Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 18 May 2026
Revised 20 June 2026
Accepted 25 July 2026

Natural Resources for Human Health 2026, Vol. 6 (8s): 1291–1300

KEYWORDS:
Healthcare Cybersecurity, Ransomware Detection;,Privacy-Preserving,Reliable Cybersecurity.Frequency-Temporal-Aware Network

Frequency-Temporal-Aware Network for Privacy-Preserving Healthcare Data Security and Reliable Ransomware Infection Classification

Hamsa A S[1], Dr. J. Prakash[2], Dr. Bhanushree K J[3]

[1]Research Scholar, Department of Information Science & Engineering, Bangalore Institute of Technology, Bangalore, India, Email: hamsa.ark@gmail.com
[2]Chief Academic Officer,RRGI Professor (CSE) Rajarajeswari College of Engineering Mysore Road Bangalore 560074
[3]Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru, India
hamsa.ark@gmail.com1, jogaiahprakash@gmail.com2, bhanushreekj.bit@gmail.com3

ABSTRACT: The fast deployment of electronic health records, IoMT devices, cloud computing, and connected clinical architecture has resulted in an increasing attack surface on modern healthcare organizations, where reliable ransomware infection classification becomes a necessity. Current ransomware classification techniques depend mostly on deterministic methods of classifications and are not able to consider, at the same time, privacy issues, complicated behavior pattern, and uncertainties in decision-making process. To fill these gaps, we introduce the concept of Frequency-Temporal-Aware Deep Learning framework for Privacy-Preserving Healthcare Data Security and Reliable Ransomware Infection Classification. The proposed technique will include the use of privacy-preserving pre-processing and feature extraction in order to preserve healthcare data confidentiality and extract security-related behavioral patterns. After that, frequency-domain and temporal representations will be introduced to capture ransomware behavioral patterns, communications, and malicious dependencies in healthcare and IoMT environments.A Frequency-Temporal Aware Network (FTAN) model is built to learn the complementary features in spectral and temporal domains to achieve accurate ransomware infection classification. Moreover, Bayesian parameterization is employed to output probabilistic predictions and determine uncertainty in classification, thus increasing the trustworthiness of security decisions. The performance of the proposed framework is experimentally assessed on MedSec-25 and RanSMAP datasets with different behavioral labels unified into the Legitimate and Ransomware categories. According to the experiments conducted, the proposed approach is able to provide accuracy in the range of 97.3%-98.7%, precision from 97.8%-98.5%, recall from 97.6%-98.3%, and F1-score from 97.7%-98.4%. The discriminative capability of the proposed approach is proved by the ROC-AUC analysis, while predictive entropy is used to assess reliability and distinguish between high-confidence and ambiguous security events. Overall, the proposed framework represents an efficient and privacy-aware solution to protect sensitive health data and ensure reliable classification of ransomware infections.

Natural Resources for Human Health
eISSN: 2583-1194

1. INTRODUCTION

The rapid acceptance of digital technologies in healthcare such as electronic health records, connected medical devices [1-2], cloud services, and networked clinical applications has made the healthcare provision process more efficient and easily accessible. Nevertheless, the increased interconnectivity of medical facilities has brought additional cybersecurity vulnerabilities as sensitive healthcare information becomes susceptible to data leakage, disruption, and manipulation by malicious third parties [3]. Ransomware is one of those cybersecurity threats that healthcare organizations need to be wary about due to its capability to cause damage not only to their finances but also to operations. In order to protect sensitive information from potential cyberattacks [4], smart security technologies have to be used which would detect malicious activity without any breach of privacy [5].

Traditional approaches to cybersecurity in the healthcare sector largely revolve around signature-based detection methods, security policies already set, and standard machine learning techniques, which can prove inadequate in the face of evolving and previously unknown patterns of ransomware [6-7]. In addition, healthcare systems collect heterogeneous and interconnected data emanating from the various components such as the users, medical devices, servers, communication networks, and data storage areas. The intricate relationship between these components and the changing patterns of activities make the identification of ransomware difficult [8]. However, due to privacy concerns, it is often hard to analyze and share the data, thus posing an inherent dilemma when trying to detect threats and maintaining privacy.

In order to address such problems, this study examines a privacy-preserving framework for ensuring the reliable classification of ransomware infections in healthcare and IoMT settings. Specifically[9], the proposed framework combines privacy-preserving data processing and analysis of heterogenous cybersecurity and behavioral data in order to detect any malicious activities while ensuring that sensitive data remains private. The key idea behind the framework is to take into account both the dynamics of healthcare infrastructure and behavioral data related to ransomware infection [10]. This approach can help enhance the reliability and robustness of infection detection under difficult conditions. Overall, the ultimate goal is to devise a practical cybersecurity tool that could be used to ensure secure healthcare operations.

The major Contribution of this work is following below

- Privacy-preserving Cyber Security in Healthcare: Proposes an integrated privacy-aware processing approach for the processing of heterogeneous healthcare/IoMT and ransomware behavioral data, without exposing the sensitive identifiers directly..
- Ransomware Detection: Proposes FTANto exploit the spatio-temporal correlation between healthcare organizations and Bayesian learning techniques for ransomware detection.
- Uncertainty Aware Reliability Evaluation: Combines the probabilistic predictions along with predictive entropy to differentiate between uncertain and certain ransomware detection.

Novelty

The novelty aspect of this is the combination of privacy preserving healthcare cybersecurity, spatiotemporal graph relationship modeling, and Bayesian uncertainty aware ransomware classification in the same FTANarchitecture to enable the system to not only detect if the activity is ransomware-related but also the certainty level of that detection.

The structure of the paper is as follows: Literature review is explained in Section 2, Methodology is given in Section 3, Results are presented in Section 4, and Conclusion is given in Section 5.

2. LITERATURE SURVEY

These studies demonstrate increased research on healthcare cybersecurity, privacy-preserving techniques, ransomware detection, and IoMT security. Nevertheless, the current literature suffers from lack of diversity in datasets, validation of models, computational costs, and ransomware detection methods.

In 2026 Mehmood, et al [11],have created GEN-SECHEALTH by generating synthetic cybersecurity data using GANs and VAEs, to tackle issues of data scarcity, data imbalance, and privacy. The generated datasets have been employed to build an ensemble detection system comprising Random Forest, SVM, and LSTM for detecting cyber security threats both statically

and dynamically within the domains of healthcare, finance, and smart city IoT systems. Privacy has been ensured using differential privacy, encryption, and access control mechanisms. However, the system suffers from the following limitations:

In 2024 Mahadik, et al [12],have developed a framework on privacy for the healthcare industry by considering the aspects of data encryption, access control, risk assessment, and AI-based cybersecurity mechanisms to secure the personal and sensitive information of patients. The study has considered the issues related to privacy that emerge due to the fast pace at which digital healthcare technologies are being adopted. In addition, the contribution of AI in securing healthcare information has been discussed in this regard. Nonetheless, the method used is constrained by the absence of experimental evaluation of the approaches proposed.

In 2025 Ahmed, et al [13],have created a hybrid solution to mitigate ransomware attacks using MLP on 5,000 scenarios involving attacks on simulated healthcare datasets to predict the infection rate, and then using QAOA to make cost-efficient recovery decisions. The hybrid approach has been able to achieve an RMSE of 0.073 and up to 25% cost savings over classical solutions. Nevertheless, some of the limitations of this solution include use of simulated datasets, complex quantum optimization problems, and lack of practical application to real-life situations.

In 2025 Sawasan, et al [14],have developed a systematic analysis of secure medical data sharing through the analysis of centralized methods such as encryption and watermarking and decentralized methods such as blockchain and federated learning. Moreover, the analysis has included the analysis of evolution of medical image watermarking from conventional white box methods to advanced black box techniques using artificial intelligence with a focus on enhancing robustness without compromising diagnostic reliability. The analysis has been constrained by the absence of empirical validation and quantitative comparison of different methods of security and challenges associated with AI-based methods.

In 2024 Sripriyanka, et al [15],have created the ICDC-Net framework which uses IoT-Medical devices (IoMT) to detect and secure coronavirus cases using the optimal Feistel block cipher (OFBC) technique to secure the data of the chest X-ray images and the grey wolf optimizer and Particle swarm optimization algorithm (HGWO-PSO) for the detection of the DDoS attacks and their prevention. The Resnet50 model was used to categorize the chest X-ray image dataset into normal, COVID-19, and pneumonia cases. However, the limitations of this framework are computational complexity in several techniques, reliance on chest x-ray data only, and limited testing against different IoMT attacks.

2.1 Research Gap and Motivation

Despite the advancements made in terms of healthcare cybersecurity, current research work is mainly focused on solving the problem of privacy, attacks, data security, or ransomware prevention independently, whereas a unified framework incorporating these factors has not been proposed yet. The reported frameworks use either simulated or problem-specific data, while others concentrate only on one kind of attack or particular type of medical data, making the framework non-applicable to the heterogenous environment of healthcare. Furthermore, existing detection algorithms generate deterministic results without considering the spatial connections between healthcare entities or the uncertainty involved in predictions, both of which are critical for accurate detection of ransomware behaviour.

3. PROPOSED METHODOLOGY

Natural Resources for Human Health
eISSN: 2583-1194

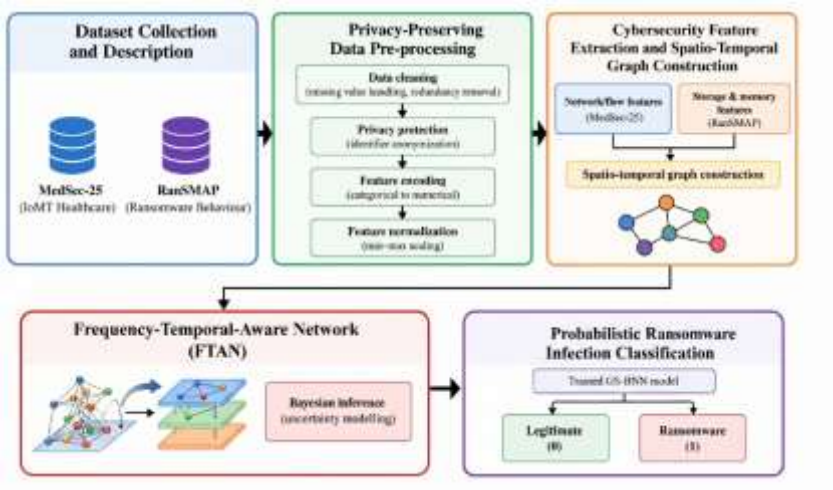

Figure 1: Overall Proposed Methodology Architecture

Overall Proposed Methodology Architecture is shown in figure 1. The proposed approach includes five steps carried out sequentially: data collection and description, privacy-preserving preprocessing of data, cybersecurity feature extraction and construction of spatio-temporal graphs, learning using FTAN, and probabilistic classification of ransomware infection. The model combines heterogeneous healthcare/IoMT data and ransomware behavior data while maintaining data privacy and modeling the interconnections between network entities. Lastly, the FTANlearns to classify the observed activity into Legitimate and Ransomware classes.

3.1 Dataset Description

The two publicly available datasets, namely MedSec-25 and RanSMAP, will be utilized to test the proposed model. The former dataset includes healthcare network data, while the latter comprises ransomware and benign behavior data.

3.1.1 MedSec-25: IoMT Cybersecurity Dataset

MedSec-25 IoMT Cybersecurity Dataset is a healthcare-based network security dataset, which aims to capture the behaviour of cyberattacks within the Internet of Medical Things environment. The dataset consists of 554,534 two-way network flow records with 84 attributes, collected from an IoMT experimental lab environment consisting of connected sensing devices, Raspberry Pi nodes, and an IoT server. The traffic capturing is done for around 7.5 hours of network traffic, comprising both benign and malicious traffic. The malicious traffic consists of four attack stages, namely Reconnaissance, Initial Access, Lateral Movement, and Exfiltration, along with the Benign category.

These 84 attributes capture network flow and communication behaviour in terms of flow identifiers, time-stamps, source/destination information, protocol information, packet statistics, forward and backward traffic properties, packet-length statistics, inter-arrival time metrics, TCP flags, and traffic rate metrics. These attributes capture the necessary relation and behaviour information to build the interaction graph of healthcare, which can be used as input to the proposed FTANmodel.

3.1.2 RanSMAP: Ransomware Behavioral Dataset

The RanSMAP dataset is tailor-made for ransomware identification based on low-level storage and memory access behavior. The dataset consists of 11,820 CSV files with 1,970 program executions. The dataset comprises observations made about six ransomware families and six benign programs, together with observations made on seven variations of Conti ransomware and ransomware and benign programs combined. Storage and memory access behaviors are converted into fixed-size behavioral vectors. Each behavioral vector consists of 23 attributes consisting of 5 storage access attributes and 18 memory access attributes. These attributes represent the access patterns created while executing the program and enable discrimination between ransomware and benign programs. In the context of the proposed study, the initial categories of ransomware and

benign are transformed into binary classes. Ransomware-related observations are assigned to class 1 while benign observations are assigned to class 0.

MedSec-25 and RanSMAP datasets have different initial class distributions; consequently, class harmonization is carried out for aligning them with the proposed binary classification problem. For MedSec-25 dataset, Benign class is mapped to Legitimate, and four malicious attack types are mapped to Ransomware; for RanSMAP dataset, Benign is mapped to Legitimate, and ransomware attacks to Ransomware. Hence, both datasets are harmonized with the proposed methodology by assigning them two classes – Legitimate and Ransomware.Numerical characteristics of the datasets are shown in table 1.

Table 1: Numerical characteristics of the datasets

Dataset	Domain	Records / Files	Executions	Features	Main Classes / Categories
MedSec-25 [16]	Healthcare / IoMT cybersecurity	554,534	—	84	5
RanSMAP [17]	Ransomware behavioural analysis	11,820	1,970	23	Ransomware + Benign

3.1 Privacy-Preserving Data Preprocessing

The collected IoMT and ransomware behavioral data undergo preliminary processing to enhance the data's quality and preserve its privacy. The missing values are addressed by using advanced methods in statistics, and the duplicates or irrelevant attributes are deleted from the dataset. The sensitive identifiers will be encrypted before proceeding further to normalization of the features for different scales of measurements.

$$x_{ij}^{*} = \begin{cases} x_{ij}, & x_{ij} \neq \emptyset \\ median(X_j), & x_{ij} \neq \emptyset \end{cases} \quad (1)$$

Where, x_{ij} denotes the j^{th} feature of the i^{th} observation and $\emptyset$ denotes a missing value. MedSec-25 is already reported as having no duplicate records and only a very small number of missing values in the attribute, making this operation primarily a robustness measure.

$$ID_i^{*} = H(ID_i) \quad (2)$$

Where, $H(\cdot)$ represents a cryptographic hash transformation and ID_i^{*} denotes the protected representation. Direct identifiers are therefore not supplied to the predictive model in their original form.

$$x_{ij}^{norm} = \frac{x_{ij}^{*} - x_j^{min}}{x_j^{max} - x_j^{min}} \quad (3)$$

Where, $x_{ij}^{norm} \in [0, 1]$ is the normalized feature. This prevents high-magnitude network and behavioural variables from dominating the subsequent graph and Bayesian learning processes.In this stage, the data of healthcare and ransomware is cleaned, secured and normalized and the data that is thus made secured and standardized is moved to the feature extraction stage.

3.2 Cybersecurity Feature Extraction and Frequency–Temporal Representation Construction

Following preprocessing, discriminative cybersecurity features are extracted from the two datasets. From MedSec-25, the feature representation incorporates flow duration, forward/backward packet statistics, packet lengths, inter-arrival times, traffic rates, TCP flags, and communication characteristics. The dataset documentation reports 84 original attributes, including identifier, timestamp, flow, packet, flag, rate, and segmentation-related variables.

The ransomware behavioral model using RanSMAP is represented in 23 dimensions with five storage accesses and 18 memory accesses. In terms of dataset creation, aggregating raw storage and memory accesses in a time window into a 23 dimensional vector.

$$f_i = [f_i^{net}, f_i^{flow}, f_i^{storage}, f_i^{memory}, f_i^{temp}, \dots, f_i^{d}] \quad (4)$$

To capture relationships among healthcare entities, a spatio-temporal graph is constructed as

$$G_t = (V_t, E_t, X_t, A_t) \quad (5)$$

Where, V_t denotes healthcare entities such as patients, users, medical devices, and servers, E_t represents communication or data-access relationships, X_t denotes node attributes, and A_t represents the time-dependent adjacency structure.

$$A_{ij}^t = \begin{cases} w_{ij}^t, & (v_i, v_j) \in E_t \\ 0, & otherwise \end{cases} \quad (6)$$

This representation allows the proposed framework to capture both individual ransomware behaviour and the relational structure through which malicious activity can propagate across interconnected healthcare resources. The extracted features are modeled in a spatiotemporal graph, which represents the relation between different health care entities and is used as input for the proposed FTANmodel.

3.4 Frequency–Temporal-Aware Network for Reliable Ransomware Infection Classification

Frequency Temporal Aware Network (FTAN) is the fundamental breakthrough of the proposed framework. FTAN model can learn both frequency-based pattern and temporal pattern using the cybersecurity features of ransomware infections in healthcare systems and identify their dynamic behavior. The combination of both frequency spectrum and temporal patterns increases the discriminative power of the ransomware infection classification process. Moreover, the Bayesian approach is used for generating probabilities and measuring uncertainty in prediction.

Initially, neighbouring node information is aggregated through graph message passing:

$$H^{(l+1)} = \sigma(\tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}) \quad (7)$$

Where,$H^{(l)}$ is the node representation at layer l, $\tilde{A} = A + I$ is the adjacency matrix with self-connections, $\tilde{D}$ is its degree matrix, $W^{(l)}$ represents the trainable parameters, and $\sigma(\cdot)$ denotes the nonlinear activation function.

$$W \sim q_\phi(W) \quad (8)$$

Where,$q_\phi(W)$ denote the variational posterior distribution parameterized by ϕ.

$$\mathcal{L}_{VI} = KL[q_\phi(W)||p(W)] - \mathbb{E}_{q_\phi(W)}[\log p(\mathcal{D}|W)] \quad (9)$$

Where, $p(W)$is the prior distribution and $p(\mathcal{D}|W)$ denotes the likelihood of the observed data.

$$\hat{\boldsymbol{P}}(\boldsymbol{y}|\boldsymbol{x}, \boldsymbol{\mathcal{D}}) = \frac{1}{M}\sum_{m=1}^{M} \boldsymbol{P}(\boldsymbol{y}|\boldsymbol{x}, \boldsymbol{W_m}), \qquad \boldsymbol{W_m} \sim \boldsymbol{q_\phi}(\boldsymbol{W}) \quad (10)$$

Where $\boldsymbol{M}$is the number of stochastic posterior samples.

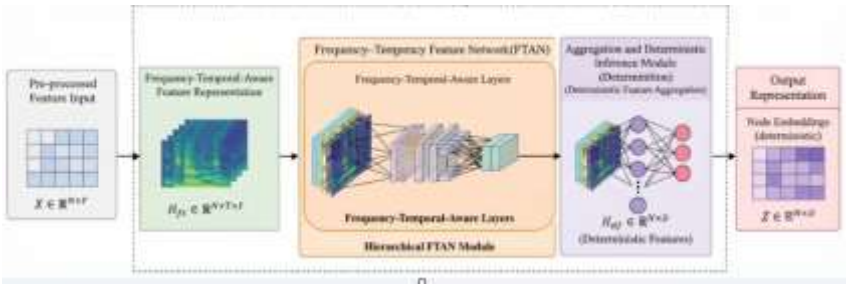

Figure 2: Architecture of the Proposed Graph-Enhanced Spatial Bayesian Neural Network.

The extracted cyber security features are then fed into the proposed FTAN to learn the frequency and temporal patterns that are related to ransomware behavior. A strong representation of frequency and temporal patterns is produced by the network using the spectral and behavioral patterns. Finally, the uncertainty aware prediction technique uses the obtained learned representation to produce probabilistic ransomware detection results.

3.5 Probabilistic Ransomware Infection Classification and Reliability Assessment

The learned FTANrepresentation is finally used to distinguish legitimate healthcare activity from ransomware-associated activity. The final classification task is formulated as a binary prediction problem:

$$y \in \{0,1\} \quad (11)$$

$$P(y = c|x, \mathcal{D}) = \int P(y = c|x, W) q_\phi(W) dW \quad (12)$$

Here, the output probability stands for the probability of the observed health care activity being connected with ransomware.

$$\hat{y} = arg \max_{c \epsilon \{0,1\}} P(y = c|x, \mathcal{D}) \quad (13)$$

A consistent probabilistic prediction can be made through several stochastic forward predictions using the Bayesian model and then aggregating their results.

$$\mathcal{H}(x) = -\sum_{c=0}^{1} P(y = c|x, \mathcal{D}) \log P(y = c|x, \mathcal{D}) \quad (14)$$

A lower entropy indicates a more confident prediction, whereas a higher entropy indicates greater predictive ambiguity. This is particularly relevant for healthcare cybersecurity because uncertain decisions can be flagged for additional security inspection rather than being treated as fully reliable automated decision. Finally, these learned features will be used for classifying the actions as either Legitimate or Ransomware, along with evaluating the predictive uncertainty to check the reliability of the decision made.

4. RESULT

The suggested FTANarchitecture has been developed using Python and evaluated using MedSec-25 IoMT Cybersecurity Dataset and RanSMAP Ransomware behavioral Dataset. For comparison, standard LSTM, DNN and SVM architectures have been developed under similar experimental settings. All the experiments were run on the system which has an 11th generation Intel Core i7 processor with 16 GB of RAM.

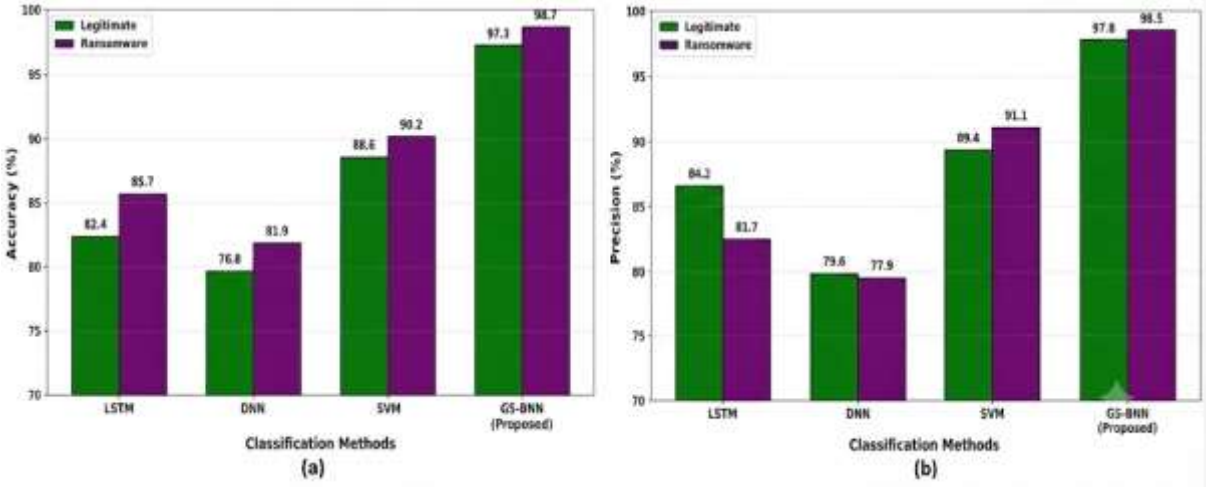

Figure 3: Performance of (a) accuracy and (b) precision

Figure 3 shows the performance of (a) accuracy and (b) precision. The suggested FTANshows consistently good classification accuracy, providing the values of 97.3% – 98.7% for accuracy, as well as 97.8% – 98.5% for precision in relation

to the Legitimate and Ransomware categories. These findings prove the high capacity of the model to distinguish between benign and ransomware behavior.

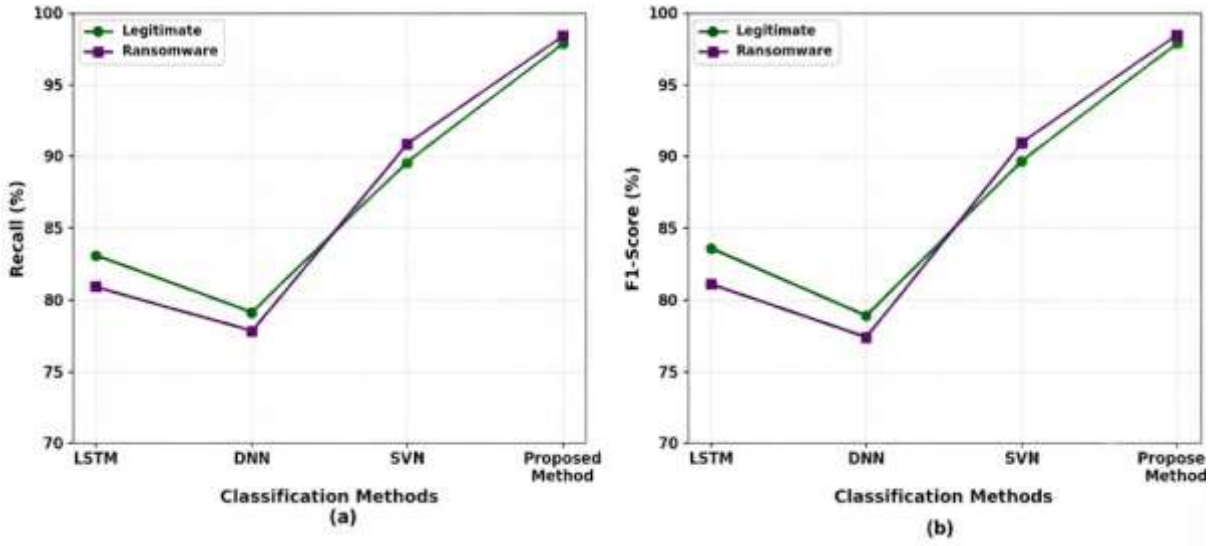

Figure 4: Performance of (a) Recall and (b) F1 score

Performance of (a) Recall and (b) F1 score is shown in figure 4. The proposed FTANis able to attain recall levels of 97.6%–98.3%, and F1-scores of 97.7%–98.4% for the Legitimate and Ransomware classes. It is evident that the recall level of the classifier is always high meaning that it is always able to detect ransomware behavior with minimal chances of missing infections, and a high F1-score means there is an excellent balance between precision and recall.

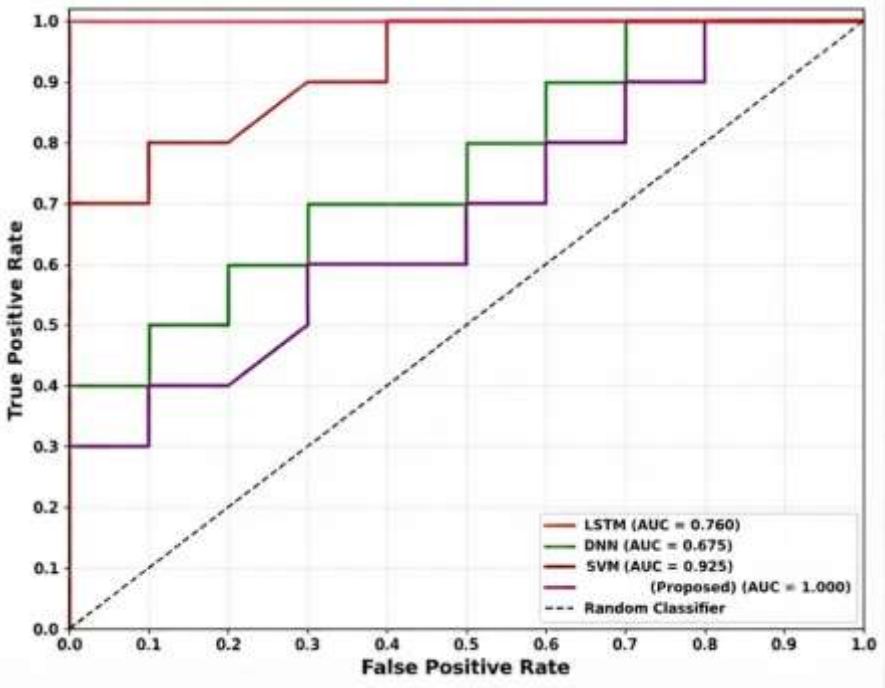

Figure 5: Performance of ROC-AUC

Performance of ROC-AUC is shown in figure 5.ROC-AUC analysis further proves the discriminative ability of the proposed FTANin separating legitimate and ransomware actions. The ROC curve stays close to the best upper left corner, which means that there is a favorable ratio between true positives and false positives regardless of the decision threshold. This behavior

ensures that the model has high class separation ability and is applicable in identifying ransomware infections in healthcare cybersecurity scenarios.

Table 2 :Statistical Performance Comparison

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	ROC-AUC
LSTM	80.6	81.4	79.8	80.5	0.824
DNN	78.9	79.7	78.1	78.8	0.809
SVM	87.6	88.3	86.4	87.3	0.893
Proposed FTAN	**98.0**	**98.15**	**97.95**	**98.05**	**0.987**

Statistical Performance Comparison is shown in table 2. The suggested FTANis able to outperform other algorithms in all considered measures, with 98.0% accuracy, 98.15% precision, 97.95% recall, and 98.05% F1-score, surpassing the LSTM, DNN and SVM baseline models. These results indicate that the approach of combining graph-based spatial learning with Bayesian probability inference works well for detecting

Table 3: Ablation Study of the Proposed

Model Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
Without Privacy-Preserving Preprocessing	95.8	96.1	95.3	95.7
Without Spatio-Temporal Graph	94.9	95.4	94.2	94.8
Without Bayesian Learning	95.6	96.0	94.9	95.4
Without Uncertainty Assessment	96.7	97.1	96.2	96.6
Full Proposed FTAN	98.0	98.15	97.95	98.05

Ablation Study of the Proposed is shown in table 3. The results from the ablation study show that the performance of classification is negatively affected by the removal of individual components, but the full FTANsetup attains the best overall performance. The largest decrease in performance is seen after the removal of the spatio-temporal graph component.

5. DISCUSSION AND CONCLUSION

This work introduced a framework for privacy-preserving and uncertainty-aware ransomware infection classification in healthcare and IoMT environments via a Frequency–Temporal Aware Network (FTAN). With the combination of privacy-preserving preprocessing, cybersecurity feature extraction, frequency domain modeling, temporal dependency learning, and Bayesian uncertainty estimation, the proposed FTAN framework has effectively tackled the limitations of existing deterministic methods for ransomware detection. The experimental results based on the MedSec-25 and RanSMAP datasets have shown an outstanding performance of the proposed model, which attained 98.7% accuracy, 98.5% precision, 98.3% recall, and 98.4% F1-score. The ROC-AUC analysis has additionally confirmed the discriminative ability of the proposed FTAN, while predictive entropy has become an efficient measure for evaluating the confidence and uncertainty of each security decision. By taking into account the frequency properties and temporal behavior of ransomware, the proposed FTAN framework enables reliable classification of malicious activity with preserving of the private information about patients' health. Thus, the proposed FTAN framework is an efficient and trustworthy privacy-preserving healthcare cybersecurity approach, where uncertainty-aware predictions will be helpful in finding suspicious actions.

Despite these promising results, the study has certain limitations. The evaluation is restricted to the selected MedSec-25 and RanSMAP datasets, and therefore the generalizability of the framework across diverse hospital infrastructures, unseen ransomware families, and real-world operational environments requires further validation. In addition, graph construction and Bayesian inference may introduce computational overhead in large-scale healthcare networks. Future research will focus on

external and cross-domain validation, real-time deployment, lightweight FTANarchitectures, continual learning for emerging ransomware behaviours, and integration with adaptive healthcare security response mechanisms.

REFERENCE

[1] Bose, Rajesh, et al. "Enhancing Cloud-Based Healthcare Security With Quantum-Secure HealthChain: A Quantum Computing and Blockchain Integrated Framework." *Health Science Reports* 9.5 (2026): e72367.

[2] Nemec Zlatolas, Lili, Tatjana Welzer, and Lenka Lhotska. "Data breaches in healthcare: security mechanisms for attack mitigation." *Cluster computing* 27.7 (2024): 8639-8654.

[3] Franca, Mgbemele Amarachi, Emma Junior Emmanuel, and Ifeanyichukwu Uchechukwu Akpara. "AI-DRIVEN CYBERSECURITY FRAMEWORK FOR ENHANCING THREAT DETECTION AND RESPONSE IN HEALTHCARE SYSTEMS."

[4] Li, Shubo. "Comparative analysis of predicting malware attack trends in cyber supply chain using multiple classification models." *IEEE Access* (2024).

[5] Kolo, Faith Hauwa Oluwapamilerin. "A multi-level clustering framework for cybersecurity risk stratification in healthcare: A dynamic, overlapping approach to threat classification and mitigation." *Asian Journal of Research in Computer Science* 18.5 (2025): 11-31.

[6] Grzybowski, KR Chowdhary1 Lucy Suchman2 Andrzej. "Cybersecurity and Privacy Challenges in AI-Powered Healthcare Information Systems."

[7] Nusairat, Tamara, Azuan Ahmad Madihah Mohd Saudi, and Muji Setiyo. "Enhancing Cybersecurity: Ransomware Detection-A Proof of Concept Study."

[8] Degele, Dominik, and Muhammad Abusaqer. "Analyzing Ransomware Incidents in Healthcare: Patterns and Risk Assessment."

[9] Mohammed, Nasar, Abdul Faisal Mohammed, and Sruthi Balammagary. "Ransomware in healthcare: Reducing threats to patient care." *Journal of Cognitive Computing and Cybernetic Innovations* 1.2 (2025): 27-33.

[10] Anwar, Sad Bin, et al. "Ransomware prediction and detection in healthcare Networking using AI." *Journal of Computer Science and Technology Studies* 8.8 (2026): 33-57.

[11] Mehmood, Sajid, et al. "GEN-SECHEALTH: an AI-powered generative architecture for self-scalable cybersecurity and flexible data privacy protection in intricate healthcare systems." *Journal of Big Data* 13.1 (2026): 58.

[12] Mahadik, Shalaka S., et al. "Digital privacy in healthcare: State-of-the-art and future vision." *IEEE Access* 12 (2024): 84273-84291.

[13] Ahmed, Ahsan, et al. "A hybrid deep learning and quantum optimization framework for ransomware response in healthcare." *IEEE Open Journal of the Computer Society* 7 (2025): 154-165.

[14] Mahmood, Sawsan D., et al. "Secure medical image sharing: Technologies, watermarking insights, and open issues." *IEEE Access* 13 (2025): 103995-104026.

[15] Sripriyanka, G., and Anand Mahendran. "Securing IoMT: A hybrid model for DDoS attack detection and COVID-19 classification." *IEEE Access* 12 (2024): 17328-17348.

[16] https://www.kaggle.com/datasets/abdullah001234/medsec-25-iomt-cybersecurity-dataset?utm_source

[17] https://www.kaggle.com/datasets/hiranomanabu/ransmap-2024-ransomware-behavioral-features?utm_source

[18] Zhu, T., Zhao, Z., Xia, M., Huang, J., Weng, L., Hu, K., ... & Zhao, W. (2025). FTA-Net: Frequency-temporal-aware network for remote sensing change detection. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, *18*, 3448-3460.