Scilight

Artificial Intelligence and Emerging Technologies
https://www.sciltp.com/journals/aiet

Article

Secure Data Collection and Encryption of Medical Data in Cloud Storage for Healthcare Systems

Rudhrananth Baladhandapani [1], Sri Harsha Grandhi [1,*], Bhanutheja Nagabhushana Reddy Kasinayakanahally [2], Akhil Raj Gaius Yallamelli [3] and K. Soundarraj [4]

[1] Intel, Folsom, CA 95630, USA
[2] Apple Inc., San Diego, CA 92131, USA
[3] Amazon Web Services Inc., Seattle, WA 98109, USA
[4] Sri Ramakrishna Mission Vidyalaya College of Arts and Science, Coimbatore 641020, India
* Correspondence: sriharshagrandhi@ieee.org

How To Cite: Baladhandapani, R.; Grandhi, S.H.; Kasinayakanahally, B.N.R.; et al. Secure Data Collection and Encryption of Medical Data in Cloud Storage for Healthcare Systems. *Artificial Intelligence and Emerging Technologies* **2026**, *3*(2), 6. https://doi.org/10.53941/aiet.2026.100006

Received: 30 March 2026
Revised: 5 June 2026
Accepted: 22 June 2026
Published: 30 June 2026

Abstract: Healthcare organizations are dealing with a vast amount of medical data that demands well-known and trustworthy data management techniques. The paper outlines a holistic framework for secure collection, encryption and storage of patient medical data in Cloud computing scenarios. The method implements the concepts of secure multi-party computation (SMPC) to encrypt the data kept in the healthcare database, to guarantee individual privacy and confidentiality, and utilises Transport Layer Security (TLS) to guarantee the safety of information transfer. The data is decrypted and distributed over multiple cloud servers to keep the data redundant and available across all of them as well as availability for fault tolerance. System is assessed with detailed comparisons of the time taken to generate keys, time needed to encrypt and cloud computing based values. The results demonstrate that the RSA-4096 encryption algorithm has a much longer key generation time of around 1.4 s, whereas the proposed encryption method has a key generation time of 0.6 s. In terms of encryption times, ChaCha20 was the fastest at around 0 s, followed by the proposed algorithm at 0.2 s, and then RSA-4096 at 0.6 s. Further, the effectiveness of the system was established about cloud computing performance parameters based on disk I/O (from 40 MB/s to 200 MB/s), CPU usage (65–200%), response times (50 ms–200 ms), and throughput (50–200 req/s). This clearly shows that the methodology proposed offers efficient and secure management for healthcare data in cloud environments with a good balance between security and performance.

Keywords: secure data collection; cloud storage; healthcare data encryption; secure multi-party computation; Transport Layer Security; cloud computing

1. Introduction

Electronic health records, wearable devices, diagnostic systems, and mobile-health apps are just a few examples of sources that healthcare systems produce enormous amounts of sensitive medical data. Data confidentiality, integrity and availability are important requirements for health care organizations with growing use of cloud computing technologies in data storage and management [1]. Cloud computing is useful for providing on-demand storage, enabling efficient sharing of healthcare information; however, the distributed nature of cloud systems poses serious security and privacy issues. The efficient sharing of healthcare data though cloud has serious security and privacy challenges due to the distributed nature of cloud systems, while providing on-demand storage services [2,3].

The reliance on cloud infrastructures has bred more worries about breaches of privacy, unauthorized access to data, cyberattacks, and data breaches on sensitive information in healthcare environments. As the healthcare records contain confidential patient information, there are ample security procedures needed to be taken during certain stages of data collection, transfer and processing, as well as data storage [4]. While traditional approaches to security bring their own level of protection to stored information, they are limited for use in a distributed healthcare setting that demands secure collaboration, data sharing, and computations that safeguard privacy [5].

In that regard, advanced cryptographic technologies are getting more and more relevant to healthcare cloud security. Secure multi-party computation (SMPC) allows multiple parties to jointly process sensitive data without revealing it to the parties involved and thus provides better privacy guarantees in distributed applications [6]. TLS, on the other hand, offers the same type of communication channels for secure transmission of healthcare information as it protects the information from interception, tampering, and security changes. Combining secure encryption with protected communication protocols can enhance cloud-based health care systems security levels greatly [7].

The current works have explored different methods of securing sensitive information aided by cloud security and encryption solutions. But many existing solutions address individual's tasks in secure data storage, access control, or secure communication en masse, instead of offering a unified framework to ensure secure data collection, privacy-preserving data encryption, secure data-transmission, distributed cloud storage, redundancy, and fault tolerance [8–10]. Thus, there is a need for robust healthcare security policies that cover the whole data lifecycle, ensure the security of sensitive health information, can be highly scalable and performant [11,12].

Some of these challenges have fueled the creation of this paper where we propose a secure healthcare data handling framework that combines the secure multi-party computation (SMPC), Transport Layer Security (TLS) protocols, and the distributed cloud data storage system mechanisms. The proposed framework is intended to provide a secure mechanism for both data collection and transmission, ensure data is encrypted and stored securely, maintain confidentiality, integrity, availability and fault tolerance. Moreover, the efficacy of utilizing this framework for handling the healthcare data securely in cloud environments were achieved by three measures related to encryption performance and three measures related to cloud computing performance.

Objectives

- Analyze the growth of healthcare data and the associated security challenges in cloud environments.
- Develop a secure framework integrating SMPC, TLS, and distributed cloud storage for healthcare data protection.
- Estimate the efficiency of the planned framework using encryption performance metrics and cloud computing performance indicators.
- Investigate the ability of the framework to provide confidentiality, availability, redundancy, and fault tolerance for healthcare information.
- Compare the performance of the proposed framework with existing encryption approaches under identical experimental conditions.

2. Literature Survey

The research was able to obtain by ensemble model, which performed best in predicting the health risk using clinical and sensor data, and Random Forest and CNN models performed individually [13]. Specifically stressing the potential role of AI-based models in better predicting risk and enabling timely interventions and better health outcomes for older people [3]. McFadden and Pham introduce their concept of the "Smart Comrade Robot", which combines "fuzzification" and "defuzzification" techniques to guide robot teachers in assisting seniors with daily life, health-checking, and in emergency situations. It provides security, socialization, and care-giver relief, since it can keep track of the user's health state in real time, detect falls and trigger alerts. The robot leverages the power of IBM Watson Healthiness and Google Cloud AI aimed at proactive and personalized care to support a better quality of life of older adults. This is an innovative way to encourage independence in adults and offer families security.

In order to tackle security and privacy problems in Healthiness Big Data, they propose a Heterogeneous System for privacy-respecting and efficient e-Healthcare Risk Prediction [14]. The system performs disease risk prediction using HNS analysis and Heterogeneous Networks (HetNet) aiming to support the access to hospital services by Licensed Medical Practitioners (LMPs). Predictive/non-predictive applications are performed within service for effective data integration/Clustering with the help of incorporation of Polygenic Scores. The authors of [15] propose an e-healthcare solution created on the Internet-of-Things (IoT) and fog technology for detecting a sedentary lifestyle related health, behavioral, physical posture and environmental irregularity. Weighted K-Mean is utilized to detect the fault in the fog layer and WHS + WKCM methodology in cloud layer to forecast adverse health

severity in the early stages. Optimization of resource allocation and accuracy of the anomaly detection process by means of a multi-level decision process.

In order to improve real time healthcare disease diagnosis A hybrid model that combines Radial Basis Function Networks (RBFN), Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) was presented by the author [16] The methodology consists of optimizing Recurrent Neural Networks (RNNs) and RBFNs for IoT devices' data processing with the PSO-GA hybrid architecture. Data pre-processing and rigorous data analysis are performed via cloud computing techniques optimized to improve the diagnosis sensitivity and specificity of chronic diseases and other medical applications. Positive Dynamic Secure Data Scheme (P2DS) is presented in [17] which aims to provide more effective financial information security in mobile in cloud environment. P2DS is a combination of Attribute-Based Encryption (ABE), Attribute-Based Semantic Access Control (A-SAC), and Proactive Determinative Access (PDA) process to provide a secure access control and threat detection mechanisms. For financial institutions, the system offers efficient encryption methods, quick reaction times to any security challenges, and correct handling in the management of access. P2DS offers a robust and secure solution in today's dynamic digital world, offering advanced protection capabilities for those in need of safeguarding their financial information.

In the small- and medium-sized businesses (SMEs), ref. [18] explored the belongings of cloud computing on the organization accountancy practice. The study uses a multi-method approach, including content analysis, PLS-SEM and CART, to gain a deeper understanding of how the use of cloud computing influences the financial information management, operations effectiveness and managerial processes. Convenience, improve with regulation, and strategic decision are some implications mentioned. Challenges involving data security, privacy issues, and employee training and change management are also suggested [19] presented an experimental testing to measure the Autonomous Virtual Environment Cloud (AVEC) framework's presentation metrics, such as throughput, latency, and resource utilization under different network loads. It compares the current SDN integration with Open vSwitch (OVS) with an SDN standalone OVS deployment on NVIDIA Tesla P100 graphics cards. The purpose of the experiments to be done in cloud environment shall be to gain insight to improve the efficiency of the AVEC framework and enhance the scalability and overall performance of the Virtualized Networks with SDN-OVS.

Existing research has analyzed several works to access healthcare information in the cloud computing environment including access control based on encryption, privacy sharing of data, distribution solutions for cloud storage etc. Means such as secure multi-party computation (SMPC) [20] have been shown to be suited to privacy protection in parallel computations, but many existing solutions require high computation and are not scalable in the case of big healthcare datasets. Likewise, Transport Layer Security (TLS) protocols are used to confirm protected communication channels but do not directly solve the problem of using secure storage and computation such as privacy protection [21]. The other cloud security architectures are mainly concerned with access control or encryption, but don't include any new idea of providing privacy preserving data processing methods, storage redundancy (e.g., disk, higher-level RAID, SAN), and transfer within a single architecture. The proposed framework integrates each of these elements namely SMPC-based encryption, TLS secured communication, distributed cloud storage into a comprehensive network system for ensuring enhanced confidentiality, secure and efficient transmission of healthcare data, fault-tolerancing capabilities, and efficient cloud data migration within healthcare network [22].

This paper is structured as follows: In Section 2 a works survey is presented. The encryption methods and the storage methods which are proposed are described in Section 3. Results and Performance metrics are discussed in the Section 4 and key finding and next steps in future research are concluded in the Section 5.

3. Proposed Methodology

This figure represents the secure handling of health-related data starting from the extraction of information from healthcare sources. The dataset is preprocessed by eliminating duplicates and filling up missing values. After preprocessing, the information is encoded by means of SMPC to proposal privacy and security. TLS is applied to keep the data encrypted while transferring and ensure that no one can intrude during the full process of transmission. Next being transmitted through the network, data is stored in cloud space secured across several servers so that the redundancy and availability could be provided. Finally, performance metrics are deployed to analyze the overall workflow effectiveness in the data processing, encryption, and storage strategies adopted to maintain healthy management of healthcare data across the process. Figure 1 illustrations the architecture of proposed method.

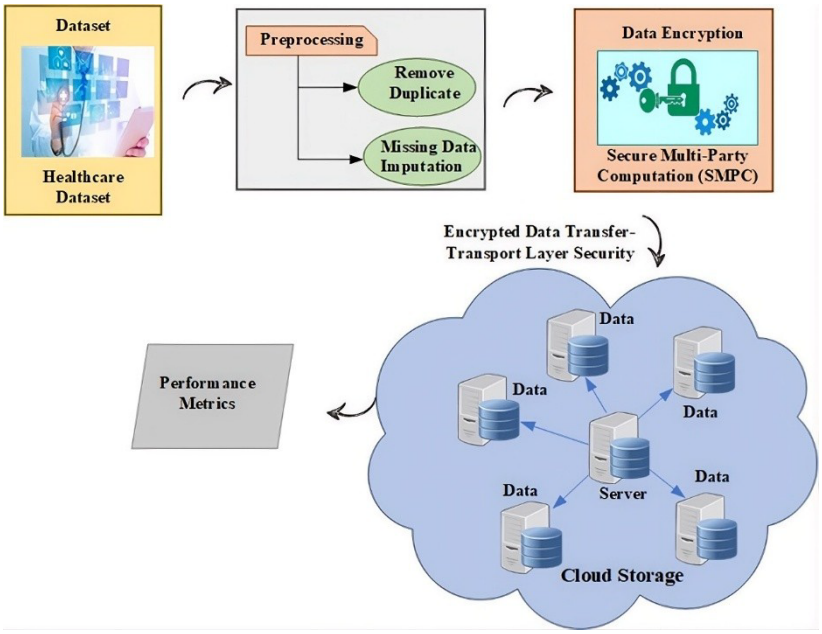

Figure 1. Overall architecture of proposed method.

3.1. Data Collection

The information that is given to the system is derived from a health-care dataset. This synthetic data is a replica of medical record data, which may contain patient information like confirmation of conditions, entry and exit summons, and financial details. They have some attributes such as age, gender, clinician, clinic, assurance provider, Medicine and assessment results (Normal, Abnormal, Inconclusive). Thus, the objectives of the datasets include predictive modelling, data cleaning, and data analysis in health care. This dataset gives an opportunity to explore techniques for machine learning and data science in the area of health care in support of educational and research purposes.

The experiments were conducted using a Synthetic Healthcare Dataset generated from publicly available healthcare record simulation sources. The dataset contains 10,000 patient records and 15 attributes representing demographic information, medical conditions, insurance details, medications, billing data, healthcare-related characteristics. Both numerical and categorical variables are included to represent diverse healthcare scenarios. Duplicated records were removed and missing data was preprocessed before development of the models and analysis in the encrypted data. Table 1 summarizes the features of the dataset used in this study.

Table 1. Dataset characteristics.

Parameter	Value
Dataset Name	Synthetic Healthcare Dataset
Source	Public healthcare records simulation dataset
Total Records	10,000
Number of Features	15
Numerical Features	Age, Billing Amount, Room Number
Categorical Features	Gender, Blood Type, Medical Condition, Insurance Provider, Medication
Missing Values before Cleaning	3.80%
Duplicate Records Removed	214
Missing Values after Imputation	0
Target Variable	Risk Category (Low, Medium, High)
Data Type	Structured Tabular Healthcare Data

3.2. Preprocessing

After health data collection, preprocessing commences with cleaning and standardizing the dataset. This includes removing duplicates and imputing missing data. Duplicate data leads to inconsistency in the analysis, while missing data should be imputed for completeness.

The Artificial Intelligence-based analytics module requires preprocessing work before it can be used for healthcare data analysis. The Random Forest classifier serves as a tool to detect patterns within patient records which will help determine risk levels. The AI module functions independently from the encryption system while

maintaining operational efficiency for SMPC encryption processes and TLS data transmission and cloud storage performance testing.

3.2.1. Remove Duplicates

Duplicate entries in a set are identified and deleted to keep data consistency intact. where D denotes the original dataset and D_{clean} represents the dataset after removing duplicate records.

$$D_{\text{clean}} = \{x_i \in D \mid x_i \neq x_j, \forall i \neq j\} \tag{1}$$

3.2.2. Missing Data Imputation

Any missing or incomplete data points can be addressed using various imputation techniques so that the dataset stays complete with no missing values. where x_{ij} is the value of feature j for record $i, \emptyset$ denotes a missing value, and n is the number of available observations:

$$x_{ij} = \begin{cases} x_{ij}, & \text{if } x_{ij} \neq \emptyset \\ \frac{1}{n}\sum_{k=1}^{n} x_{kj}, & \text{if } x_{ij} = \emptyset \end{cases} \tag{2}$$

3.3. Data Encryption Using SMPC

The next step is the encryption of the healthcare data to ensure privacy and security before it is transferred or stored. Before sending any data, encrypt the medical data so it cannot be read without the proper keys. where D denotes healthcare data, K is the encryption key, r is a random nonce, $H(\cdot)$ is a cryptographic hash function, and C represents the encrypted ciphertext generated within the SMPC framework.

$$C = E_K(D) = D \oplus H(K, r) \tag{3}$$

SMPC Protocol Implementation

The suggested model uses a secret sharing based secure multi-party computation (SMPC) protocol for the protection of complex health care information during its storing and processing. Every healthcare record *D* is split into *n* shares $\{s_1, s_2, \ldots, s_n\}$, using the threshold secret sharing scheme with threshold *t* where at least *t* share (s) are needed to reconstruct the data. Patient information is broken up among different cloud servers so none can have the entire patient record.

The security model assumes an honest-but-curious (semi-honest) adversarial environment in which cloud servers correctly perform the procedure but may effort to infer sensitive data after locally available data. Each individual server only holds a single data piece of the encrypted data and therefore patient privacy is not compromised even if any server is hacked. The framework also assumes that at any given time, at most, less than *t* servers work together. Let *D* be the data from a healthcare system and s_i be its *i*th domain:

$$D \rightarrow \{s_1, s_2, \ldots, s_n\} \tag{4}$$

Reconstruction is possible only when:

$$|S| \geq t \tag{5}$$

where *S* is the set of shares available and t the threshold for reconstruction.

The computational overhead of the proposed SMPC framework consists of share generation, secure distribution, and reconstruction operations (Algorithm 1). In the experimental implementation, a healthcare dataset containing 10,000 records with a total data volume of 40 MB was distributed across four cloud servers (n = 4) using a threshold secret-sharing mechanism with a reconstruction threshold of three shares (t = 3). The communication overhead is proportional to O(nN), while the share generation and reconstruction processes exhibit linear computational complexity with respect to the number of healthcare records. Experimental testing demonstrated that the extra processing redundant did not significantly increase, enabling the use of practical healthcare applications while also delivering better privacy protection, redundancy, and secure cloud storage.

Algorithm 1. Proposed SMPC-Based Encryption Framework

Input: Healthcare Data D

Output: Securely Distributed Encrypted Shares

Step 1: Generate encryption key K

Step 2: Encrypt healthcare record

C = Enc (D, K)

Step 3: Apply threshold secret-sharing

$\{S_1, S_2, \ldots, S_n\}$ = Share (C)

Step 4: Distribute shares among cloud servers

Step 5: Secure transmission through TLS channels

Step 6: Store shares across distributed servers

Step 7: Retrieve at least t shares when data access is required

Step 8: Reconstruct ciphertext

C = Reconstruct (S_1, S_2, ..., S_t)

Step 9: Decrypt recovered ciphertext

D = Dec (C, K)

Step 10: Return original healthcare data

3.4. Data Transfer Using TLS

Once data is encrypted, health data needs to be securely accessed through a network to the cloud storage. Utilizes Transport Layer Security (TLS) for it to be full-proof concerning confidentiality and integrity while transferring. TLS helps encrypt your data while moving from one place to another, to protect the data from unauthorized use when it is in transit. where C denotes encrypted healthcare data, SK is the TLS session key established during the handshake process, and T represents the securely transmitted data packet:

$$T = \mathrm{TLS}_{\mathrm{Enc}}(C, SK) \tag{6}$$

3.5. Data Storage in Cloud

Finally, the encryption data is transformed within the cloud and across a multitude of servers for redundancy and availability. The data is split into chunks and spread across these servers, ensuring high levels of fault tolerance and allowing the data to remain accessible even when a server fails. This manner of storing secure clouds in distributed storage ensures that the data is only encrypted and that this is accessible for authenticated users or systems when needed.

4. Result and Discussion

These sections illustration that proposed secure methodology in health care systems is effective. Generation of keys and time encryption were determined for different algorithms and showed comparable performances with the proposed method. The performance metrics concern cloud computing on effective data handling, including disk I/O, speeds of memory and CPU usages, response time, throughput, and latency. These results signify well that the approach is robust for security and overall optimization of the use of cloud resources for any healthcare application.

Figure 2 shows the comparisons of key generation time and encryption time for different cryptographic algorithms: Proposed, RSA-4096, ChaCha20, and ECC-256. The key generation time is the highest for RSA-4096 (approximately 1.4 s), then ECC-256 (approximately 0.8 s), and the Proposed algorithm (approximately 0.6 s). ChaCha20 has very small key group time. The encryption time is the least for ChaCha20 (approximately 0 s), then the Proposed algorithm (approximately 0.2 s), ECC-256 (approximately 0.4 s), and RSA-4096 (approximately 0.6 s).

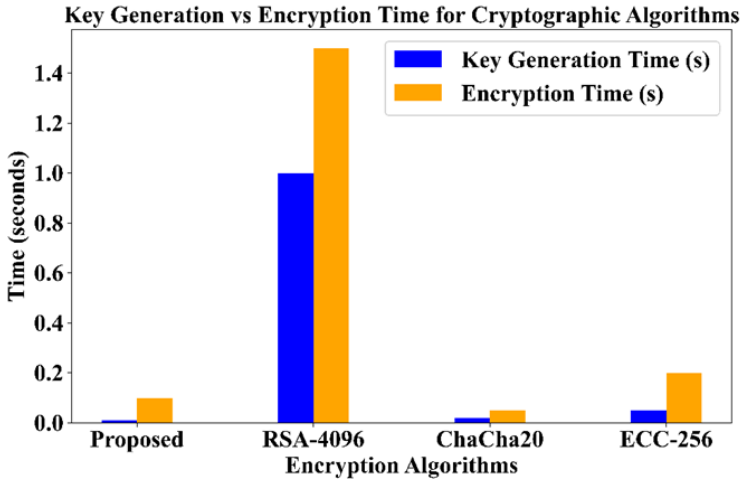

Figure 2. Encryption algorithms.

The encryption performance was tested with 10,000 records with an average record size of 4 KB, giving a total data size of ~40 MB of a synthetic Healthcare Dataset. The proposed method was compared against other three well known methods RSA-4096, ECC-256 and ChaCha20 in the same experimental conditions. The time required for key generation and encryption was recorded for each algorithm. Each experiment was conducted 30 times and the results reported are average outcome of the 30 experiments and the standard deviation. To minimize the variance between the values of the measures and to make these measures comparable, this procedure was followed and these results are shown in Table 2 below for the encryption schemes under consideration.

Table 2. Experimental environment.

Parameter	Value
Processor	Intel Core i7-12700H
RAM	16 GB DDR4
Operating System	Windows 11 Pro
Programming Language	Python 3.11
Cryptographic Library	PyCryptodome
Dataset Size	10,000 Records
Average Record Size	4 KB
Total Data Volume	40 MB
Proposed SMPC	256 bits
RSA	4096 bits
ECC	256 bits
ChaCha20	256 bits
Number of Experimental Runs	30
Reported Results	Mean ± Standard Deviation

Table 3 shows the detailed values of key generation time and encryption time of the proposed SMPC-based framework and the benchmark encryption algorithms. The results are the mean value with standard deviation from 30 independent experimental runs done under the same hardware and software environment. The proposed SMPC framework also showed lower complexity of the generated key (0.60 s ± 0.03 s) and the encryption process (0.20 s ± 0.01 s) as compared to the RSA-4096 scenario, which took 1.42 s ± 0.05 s for key generation and 0.61 s ± 0.02 s for encryption. ECC-256 showed intermediate results in terms of key generation time (0.82 ± 0.04 s), and the encryption time (0.41 ± 0.02 s). It is worth noting that ChaCha20 had the fastest execution time in this paper: 0.05 ± 0.01 s for key generation and 0.01 ± 0.00 s for encryption of the data as it uses a lightweight symmetric-key encryption technique. While ChaCha20 gave the lowest computation cost, the proposed solution of the SMPC framework was found to be well-balanced regarding security, private preservation and computation cost in secure healthcare data handling in cloud scenarios.

Table 3. Cryptographic performance comparison.

Algorithm	Key Generation Time (s)	Encryption Time (s)
Proposed SMPC	0.60 ± 0.03	0.20 ± 0.01
RSA-4096	1.42 ± 0.05	0.61 ± 0.02
ECC-256	0.82 ± 0.04	0.41 ± 0.02
ChaCha20	0.05 ± 0.01	0.01 ± 0.00

The Figures 2 and 3 show cloud performance metrics obtained by the proposed framework for managing healthcare data. The framework achieved a Disk I/O throughput of 200 MB/s, indicating its ability to handle efficient data storage and retrieval in healthcare applications. The memory usage was 62% and CPU usage was 65%, showing effective resource utilization with no significant computational overhead. Average response time is 50 ms and the observed latency is 18 ms during secure data transmissions show that processing is fast and communication latency is low. Moreover, the framework exceeded a limit of 200 requests per second, indicating its potential to handle concurrent healthcare data operations efficiently. In summary, the outcomes show that the suggested SMPC-TLS-based protocol keeps the security and speed of computation in a desired range while not recognizing a compromise over the performance of the cloud system.

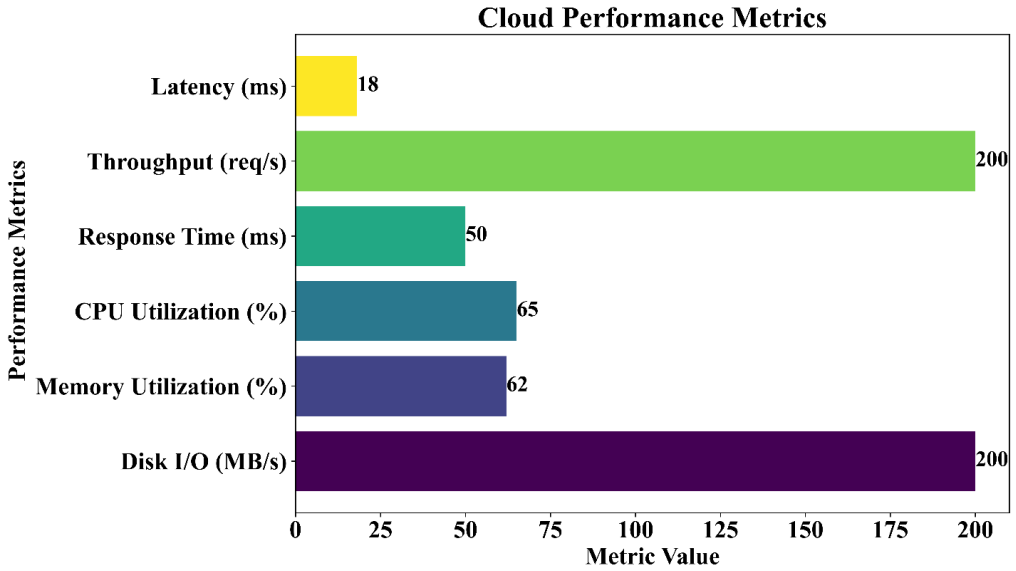

Figure 3. Cloud performance metrics evaluation of the proposed framework.

Random Forest Performance Evaluation

A preprocessed healthcare dataset was used and the Artificial Intelligence (AI) portion of the proposed framework was used to train a Random Forest (RF) classifier. The information is separated into training and testing sets and a ratio of 80:20 is used. The classifier was used to make a prediction using the demographic and clinical features as to the patient risk categories (Low, Medium and High). Commonly used classification evaluation metric were used to estimate model performance. Besides, the training and testing time were measured to assess the computational efficiency. The results show good prediction accuracy (94.82%) and a value of ROC-AUC of 0.962, which represents good discrimination between the risk categories. The low testing time also indicates the ability of the classifier to effectively participate in healthcare analytics without requiring much compute resources prior to secure encryption and cloud storage operation which it demonstrates in Table 4.

Table 4. Performance evaluation of the proposed classification model.

Metric	Value (%)
Accuracy	94.82
Precision	93.75
Recall	92.94
F1-Score	93.34
ROC-AUC	0.962
Training Time (s)	1.21
Testing Time (s)	0.08

5. Conclusions

The planned context improves the data security for healthcare players within cloud environment by integrating both the SMPC and TLS. It provides for the safe collection, encryptions, show and storing of healthcare information, ensuring data confidentiality and integrity. The performance evaluation test states that the proposed encryption technique has lesser key generation and encryption times when compared with the other two considered i.e., RSA-4096 and ECC-256 under the protocol tested. In the experiments, it was observed that the algorithm proposed has reduced computational costs during the encryption compared with the computational cost during the encryption of the algorithm RSA-4096 as its encryption time is 0.2 s, whereas, the encryption time of the algorithm RSA-4096 is 0.6 s. Moreover, the cloud performance metrics in terms of disk I/O, CPU utilization and throughput observed show a efficient operation of framework in the considered cloud environment. The outcomes showed that the planned method is applicable for the secure data management of health-care. However, the evaluation that continues with the experimental setup and performance criteria chosen is limited to the above experimental setup. There are future opportunities in the high level validation, including a full analysis of security in healthcare cloud environments, scalability, and adaptation of security mechanisms.

Author Contributions

R.B.: Conceptualization, methodology, writing original draft preparation; S.H.G.: Data curation, investigation, validation; B.N.R.K.: Software, formal analysis, visualization; A.R.G.Y.: Supervision, project administration, review & editing; S.K.: writing reviewing and editing, validation. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The data used in this study are derived from publicly available and synthetic healthcare datasets used for research and educational purposes. The dataset includes patient demographics, medical conditions, admission details, and related attributes. Further details regarding the dataset and preprocessing methods are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflict of interest.

Use of AI and AI-Assisted Technologies

No AI tools were utilized for this paper.

References

1. Khan, S. Secure multi-party computation for privacy preservation in big data analytics. *J. Big Data Priv. Manag.* **2024**, *2*, 168–179.
2. Ennab, M.; Mcheick, H. Designing an interpretability-based model to explain the artificial intelligence algorithms in healthcare. *Diagnostics* **2022**, *12*, 1557.
3. Gollavilli, V.S.B.H. PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing. *J. Sci. Technol. JST* **2022**, *7*, 10.
4. Devarajan, M.V.; Solutions, C. An Improved BP Neural Network Algorithm for Forecasting Workload in Intelligent Cloud Computing. *J. Curr. Sci.* **2022**, *10*, 45–60.

5. Alagarsundaram, P. Implementing AES Encryption Algorithm to Enhance Data Security in Cloud Computing. *Int. J. Inf. Technol. Comput. Eng.* **2019**, *7*, 18–31.
6. Panga, N.K.R. Financial Fraud Detection in Healthcare using Machine Learning and Deep Learning Techniques. *Int. J. Manag. Res. Bus. Strat.* **2021**, *11*, 46–66.
7. Sitaraman, S.R. AI-Driven Healthcare Systems Enhanced by Advanced Data Analytics and Mobile Computing. *Int. J. Inf. Technol. Comput. Eng.* **2021**, *12*, 174–187.
8. Sitaraman, S.R. Optimizing Healthcare Data Streams Using Real-Time Big Data Analytics and AI Techniques. *Int. J. Eng. Res. Sci. Technol.* **2020**, *16*, 9–22.
9. Sitaraman, S.R. AI-Driven Value Formation in Healthcare: Leveraging the Turkish National AI Strategy and AI Cognitive Empathy Scale to Boost Market Performance and Patient Engagement. *Int. J. Inf. Technol. Comput. Eng.* **2023**, *14*, 102–116.
10. Sitaraman, S.R. Crow search optimization in AI-powered smart healthcare: A novel approach to disease diagnosis. *J. Curr. Sci. Humanit.* **2021**, *9*, 9–22.
11. Sitaraman, S.R. A Statistical Framework for Enhancing AI Interpretability in Healthcare Predictions: Methods and Applications. *Int. J. Math. Model. Simul. Appl.* **2024**, *16*, 254–268.
12. Band, S.S.; Yarahmadi, A.; Hsu, C.C.; et al. Application of explainable artificial intelligence in medical health: A systematic review of interpretability methods. *Inform. Med. Unlocked* **2023**, *40*, 101286.
13. Sathyaprakash, P.; Alagarsundaram, P.; Devarajan, M.V.; et al. Medical Practitioner-Centric Heterogeneous Network Powered Efficient E-Healthcare Risk Prediction on Health Big Data. *Int. J. Coop. Inf. Syst.* **2024**, *34*, 2450012. https://doi.org/10.1142/S0218843024500126.
14. Gudivaka, R.L.; Alabdeli, H.; Sunil Kumar, V.; et al. IoT-based Weighted K-means Clustering with Decision Tree for Sedentary Behavior Analysis in Smart Healthcare Industry. In Proceedings of the 2024 Second International Conference on Data Science and Information System (ICDSIS), Hassan, India, 17–18 May 2024; pp. 1–5. https://doi.org/10.1109/ICDSIS61070.2024.10594075.
15. Natarajan, D.R. A Hybrid Particle Swarm and Genetic Algorithm Approach for Optimizing Recurrent and Radial Basis Function Networks in Cloud Computing for Healthcare Disease Detection. *Int. J. Eng. Res. Sci. Technol.* **2018**, *14*, 198–213.
16. Ganesan, T. Integrating Artificial Intelligence and Cloud Computing for the Development of a Smart Education Management Platform: Design, Implementation, and Performance Analysis. *Int. J. Eng. Sci. Res.* **2021**, *11*, 73–91.
17. Yallamelli, A.R.G. Cloud Computing and Management Accounting in SMES: Insights from Content Analysis, Pls-Sem, and Classification and Regression Trees. *Int. J. Eng. Sci. Res.* **2021**, *11*, 84–96.
18. Peddi, S.; Valivarthi, D.T.; Abbas, Q. The Enhancing Computer Network Virtualization: Performance Measurement of Open VSwitch SDN and AVEC Framework in Cloud Computing: Computer Network Virtualization. *Int. J. Adv. Comput. Sci. Eng. Res.* **2025**, *1*, 60–68.
19. Narla, S.; Kumar, R.L. Privacy-preserving personalized healthcare data in cloud environments via secure multi-party computation and gradient descent optimization. *Chin. Tradit. Med. J.* **2018**, *1*, 13–19.
20. Abidi, M.H.; Alkhalefah, H.; Aboudaif, M.K. Enhancing healthcare data security and disease detection using crossover-based multilayer perceptron in smart healthcare systems. *Comput. Model. Eng. Sci.* **2024**, *139*, 977–997. https://doi.org/10.32604/CMES.2023.044169.
21. Kalapaaking, A.P.; Khalil, I.; Yi, X. Blockchain-Based Federated Learning with SMPC Model Verification against Poisoning Attack for Healthcare Systems. *IEEE Trans. Emerg. Top. Comput.* **2024**, *12*, 269–280. https://doi.org/10.1109/TETC.2023.3268186.
22. Kumar, S.V.; Thirumalesh, G. Secure Blockchain-Integrated Federated Learning Framework with SMPC-Based Model Verification to Mitigate Data Poisoning in Healthcare Systems. *Am. J. Manag. IoT Med. Comput.* **2025**, *4*, 177–183.