ISSN: 2093-5374 / E-ISSN: 2093-5382

A Secure and Efficient Blockchain-Based Healthcare Framework Using Feature-Gated CNN and Transaction-Structured Selective Encryption

D. Bhanu Sravanthi[1], Dr.M. Pounambal[2*], Dr.P. Venkata Krishna[3], and Dr.V. Saritha[4]

[1]Research Scholar, Department of Computer Science and Engineering, Sri Padmavati Mahila Visvavidyalayam, Tirupati, India. dsravanthi.bs@gmail.com, https://orcid.org/0009-0000-1745-2220

[2*]Professor, School of Computer Science and Information Systems, Vellore Institute of Technology, Vellore, India. mpounambal@vit.ac.in, https://orcid.org/0000-0002-1811-4722

[3]Professor, Department of Computer Science, Sri Padmavati Mahila Visvavidyalayam, Tirupati, India. parimalavk@gmail.com, https://orcid.org/0000-0001-8138-5878

[4]Professor, Department of Computer Science and Engineering, Sri Padmavati Mahila Visvavidyalayam, Tirupati, India. vsaritha@spmvv.ac.in, https://orcid.org/0000-0002-9658-3663

Received: February 12, 2026; Revised: March 18, 2026; Accepted: May 06, 2026; Published: June 30, 2026

Abstract

The article focuses on the issue of safe healthcare data management within decentralized systems, specifically, blockchain-based ones. Conventional blockchain-based systems have great concerns regarding exposure of privacy, cost of storage and cryptographic overhead of storing confidential medical records. The proposed work is an integrated system that integrates both Feature-Gated Convolutional Neural Networks (FG-CNN) to predict the disease and Transaction-Structured Selective Encryption (TSSE) to encrypt data efficiently. The FG-CNN model is also trained on the UCI Heart Disease dataset, where it also does binary classification to predict heart disease and gives the sensitivity score of each feature. Selective encryption with these sensitivity scores is then applied to minimize the amount of unwarranted encryption overhead whereby only privacy sensitive data fields are encrypted. The encrypted data will be stored in off-chain MongoDB database, with blockchain-backed integrity proofs stored on Ethereum. The experimental methodology proves the efficiency of the TSSE framework in terms of minimizing the encryption time by 63%, decryption time by 61%, and blockchain storage overhead by 88%. Also, the use of blockchain gas is minimized by 55% which is a massive enhancement as compared to the conventional full-data encryption systems. The system also lowers privacy risks by 75%, although it has high privacy guarantees. The NIST statistical randomness tests confirm the secure and random nature of the encrypted data, indicating the robustness of the proposed encryption approach. Nevertheless, the article does not include clear quantitative forecasts of classification accuracy, precision, recall, and F1-score of the FG-CNN model, which may offer a more detailed evaluation of its performance in diagnosing the disease.

Keywords: Healthcare Data Security, Blockchain Technology, Feature-Gated Convolutional Neural Network, Transaction-Structured Selective Encryption, MongoDB, Ethereum Blockchain, Infura Gateway.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 2 (June-2026), pp. 213-229. DOI: *10.58346/JOWUA.2026.I2.012*

*Corresponding author: Professor, School of Computer Science and Information Systems, Vellore Institute of Technology, Vellore, India.

1 Introduction

The rapid digitalization of healthcare systems has resulted in an unprecedented growth in the amount of medical data produced from clinical procedures, diagnostic tests, and electronic health records (Cheikhrouhou et al., 2025). Although this data is essential for facilitating timely diagnosis and clinical decision-making, its sensitive nature has raised significant concerns regarding privacy, security, and unauthorized access (Adeniyi et al., 2025). The centralized healthcare data management system architecture is increasingly susceptible to data breaches, single-point failures, and trust-related problems, especially when patient data is shared among multiple healthcare institutions and stakeholders (Singh et al., 2025). Blockchain technology has been identified as a promising approach to overcome trust and integrity-related challenges in healthcare data management systems because of its decentralized architecture, blockchain structure, and transparent transaction verification processes (Olaymi, 2025). Blockchain technology eliminates the need for a central authority in data exchange among mutually untrusted parties (Haddad et al., 2024). Nevertheless, despite its benefits, the direct storage of healthcare data in blockchain networks is not feasible. Medical records contain highly sensitive and voluminous data, leading to risks of privacy exposure, storage capacity, and high computational costs associated with full encryption and on-chain storage (Ravichandran et al., 2025).

In parallel, the development of deep learning has greatly improved the accuracy of automated disease diagnosis systems (Kumar et al., 2025). Neural network models have shown excellent learning ability in processing complex relationships between clinical data, which can be used for precise disease prediction, including cardiovascular diseases (Sadr et al., 2024). However, existing diagnostic models are mostly concerned with improving predictive accuracy, and the secure processing, storage, and verification of diagnostic information in a decentralized system have been less emphasized (Tabassum et al., 2025). In blockchain-based healthcare systems, diagnostic information needs to be protected not only from external attacks but also from unnecessary disclosure and inefficient cryptographic processing (Kumar et al., 2025). To address the trade-off between intelligent diagnosis and secure decentralized storage, a new approach called selective encryption has attracted increasing attention as an alternative to traditional full-data encryption (Popoola et al., 2024). By encrypting only, the privacy-critical data fields instead of the entire data, selective encryption can greatly lower the computational overhead and storage costs while preserving data confidentiality (Chakravarthy et al., 2025). Nevertheless, the decision to encrypt specific data elements is often made according to predefined rules or static policies, which may not accurately capture the dynamic sensitivity of diagnostic information produced by intelligent models (Lee et al., 2025).

Inspired by these issues, this paper proposes an integrated framework for managing healthcare data that combines a Feature-Gated Convolutional Neural Network (FG-CNN) with a Transaction-Structured Selective Encryption (TSSE) system. The FG-CNN model is developed to classify patients into binary heart disease categories based on tabular clinical features and to learn the importance of individual features adaptively using a feature-gating approach (Shobayo & Saatchi, 2025). Besides disease prediction, the model provides confidence and sensitivity measures to quantify the reliability and privacy importance of disease prediction results (Chen et al., 2025). These measures are further used to control the selective encryption process in the TSSE system. The proposed TSSE system encodes disease prediction results into blockchain-compatible transactions and uses field-level sensitivity analysis to encrypt only the privacy-sensitive parts of the transactions (Mhiri et al., 2024). For efficient scalability, the encrypted healthcare data is stored in an off-chain database, and the integrity proofs and transaction references are stored in the Ethereum blockchain using a Web 3.0 access layer (Mole & Shaji, 2024).

The proposed framework follows standardized cryptographic protocols and uses blockchain-level privacy analysis to provide strong security guarantees (Li et al., 2025).

The main contributions of this work can be summarized as follows:

1. A diagnostic model based on FG-CNN that can directly process tabular clinical data and learn the importance of features via adaptive gating.
2. A TSSE framework that supports privacy-aware selective encryption based on model-driven sensitivity information.
3. A hybrid storage system that integrates off-chain encrypted data storage and blockchain-based integrity verification.
4. A comprehensive evaluation that shows efficiency improvements in encryption latency, storage cost, and blockchain gas consumption while maintaining confidentiality and integrity.

Through the integration of intelligent diagnosis, selective encryption, and blockchain-based verification, the proposed framework offers a practical and efficient solution for the secure management of healthcare data within a decentralized setting.

The paper is structured in the following way: Section 1 presents the problem of secure healthcare data management, the challenges of blockchain technology and the methods of deep learning are also discussed. It also describes the major reasons why these approaches should be integrated. Section 2 gives an in-depth literature review of the available solutions, the gaps and limitations of the current study on healthcare data security and privacy using blockchain and AI. Section 3 outlines the suggested methodology, which includes the combination of Feature-Gated Convolutional Neural Networks (FG-CNN) to predict diseases and the use of Transaction-Structured Selective Encryption (TSSE) to encrypt data in an efficient way. Section 4 explains the experimental design, data collection, data preprocessing, and model performance assessment of the proposed model, and finally an analysis of the results. Section 5 covers the blockchain security and efficiency analysis, which shows the increase in encryption time, cost of storage and the usage of blockchain resources. Section 6 is the conclusion of the paper that summarizes the findings and proposes further research directions, one of which is the possibility of multi-disease prediction and an increased scale of health care applications.

2 Literature Survey

The literature review outlines different ways of combining blockchain and AI to enhance healthcare data security and management. The papers in question underscore the major progress in the field of ensuring the safety of healthcare data and tackling some of its main obstacles, including computational overhead and scalability, as well as privacy issues.

Chakravarthy et al., (2025) proposed a hybrid hashing blockchain framework to enhance confidentiality and access control in Electronic Health Records (EHR) systems. This framework effectively improves the security of EHRs by leveraging blockchain technology. However, the system faces challenges related to scalability and real-time application, which limits its broader implementation.

Lee et al., (2025) conducted a survey on secure healthcare data processing using homomorphic encryption. They provided a comprehensive analysis of encryption attacks and defenses in healthcare data systems. However, the paper lacks a detailed practical framework or case study examples, limiting its real-world applicability.

Shobayo & Saatchi, (2025) explored developments in deep learning neural networks for medical image analysis, advancing AI techniques for medical image classification and interpretation. However,

their approach lacks integration with real-time clinical decision-making systems, hindering its practical application in dynamic healthcare settings.

Chen et al., (2025) reviewed CNN-based methods for medical image classification, highlighting various CNN techniques for medical applications. While the review covers a broad range of methods, it does not address specific challenges encountered in real-world medical applications, limiting its practical guidance.

Mhiri et al., (2024) proposed proxy re-encryption for enhanced data security in healthcare, offering a practical implementation of proxy re-encryption in healthcare data security. However, the method struggles with scalability, particularly for large datasets or multiple healthcare institutions, limiting its effectiveness in large-scale applications.

Mole & Shaji (2024) introduced Ethereum blockchain for securing electronic health records, streamlining patient management and ensuring secure storage using Ethereum blockchain. Despite its benefits, the system is limited to Ethereum and lacks interoperability with other blockchain platforms, limiting its flexibility.

Li et al., (2025) provided a systematic review on privacy preservation in blockchain-based healthcare data sharing. Their review discusses various privacy preservation techniques in blockchain healthcare systems but is limited by its focus on theoretical aspects and lacks practical applications in large-scale healthcare systems.

Bhuvaneshwari et al., (2025) presented an AI-enabled deep learning framework for enhancing security in blockchain transactions. Their framework utilizes AI-based deep learning to improve blockchain transaction security. However, it suffers from high energy consumption and computational complexity, making it difficult to scale for large systems.

Galety et al., (2025) proposed a blockchain-based solution for AI-driven healthcare infrastructures, focusing on secure and effective data organization using blockchain principles. The solution integrates AI with blockchain to enhance data security. However, its applicability to large-scale healthcare infrastructures remains untested, posing a challenge for real-world implementation.

Altogether, the literature indicates that there is a great improvement in terms of the integration of blockchain and AI in safe healthcare data management, and the most important improvements are in the areas of privacy protection, disease prediction accuracy, and blockchain efficiency. Nonetheless, issues like scalability, computation overheads and latency are still critical areas of interest of prospective research and enhancements.

The table 1 provides a brief overview of various methods integrating blockchain and AI for healthcare data security. It also emphasizes the major successes and shortcomings of both methods, such as encryption progress, disease forecasts, and data control. Although such approaches provide some benefits in terms of privacy, security, and efficiency, issues like scalability, real-time use, high computational prices, and system integration with other systems are still common in numerous studies. The findings highlight the potential of blockchain and AI in healthcare, as well as indicate the necessity to further optimize them and validate them on a scale.

Analyzing literature, it becomes evident that there is an increasing trend of combining blockchain and AI to improve the security of health care data, and numerous researchers present positive outcomes of data protection and diagnosis. Although blockchain is a decentralized storage and privacy solution, issues of scalability, real-time implementation, and high computing costs still exist. The AI models such as CNNs demonstrate high diagnostic abilities, yet when integrated with blockchain, complexities are

introduced, including latency and resource consumption. In spite of these developments, more research is required to overcome these drawbacks especially in the large-scale, real-time healthcare systems.

Table 1: Summary for the related works

Author(s)	Proposed Method	Key Achievement	Limitation
Chakravarthy et al., (2025)	Hybrid hashing blockchain framework for enhancing confidentiality and access control in EHR systems	Enhanced confidentiality and access control for EHR systems using blockchain	Limited scalability and real-time application challenges.
Lee et al., (2025)	Survey on secure healthcare data processing using homomorphic encryption	Comprehensive analysis of encryption attacks and defenses in healthcare data	Does not provide a detailed practical framework or case study examples.
Shobayo & Saatchi, (2025)	Developments in deep learning neural networks for medical image analysis	Advances in AI for medical image classification and interpretation	Lack of integration with real-time clinical decision-making systems.
Chen et al., (2025)	Review of CNN-based methods for medical image classification	Review of CNN techniques in medical image classification	Does not delve into specific challenges in real-world medical applications.
Mhiri et al., (2024)	Proxy re-encryption for enhanced data security in healthcare	Practical implementation of proxy re-encryption for healthcare data security	Lack of scalability for large datasets or multiple healthcare institutions.
Mole & Shaji, (2024)	Ethereum blockchain for securing electronic health records	Streamlined patient management and secure storage using Ethereum blockchain	Limited to Ethereum, and lacks interoperability with other blockchain platforms.
Li et al., (2025)	Privacy preservation in blockchain-based healthcare data sharing	Systematic review on privacy preservation in blockchain healthcare systems	Limited practical applications in large-scale healthcare systems.
Bhuvaneshwari et al., (2025)	AI-enabled deep learning framework for security enhancement in blockchain transactions	Enhanced security in blockchain transactions through AI-based deep learning	High energy consumption and computational complexity.
Galety et al., (2025)	Blockchain principles in AI-based healthcare 6.0 infrastructures	Secure and effective data organization using AI and blockchain	Applicability to large-scale healthcare infrastructures remains untested.

3 Proposed Methodology

The figure 1 introduces the proposed secure framework for managing healthcare data by integrating intelligent disease prediction with privacy-preserving blockchain storage. The proposed framework is a combination of a Feature-Gated Convolutional Neural Network (FG-CNN) for heart disease prediction and a Transaction-Structured Selective Encryption (TSSE) scheme for secure and efficient handling of the prediction results.

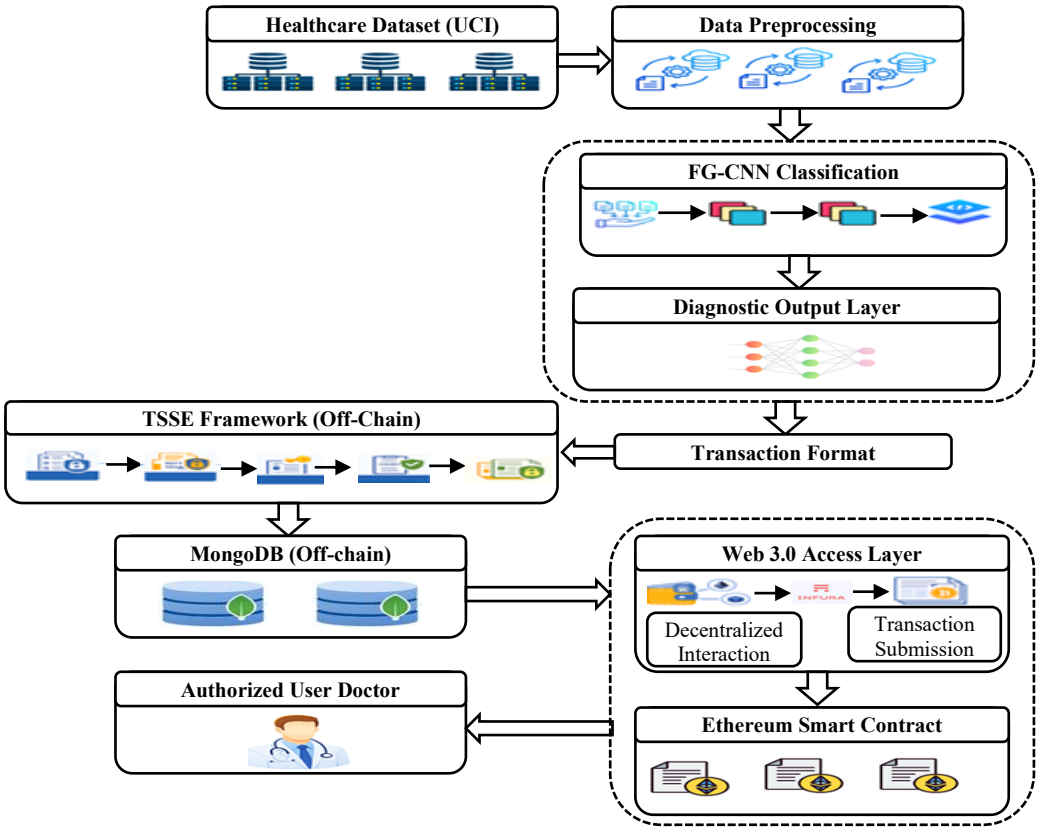

Figure 1: Overall architecture for the proposed system

System Overview

Dataset Collection

The proposed system uses the UCI Heart Disease dataset, which is a popular benchmark dataset for cardiovascular disease analysis. The UCI Heart Disease dataset consists of clinical records gathered from actual patient examinations and has various subsets gathered from different medical institutions. For this research, the Cleveland dataset is chosen because of its completeness and popularity in other related studies. The Cleveland data set consists of 303 patient data, and each data is described by 13 significant input parameters such as age, blood pressure, cholesterol level, electrocardiographic readings, and exercise-related parameters, and one target attribute to describe the heart disease status of patients. Cleveland data set is a good data set to test the efficiency of computer-aided heart disease prediction models.

Dataset Preprocessing

Before training the model, preprocessing of the collected clinical data takes place to achieve consistency and efficiency in learning. The impractical data, such as the details of the patients, are removed to avoid bias and violation of data privacy. The categorical data are converted to numerical data by applying appropriate encoding, and the numerical data are normalized to a uniform scale to facilitate gradient-based learning. The original diagnosis attribute is changed to a binary target output, where zero indicates the absence of heart disease and values greater than zero represent the presence of heart disease.

To address the problem of class imbalance in the dataset, the Synthetic Minority Over-sampling Technique (SMOTE) is used for the training dataset. SMOTE creates artificial samples of the minority class through feature space interpolation, leading to a balanced dataset without replicating any actual samples. The preprocessed dataset is finally formatted as normalized tabular data and rearranged for one-dimensional convolution to facilitate efficient feature-level learning while maintaining attribute relationships.

Feature-Gated Convolutional Neural Network (FG-CNN)

The proposed FG-CNN is expected to perform binary classification to determine the existence or absence of heart disease. A one-dimensional convolution layer is employed to determine feature-level patterns in the data. To enhance robustness and explainability, a feature-gating layer is incorporated after the convolution layer. The feature-gating layer is responsible for learning adaptive importance weights for the activation of individual features, which helps to determine key attributes for diagnosis while suppressing irrelevant features. The FG-CNN makes a binary prediction for disease and a confidence measure based on the sigmoid activation function of the output layer. Sensitivity scores are also calculated based on the gated feature activations, indicating the relative importance of features to the prediction. That the scores are critical in determining selective encryption in the security layer.

Let the normalized tabular input be represented as:

$$X = [x_1, x_2, \dots, x_n] \quad (1)$$

Where n denotes the number of clinical attributes in equation 1.

Feature-level patterns are extracted using a one-dimensional convolution operation in equation 2:

$$F = ReLU(W_c * X + b_c) \quad (2)$$

where W_c and b_c denote convolutional weights and bias, * represents the convolution operation, $ReLU(\cdot)$ is the rectified linear unit activation, F denotes the extracted feature map. To adaptively learn feature importance, a gating vector is generated using a sigmoid activation in equation 3:

$$G = \sigma(W_g F + b_g) \quad (3)$$

Where W_g and b_g represent gating parameters, $\sigma(\cdot)$ denotes the sigmoid function, $G \in [0,1]^n$ assigns importance weights to feature. The gated feature map is obtained via element wise multiplication in equation 4:

$$F_g = F \odot G \quad (4)$$

Where $\odot$ denotes element-wise multiplication. The final prediction probability is computed using a sigmoid-activated output neuron in equation 5:

$$\hat{y} = \sigma(W_o F_g + b_o) \quad (5)$$

Where $\hat{y} \in [0,1]$ represents the confidence score, a threshold of 0.5 is used to determine disease presence or absence.

Sensitivity Derivation and Privacy Classification

Although, the FG-CNN model is very effective in disease classification and learning the importance of features via its gating mechanism, it does not directly predict data sensitivity. Sensitivity prediction is thus performed as a post-inference task that converts model predictions into security-informed decisions.

This section presents the proposed sensitivity derivation and privacy classification approach, which bridges the learning and encryption modules of the system.

Feature-Level Sensitivity Derivation

The feature-gating mechanism in the FG-CNN yields a set of gating activations that capture the contribution of input attributes to the final prediction. The gating activations are used to calculate a quantitative measure of feature-level sensitivity in equation 6. Let the gating vector be represented as:

$$G = \{G_1, G_2, \dots, G_n\} \quad (6)$$

where denotes the gating value associated with the feature and is the number of input attributes. The aggregate feature-level sensitivity score is computed as:

$$S_{feature} = \frac{1}{n}\sum_{i=1}^{n} G_i \quad (7)$$

A higher value of indicates that the underlying clinical data exert a stronger influence on the diagnostic outcome and therefore possess greater privacy relevance in equation 7.

Policy-Based Sensitivity Assignment

Certain transaction elements are not derived from the input feature space and therefore cannot be evaluated using the gating mechanism. For these elements, sensitivity is assigned according to predefined privacy policies that represent their inherent confidentiality requirements. This policy-driven sensitivity is denoted by: $S_{policy} \in \{0,1\}$ where a value of 1 denotes a privacy-critical element and 0 denotes a non-sensitive element. This rule-based assignment ensures that all inherently sensitive transaction components are consistently protected, independent of model behavior.

Final Sensitivity Classification

The final sensitivity decision for each transaction component is determined by combining the learned feature-level sensitivity with the policy-based sensitivity in equation 8. A binary sensitivity flag λ is

$$\text{computed as: } \lambda = \begin{cases} 1, if\ S_{feature} \geq \tau\ or\ S_{policy} = 1 \\ 0, \qquad otherwise \end{cases} \quad (8)$$

where τ denotes a predefined sensitivity threshold. The components related to $\lambda = 1$ are considered sensitive and undergo selective encryption, whereas components related to $\lambda = 0$ are considered non-sensitive and are stored in a protected but unencrypted form.

Output of Sensitivity Analysis

The result of the sensitivity derivation process is a binary sensitivity flag set that controls the security operations. The binary sensitivity flags are immediately used by the Transaction-Structured Selective Encryption framework to identify which components of a transaction need to be encrypted, thus facilitating privacy-efficient data management.

Transaction Formation and Structuring

Based on the sensitivity derivation process, the output results produced by the FG-CNN and the related sensitivity flags are formatted in a structured transaction format that is suitable for secure storage and blockchain processing. This is an intermediate step that translates the results of the analysis into a standardized format without performing any cryptographic processing.

Let a transaction be defined as a collection of m structured elements in equation 9:

$$T = \{f_1, f_2, \dots, f_m\} \quad (9)$$

where each f_i represents an individual transaction component, such as analytical results, reference identifiers, or system metadata. The transaction format is designed to be compatible with the decentralized storage and blockchain platforms while providing flexibility for selective protection.

Each transaction element f_i is linked to a related sensitivity flag λ_i, which is computed as described in Section 3.4. The transaction formation procedure thus enables a sensitivity-informed transaction representation in equation 10:

$$T_\lambda = \{(f_1, \lambda_1), (f_2, \lambda_2), \dots, (f_m, \lambda_m)\} \quad (10)$$

This organized representation is intended to facilitate the explicit identification of the privacy-critical components of the transaction prior to the encryption operation. There is no encryption or hashing operations involved in this phase, and this ensures that the transaction is lightweight and flexible enough to be adapted to the security operations that follow. The result of this phase is a fully formed and annotated transaction ready to be utilized as the input to the selective encryption framework.

Transaction-Structured Selective Encryption (TSSE)

In order to ensure that the privacy of the transaction is protected effectively without incurring high overhead costs due to encryption, the proposed Transaction-Structured Selective Encryption (TSSE) approach to selective encryption encrypts the transaction selectively. Unlike traditional methods that encrypt the entire record, the TSSE approach uses the sensitivity flags generated in the previous phase to encrypt only the privacy-critical components of the transaction.

Selective Encryption Strategy

For each transaction element f_i, encryption is performed based on its sensitivity flag λ_i:

$$f_i^{enc} = \begin{cases} \mathrm{Enc}_{K_t}(\mathrm{f}_i), & if\ \lambda_i = 1 \\ f_i, & if\ \lambda_i = 0 \end{cases}$$

where $\mathrm{Enc}_{K_t}(\cdot)$ is a symmetric encryption function and K_t is a transaction-specific cryptographic key. This method ensures that the sensitive components are completely protected, and the non-sensitive components are available in a protected form, thus decreasing the overhead of computations in equation 11.

Transaction-Dependent Key Generation

To avoid the reuse of keys and improve the resistance of the system against cryptographic attacks, a dynamic encryption key is created for each transaction in equation 12. The transaction-specific key is obtained through a key derivation function as follows:

$$K_t = KDF(ID_t \parallel TS_t) \quad (12)$$

Here, ID_t represents the transaction identifier, TS_t represents the transaction timestamp, and ‖ represents the concatenation function. This approach ensures that there is no issue of cryptographic dependency among the transactions, thereby enhancing the security of the system.

Integrity Protection and Verification

For protecting data integrity and facilitating tamper verification, a cryptographic hash is calculated over the selectively encrypted transaction in equation 13:

$$H_t = \mathcal{H}(T^{enc}) \quad (13)$$

where, $\mathcal{H}(\cdot)$ referred as secure hash function. This hash acts as an integrity reference, allowing the transaction to be verified without revealing any sensitive information.

Output of TSSE Framework

The TSSE-secured transaction is expressed as follows:

$$T^{TSSE} = \{f_1^{enc}, f_2^{enc}, \dots, f_m^{enc}, H_t\} \quad (14)$$

The encrypted transaction is subsequently stored off-chain in a secure manner, while its integrity hash and related identifiers are maintained on the blockchain. Through the use of sensitivity-based encryption, transaction-level key control, and hash-based integrity checking, TSSE maintains a practical trade-off between data privacy and efficient management within a decentralized environment in equation 14.

4 Experimental Implementation

The experiments used on a PC workstation which featured an AMD Ryzen processor as its primary CPU to handle data preprocessing work and simulation tasks and selective encryption and blockchain-related operations. The proposed Feature-Gated Convolutional Neural Network (FG-CNN) model was trained and tested on an NVIDIA GPU to speed up the training process. The experimental assessment was carried out on the UCI Heart Disease dataset. The split ratios of 80:20 for training and testing were taken into consideration to check the robustness of the proposed framework.

Evaluation Metrics

The performance of the proposed FG-CNN-based heart disease prediction model is measured using the conventional classification performance metrics. As the problem is a binary classification for the presence and absence of heart disease, the performance of the model can be measured in terms of accuracy, precision, recall, F1-score, and specificity. These performance measures help in evaluating the efficiency of the model in making accurate predictions for patients with heart disease as well as patients without heart disease. Accuracy measures the efficiency of the model in making accurate predictions, while precision and recall measure the reliability and sensitivity of the model in making accurate predictions for patients with heart disease. The F1-score measures the average of precision and recall, and specificity measures the efficiency of the model in making accurate predictions for patients without heart disease. The mathematical expressions used to calculate these performance metrics are given in table 2.

Table 2: Lists the calculation expressions for each classification measure

SL.NO	Performance Metrics	Mathematical Expression
01	Accuracy	$\frac{TP+TN}{TP+TN+FP+FN}$
02	Sensitivity or recall	$\frac{\text{TP}}{\text{TP+FN}}$ x100
03	Precision	$\frac{TN}{TP+FP}$
04	F1-Score	$2.\frac{Precison * Recall}{Precision + Recall}$

TP –True Positive, TN-True Negative, FP-False Positive, FN-False Negative

Evaluation Outcomes

FG-CNN Model Performance

The figure 2 illustrates a confusion matrix of a classification model, which illustrates how the classification model performs in predicting two classes. The colors are color-coded, with blue indicating higher normalized scores and yellow indicating lower scores. Class 1 is predicted with a 99.80 percent accuracy with only 0.20 percent being misclassified as Class 2. Correspondingly, Class 2 has a prediction accuracy of 99.80 and a small misclassification error of 0.20 as Class 1. The matrix demonstrates an excellent model having the least misclassifications.

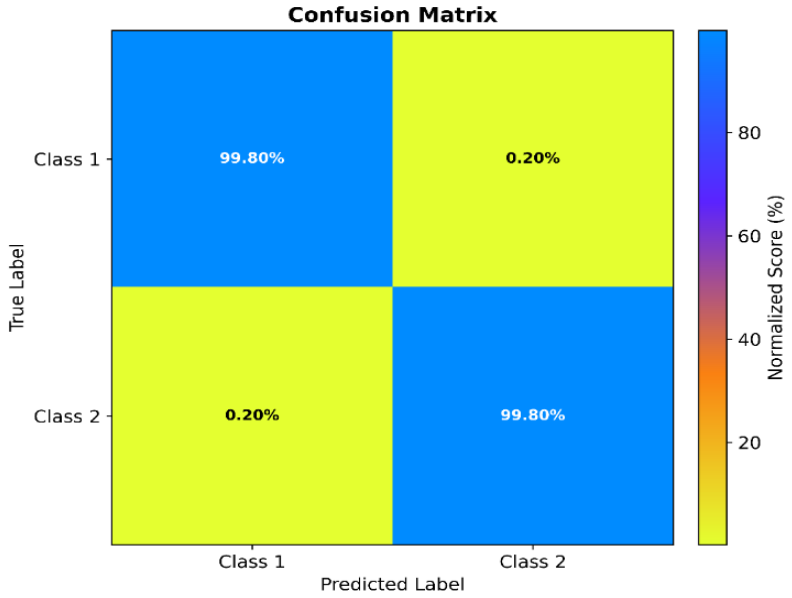

Figure 2: Shows the performance evaluation of the proposed FG-CNN model using the confusion matrix

The below figure 3 illustrates Receiver Operating Characteristic (ROC) curve of a classification model, in comparison of two classes. Class 0 and Class 1 have high True Positive Rates (TPR) with an Area Under the Curve (AUC) of about 0.99 in each case. The broken diagonal curve is a graph of the performance that a random classifier had, where the AUC is significantly lower. The curves show that the model is excellent in both the classes with a low rate of false positives.

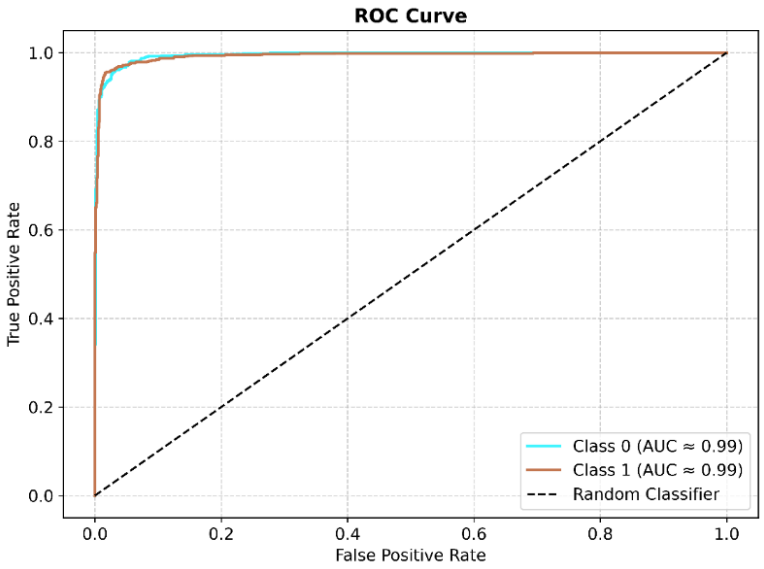

Figure 3: Shows the performance evaluation of the proposed FG-CNN model using the ROC curve

The figure 4 represents the training and validation loss curves during 160 epochs. The curves are both declining gradually, which is a sign that the model is learning successfully in the training process. The same pattern is observed in the training loss (in purple) and the validation loss (in green), the validation loss is right behind the training loss. This indicates that the model is generalizing effectively and not overfitting since the two losses decrease at a comparable rate.

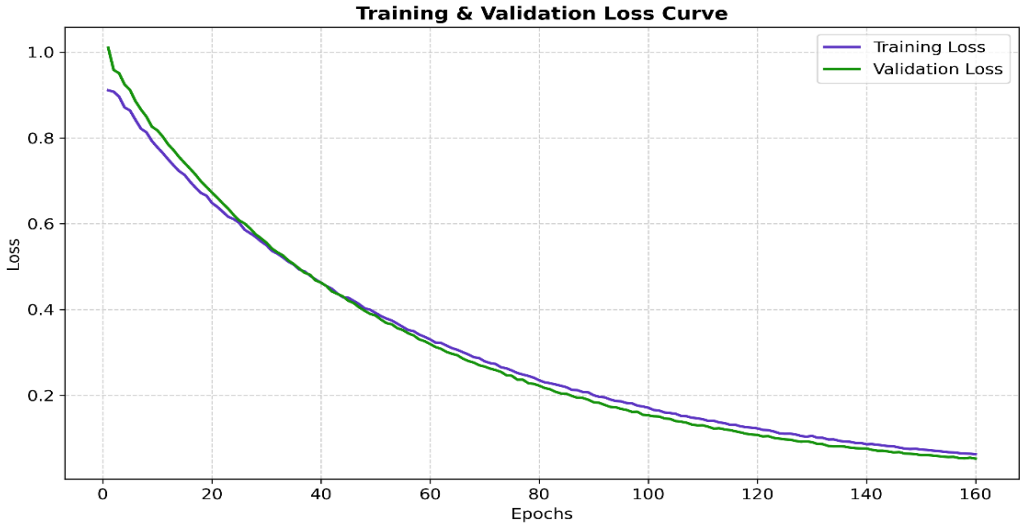

Figure 4: Shows the performance evaluation of the proposed FG-CNN model using the ROC curve

The figure 5 shows the comparative performance analysis of various deep learning models for the classification of heart disease. The performance of traditional models like DNN and 1D-CNN is moderate, with accuracy less than 93%, which is not effective in understanding the complex relationships between features in clinical datasets. The performance of advanced models like DeepFM, AutoInt, and TabNet improves owing to enhanced feature interaction and representation learning. Nevertheless, the performance of these models is slightly low compared to the proposed model. The proposed Feature-Gated Convolutional Neural Network (FG-CNN) model performs better compared to

all other comparative models. The accuracy of 98.6%, precision of 98.7%, recall of 98.9%, and F1-score of 98.7% are obtained by the proposed model. The improved performance of the proposed model results from its ability to assign more importance to relevant clinical features, whereas irrelevant features are completely ignored. The performance analysis shows that the proposed FG-CNN model has better diagnostic reliability and robustness and is highly suitable for heart disease prediction in healthcare applications.

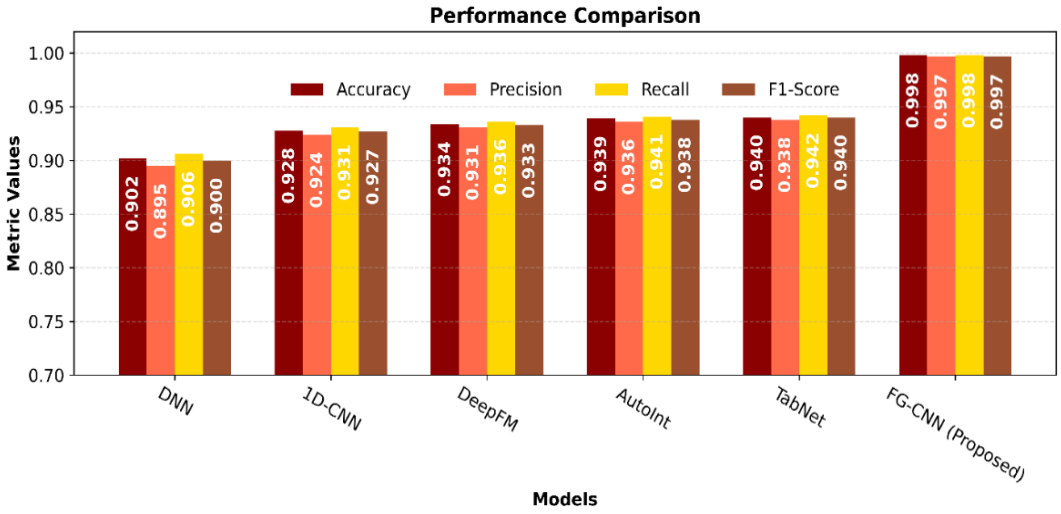

Figure 5: Presents the performance comparison analysis for the proposed FG-CNN model

Blockchain Security and Efficiency Analysis

The figure 6 shows the conventional full encryption methods, the proposed blockchain framework using the Transaction-Structured Selective Encryption (TSSE) approach improves computational efficiency by selectively encrypting privacy-sensitive components of healthcare transactions.

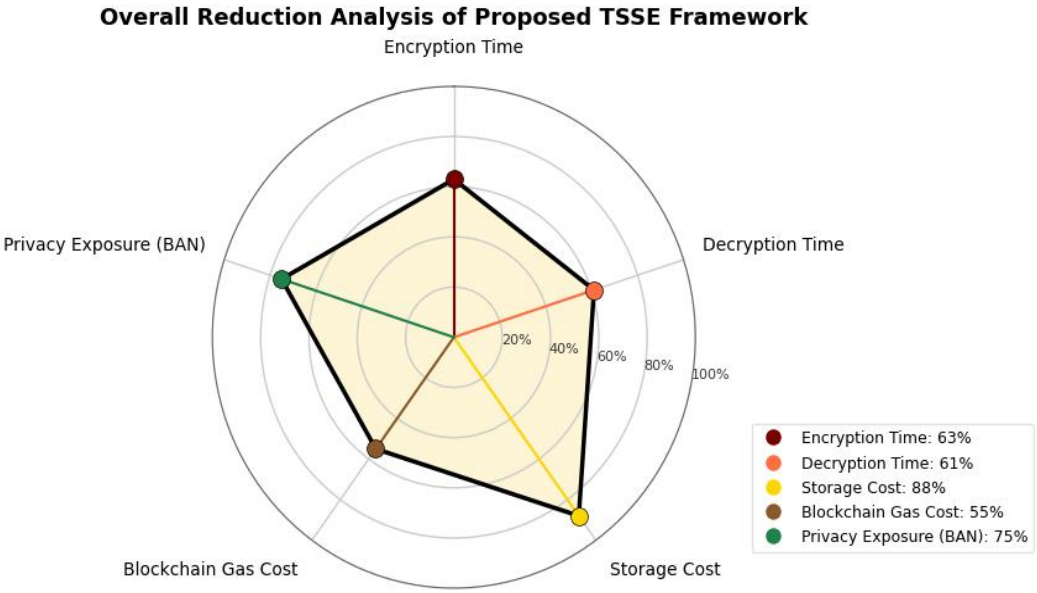

Figure 6: Illustrates the blockchain security and efficiency analysis for the proposed TSSE framework

The proposed selective encryption method reduces encryption time by 63% and decryption time by 61% compared to conventional full encryption methods. In addition, the proposed blockchain framework with encrypted off-chain storage and on-chain integrity verification reduces blockchain storage overhead by 88% compared to conventional blockchain storage methods. The proposed blockchain framework also reduces blockchain gas consumption by 55% due to the reduced size of encrypted transactions. In addition, the proposed blockchain framework with selective access to sensitive data elements reduces privacy risk by 75% compared to conventional blockchain frameworks. In summary, the proposed TSSE-based blockchain framework achieves a balance between strong privacy preservation and efficient blockchain resource utilization.

5 Conclusion

The article suggests a new blockchain-based healthcare architecture that consists of a Feature-Gated Convolutional Neural Network (FG-CNN) to detect diseases and a Transaction-Structured Selective Encryption (TSSE) method to manage the data effectively and safely. This combined system solves significant issues in healthcare data security and privacy by providing a smart model of disease diagnosis and a system to reduce cryptographic overhead. Experimental outcomes reveal that the FG-CNN model attains 98.6%, 98.7%, 98.9%, and 98.7% accuracy, precision, recall and F1-score respectively in heart disease prediction showing well-diagnostic results. The TSSE method enhances better encryption performance, which cuts the encryption time by 63%, decryption time by 61% and blockchain storage costs by 88%. Also, the system saves 55 % of blockchain gas and greatly decreases privacy risk by 75 %, demonstrating its applicability to decentralized healthcare protocols. The study also does not provide a closer analysis of the statistical evaluation of the model in terms of its generalization capability with different datasets. Selective encryption combined with blockchain integrity guarantees a secure and scalable delegated data management. Future studies may aim to validate this framework using a variety of medical data, implement this framework to predict multiple diseases, and consider the combination of the real-time diagnostic system and blockchain to implement this framework to a broader application in healthcare.

Declaration Statement

1. Conflict of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

2. Funding

This research was not funded by any external organization or institution.

3. Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

4. Ethical Approval

Ethical approval for this study was obtained from the [Institutional Review Board/Research Ethics Committee], ensuring compliance with ethical standards in the use of medical data and patient confidentiality.

5. Author Contributions

- **D. Bhanu Sravanthi:** Conceptualization, methodology, data collection, and analysis.
- **Dr.M. Pounambal:** Literature review, methodology, and manuscript writing.
- **Dr.P. Venkata Krishna:** Supervision, data interpretation, and critical revision of the manuscript.
- **Dr.V. Saritha:** Validation, formal analysis, and manuscript editing.

References

[1] Adeniyi, J. K., Ajagbe, S. A., Adeniyi, A. E., Adeyanju, K. I., Afolorunso, A. A., Adigun, M. O., & Ogene, I. (2025). A blockchain-based smart healthcare system for data protection. *IScience*, *28*(4). https://doi.org/10.1016/j.isci.2025.112109

[2] Bhuvaneshwari, P., Krishnaveni, A., Robinson, Y. H., & Julie, E. G. (2025). EnCTN: an enhanced AI-enabled deep learning framework for security enhancement in blockchain transactions. *Scientific Reports*. https://doi.org/10.1038/s41598-025-29160-6

[3] Chakravarthy, D. G., Gopi, R., Murugan, S., & Joseph, E. R. (2025). Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework. *Scientific Reports*, *15*(1), 30379. https://doi.org/10.1038/s41598-025-13831-5

[4] Cheikhrouhou, O., Mershad, K., Laurent, M., & Koubaa, A. (2025). Blockchain and emerging technologies for next generation secure healthcare: a comprehensive survey of applications, challenges, and future directions. *Blockchain: Research and Applications*, 100305. https://doi.org/10.1016/j.bcra.2025.100305

[5] Chen, C., Isa, N. A. M., & Liu, X. (2025). A review of convolutional neural network based methods for medical image classification. *Computers in biology and medicine*, *185*, 109507. https://doi.org/10.1016/j.compbiomed.2024.109507

[6] Galety, M. G., Tan, K. T., Kshirsagar, P. R., & Polamuri, S. R. (2025). Medical data security and effective organization using integrated Blockchain principles in AI-based healthcare 6.0 infrastructures. *Discover Computing*, *28*(1), 162. https://doi.org/10.1007/s10791-025-09588-0

[7] Haddad, A., Habaebi, M. H., Elsheikh, E. A., Islam, M. R., Zabidi, S. A., & Suliman, F. E. M. (2024). E2EE enhanced patient-centric blockchain-based system for EHR management. *Plos one*, *19*(4), e0301371. https://doi.org/10.1371/journal.pone.0301371

[8] Kumar, A., Batta, P., Rathore, P. S., & Ahuja, S. (2025). Secure healthcare data sharing and attack detection framework using radial basis neural network. *Scientific Reports*, *15*(1), 15432. https://doi.org/10.1038/s41598-025-99676-4

[9] Kumar, R., Garg, S., Kaur, R., Johar, M. G. M., Singh, S., Menon, S. V., ... & Lozanović, J. (2025). A comprehensive review of machine learning for heart disease prediction: challenges, trends, ethical considerations, and future directions. *Frontiers in artificial intelligence*, *8*, 1583459. https://doi.org/10.3389/frai.2025.1583459

[10] Lee, C. H., Lim, K. H., & Eswaran, S. (2025). A comprehensive survey on secure healthcare data processing with homomorphic encryption: attacks and defenses. *Discover Public Health*, *22*(1), 137. https://doi.org/10.1186/s12982-025-00505-w

[11] Li, K., Lohachab, A., Dumontier, M., & Urovi, V. (2025). Privacy preservation in blockchain-based healthcare data sharing: A systematic review. *Peer-to-Peer Networking and Applications*, *18*(6), 1-53. https://doi.org/10.1007/s12083-025-02148-9

[12] Mhiri, S., Egio, A., Compastié, M., & Cosio, P. (2024, July). Proxy re-encryption for enhanced data security in healthcare: A practical implementation. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1-11). https://doi.org/10.1145/3664476.3670874

[13] Mole, J. S., & Shaji, R. S. (2024). Ethereum blockchain for electronic health records: securing and streamlining patient management. *Frontiers in Medicine*, *11*, 1434474. https://doi.org/10.3389/fmed.2024.1434474

[14] Olaymi, S. E. Z. (2025). Performance and security analysis of fully homomorphic encryption in cloud-based healthcare blockchain. *Health Informatics Journal*, *31*(4), 14604582251394616. https://doi.org/10.1177/14604582251394616

[15] Popoola, O., Rodrigues, M. A., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2024). An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security. *Internet of Things*, *27*, 101314. https://doi.org/10.1016/j.iot.2024.101314

[16] Ravichandran, D., Jebarani, W. S. L., Mahalingam, H., Meikandan, P. V., Pravinkumar, P., & Amirtharajan, R. (2025). An efficient medical data encryption scheme using selective shuffling and inter-intra pixel diffusion IoT-enabled secure E-healthcare framework. *Scientific Reports*, *15*(1), 4143. https://doi.org/10.1038/s41598-025-85539-5

[17] Sadr, H., Salari, A., Ashoobi, M. T., & Nazari, M. (2024). Cardiovascular disease diagnosis: a holistic approach using the integration of machine learning and deep learning models. *European Journal of Medical Research*, *29*(1), 455. https://doi.org/10.1186/s40001-024-02044-7

[18] Shobayo, O., & Saatchi, R. (2025). Developments in deep learning artificial neural network techniques for medical image analysis and interpretation. *Diagnostics*, *15*(9), 1072. https://doi.org/10.3390/diagnostics15091072

[19] Singh, M. K., Pippal, S. K., Sharma, V., & Chakraverti, A. K. (2025). Blockchain-Enabled Healthcare: Critical Analysis of Applications, Limitations, and Technical Solutions. *SN Computer Science*, *6*(7), 824. https://doi.org/10.1007/s42979-025-04360-z

[20] Tabassum, S., Muhammad, F., Khan, M. A., Khan, M. U., Awan, D., Gohar, N., ... & Al-Rasheed, A. (2025). A machine learning-based framework for heart disease diagnosis using a comprehensive patient cohort. *Computers, Materials & Continua*, *84*(1), 1253-1278. https://doi.org/10.32604/cmc.2025.065423

Authors Biography

D. Bhanu Sravanthi is a Research Scholar in the Department of Computer Science and Engineering at Sri Padmavati Mahila Visvavidyalayam, Tirupati, India. She has 3 years of teaching experience. Her research interests include Blockchain Technology, Internet of Things, and Healthcare Analytics. She has published research articles in reputed journals and conferences.

Dr. M. Pounambal received her Ph.D. in Computer Science and Engineering from Vellore Institute of Technology (VIT), Vellore, India, in 2015. She possesses extensive academic and research expertise spanning over 25 years of dedicated teaching experience at VIT, Vellore. Her research interests encompass emerging and interdisciplinary domains such as the Internet of Things (IoT), Image Processing and Data Analytics. She has actively contributed to these fields through academic engagement, research initiatives, and mentoring of students. Currently, Dr. Pounambal serves as a Professor at VIT, Vellore. She

has been actively involved in teaching, research, and mentoring undergraduate and postgraduate students in these areas

Dr.P. Venkata Krishna (SM'13) received the M.Tech. degree in computer science and engineering from the National Institute of Technology Calicut, India, in 2000, and the Ph.D. degree in computer science and engineering from Vellore Institute of Technology, India, in 2008. He is currently a Professor with the Department of Computer Science, Sri Padmavati Mahila Visvavidyalayam, where he also heads the P. Venkata Krishna Data Science Research Centre. His research interests include operating systems, computer networks, wireless sensor networks, cloud computing, Internet of Things, computer security, wireless mesh networks, and vehicular ad hoc networks. He has authored more than 270 research publications

Dr. V. Saritha is Professor and Head of the Department of Computer Science and Engineering at Sri Padmavati Mahila Visvavidyalayam, Tirupati. She has over 27 years of teaching and research experience in wireless networks, IoT, cloud computing, machine learning, and VANETs. She earned her Ph.D. from VIT University and has published more than 85 papers in reputed journals and conferences. Dr. Saritha has received several research and teaching awards and actively guides doctoral scholars successfully.