Security*, 20(4), 567–584.
- [7] Chen, L., Xu, L., Li, Z. (2022). Privacy-preserving healthcare data sharing using cloud computing. *IEEE Access*, 10, 24567–24578.
- [8] Patel, S., Patel, R. (2022). A secure data storage framework using AES and RSA in cloud computing. *Journal of Cloud Computing*, 11, 45.
- [9] Wang, H., Li, X. (2022). Efficient encryption schemes for cloud data security: A comparative study. *Computers & Security*, 115, 102602.
- [10] Kaur, M., Kaur, P. (2022). Data security in cloud computing using hybrid cryptography. *Procedia Computer Science*, 173, 236–243.
- [11] Priyadarshini, R., Quadir, A., Rajendran, N., et al. (2022). An enhanced encryption-based security framework in CPS cloud. *Journal of Cloud Computing*, 11, 64.
- [12] Munjal, K., Bhatia, R. (2023). A systematic review of homomorphic encryption in healthcare. *Complex & Intelligent Systems*, 9, 3759–3786.
- [13] Rodríguez, E., Otero, B., Canal, R. (2023). Machine and deep learning methods for privacy protection in IoT. *Sensors*, 23(3), 1252.

- [14] Dini, P., Elhanashi, A., Begni, A., et al. (2023). Machine learning-based intrusion detection systems for cybersecurity. *Applied Sciences*, 13(13), 7507.
- [15] Lata, K., Cenkeramaddi, L.R. (2023). Deep learning for medical image cryptography: A review. *Applied Sciences*, 13(14), 8295.
- [16] Qayyum, A., Ijaz, A., Usama, M., et al. (2020). Securing machine learning in the cloud: A systematic review. *Frontiers in Big Data*, 3, 587139.
- [17] Ahmad, S., Mehruz, S., Mebarek-Oudina, F., Beg, J. (2022). Cloud access security broker: A systematic review. *Cluster Computing*, 25(5), 3733–3763.
- [18] Kayode, Y.S., Abiodun, A.I., Misra, S., et al. (2022). Machine learning-based intrusion detection for IoT attacks. *Alexandria Engineering Journal*, 61(12), 9395–9409.
- [19] Majeed, A., Khan, S., Hwang, S.O. (2022). Privacy preservation using clustering-based anonymization. *IEEE Access*, 10, 53066–53097.
- [20] Abushark, Y.B., Hassan, S., Khan, A.I. (2025). AdaBoost SVM-based encryption for IoT-cloud healthcare data. *Sensors*, 25(3), 731.
- [21] Jayaweera, R., Agrawal, H., Karie, N.M. (2025). Federated security for healthcare data in edge-cloud environments. *Sensors*, 25(16), 5108.
- [22] Satpathy, S., Mohapatra, S., Swain, P.K., Paikaray, B.K. (2025). Securing healthcare cloud using machine learning techniques. *International Journal of Internet Manufacturing and Services*, 11(2), 114–131.
- [23] Gupta, S. (2025). Zero-trust AI architecture for healthcare cloud security. *International Journal of Research and Applied Innovations*.
- [24] Ngwenya, T., Ndlovu, B. (2025). Post-quantum cryptography for healthcare data protection. *Journal of Applied Informatics and Computing*.
- [25] Munirathinam, T., Ganapathy, S., Kannan, A. (2020). Privacy-preserved e-healthcare system using deep learning. *Journal of Information Security and Applications*, 39, 3011–3023.
- [26] Liu, Y., et al. (2024). AI-based secure medical image retrieval using deep learning and encryption. *EURASIP Journal on Image and Video Processing*.
- [27] Sharma, S., et al. (2024). Privacy-preserving healthcare analytics using homomorphic encryption and machine learning. *BMC Medical Informatics and Decision Making*.