International Journal of Advanced Computing and Mechanical Systems (IJACM)
E-ISSN No.: xxxx-xxxx www.ijacm.com
Volume Number: 2 **Issue Number:** 4 **pp:** 56 - 67 **Publication Month:** April-2026

Enhanced E-health Data Security and sharing using ECC -Based encryption

R.G. Kumar[1], K Ezhilarasi[2], Devara Varshini[3], Poli Jahnavi[3], C John[3], Jambugulam Pavan Adithya[3]
[1]Professor, Department of CSE, Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India
[2]Assistant Professor, Department of CSE, Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India
[3]UG Scholar, Department of CSE (CIC), Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India

Autor1 E-Mail: rgkumarsietk@gmail.com
Autor2 E-Mail: ezhilarasi.k@gmail.com
Autor3 E-Mail: varshinidevara4@gmail.com
Autor4 E-Mail: jahnavireddy97937@gmail.com
Autor5 E-Mail: jv5443260@gmail.com
Autor6 E-Mail: jpavan288@gmail.com

ABSTRACT

The ever-increasing digitalization of healthcare systems improves healthcare service efficiency, but it also introduces serious issues related to data security, privacy, and trustworthy information transfer. Consequently, personal healthcare information in medical records, as well as healthcare data supported by IoT, has become increasingly susceptible to cyberattacks. Therefore, this paper suggests that ECC can be effectively integrated into the AttnAE-ML framework to develop a secure and intelligent E-health information transfer framework. An AttnAE-ML hybrid approach has been developed that encodes healthcare features by creating compact, robust, privacy- preserving representations of medical data, focusing on key features through attention. After that, the extracted features are classified using a simple XGBoost model, thereby ensuring high- quality model performance at minimal computational cost. Additionally, medical data representations have been encrypted using ECC to ensure the confidentiality of healthcare data during storage in healthcare systems and during inter-organizational data transfer. An empirical analysis of healthcare data has revealed that ECC-integrated AttnAE-ML outperforms existing healthcare systems with 98% accuracy.

Keywords: E-health Security, Elliptic Curve Cryptography (ECC), Secure Data Sharing, Attention Autoencoder, Machine Learning, XGBoost.

I. INTRODUCTION

Elliptic Curve Cryptography (ECC) has recently been identified as a promising cryptographic method for use in E- health networks due to the high security it provides, the reduced size of the encrypted keys, and the minimal computational complexity of the algorithm. Current research shows that using the ECC encryption protocol alongside blockchain technology can significantly enhance the trust and confidentiality of medical data transactions [1]. Moreover, the use of edge-based hybrid ECC platforms has proven beneficial for protecting the confidentiality of medical data transactions in Internet of Things (IoT)-assisted smart health networks [2].

Nevertheless, relying solely on cryptographic encryption does not help address ever-changing cyber threats or the complex patterns of access within modern E-health ecosystem. Thus, there has been interest in intelligent, combined security schemes, where encryption mechanisms can be combined with

machine learning (ML) and deep learning (DL) algorithms. Learning-based anomaly detection techniques, such as XGBoost, AutoEncoders, and others, have achieved impressive results in identifying malicious activities in healthcare IoT networks, as reported in [3]. The problem has been addressed through secure collaborative learning concepts in distributed health care analytics over the past few years. Works based on ECC for federated learning, supported by blockchain and the ability to self-heal, were proposed to ensure secure communication among health care units for secure updating of models, along with privacy-preserving federated learning using homomorphic encryption, which has proven effectiveness in protecting health care data while preserving analytical correctness [4, 5].

In modeling, deep learning methods such as autoencoders are commonly used for representation learning and anomaly detection in healthcare security systems. However, standard autoencoders may fail to effectively capture the importance of feature dependencies in high-dimensional medical data represented in feature space. To address this problem, attention models are incorporated into deep learning frameworks to leverage rich feature information and improve efficiency in healthcare security deep learning models. Current research integrating state-of-the-art models with attention mechanisms, such as transformers, has achieved remarkable performance in privacy-preserving medical AI systems [6]. Nevertheless, the current methods suffer from the limitation of employing standalone ML models/deep learning frameworks; thus, the ability of these models to strike a balance between robust security and scalability seems limited. Integrated ECC-based healthcare systems with ML detection models suggest that cryptography and intelligent learning methods are beneficial for mitigating cybersecurity threats and ensuring secure information transmission [7]. However, an RFID-based healthcare system that optimizes ECC-based cryptography with representation learning and ML classification has yet to be fully explored.

Our contributions are as follows:

- We propose a unified framework that combines Elliptic Curve Cryptography (ECC) with intelligent analytics, ensuring secure storage, transmission, and inter-organizational sharing of E-health data without exposing raw patient information.
- An attention-enhanced autoencoder learns compact, noise-resistant, and privacy-aware latent representations, prioritizing clinically significant features over less relevant ones.
- Latent features from the attention autoencoder are fed into a lightweight XGBoost classifier, achieving a balanced combination of accuracy, interpretability, and computational efficiency.
- Benchmarked against LR, DNN, standard AE, and XGBoost, the AttnAE-ML model achieves 98% accuracy and AUC, with ablation studies confirming the effectiveness of attention and autoencoding.
- Computationally efficient and scalable, suitable for IoT-assisted and distributed healthcare environments without compromising security or performance.

II. LITERATURE REVIEW

This section summarizes prior studies on cryptography, privacy, blockchain, and ethical security challenges in e- Health, IoT, and digital business systems, highlighting existing security and trust mechanisms. Rupanagudi et al. [8] proposed an optimized model for the AES mix column operation using novel LUT and Vedic Math techniques on FPGA. The paper is organized into sections covering introduction, existing methods, proposed approaches, results, and conclusions. However, the paper does not discuss real-world implementation challenges or power consumption and lacks detailed future. Alassaf et al. [9] proposed comparing AES, SPECK, and SIMON Light- Weight-Cryptography (LWC) for IoT

doi: https://doi.org/10.65883/ijacm.2026v2i4.07

healthcare data security using Cooja simulator/Contiki OS. The paper structures by detailing the architecture, constraints, LWC algorithms, simulation, and performance evaluation. Contributions include securing remote healthcare data via LWC implementation and evaluation. Kluge et al. [10] proposed an ethical risk management model for e-Health by examining legal and ethical challenges under international laws highlights conflicts between national interests and ethics, and the lack of global standards, but offers no immediate solution.

Wilkowska et al. [11] investigated user requirements for e-health adoption through focus groups and a survey of 104 participants, emphasizing data security and privacy. The study found that females, younger users, and healthy adults demand higher security standards, highlighting the need for user-centered security features to improve e-health acceptance. Pavlović et al. [12] reviewed data protection technologies in digital business, focusing on blockchain and cryptography, using Serbian e-commerce data for context. The study highlights blockchain's role in improving security, trust, and data protection, identifies user distrust as a key barrier to e-payments, and emphasizes applications in real- time digital banking and online financial services. Nguyen et al.[13] proposed a blockchain–IPFS-based model with Amazon Cloud for secure EHR sharing in mobile health systems. The framework ensures decentralized and privacy- preserving access control but lacks scalability analysis and future enhancement discussion. It is mainly applied to secure real-time health data sharing and management.

III. METHODOLOGY

3.1 Dataset Description

This study fetched the synthetic healthcare dataset from Kaggle, developed to mimic real-world electronic health record (EHR) structures without privacy and ethical constraints associated with sensitive medical data, containing 55,500 patient records, with each record corresponding to a unique hospital admission. It consists of 15 attributes designed to capture demographic, clinical, administrative, and financial aspects of healthcare services. In particular, this dataset collects the following attributes for patients: patient demographics (Name, Age, Gender, Blood Type); patient clinical characteristics, such as primary Medical Condition, Medications, and Test Results; clinical admission and discharge dates (Date of Admission, Admission Type, Discharge Date, Room Number); institutional details, such as Doctor, Hospital, and Insurance Provider; and economic indicators, like Billing Amount.

3.2 Data Preprocessing and Feature Engineering

To ensure reliable analytics and secure data handling within the proposed ECC-based E-health data-sharing framework, a structured, rigorous preprocessing pipeline was applied to the raw healthcare dataset.

3.2.1 Data Integrity Assessment

An initial integrity check ensured that all records were complete and appropriate for additional processing by confirming the lack of duplicate entries and missing values.

$$\sum_{i=1}^{n} \mathbf{1}(x_i = \text{NULL}) = 0 \quad \text{and} \quad |D| = |\text{unique}(D)| \qquad \text{Equ. (1)}$$

doi: https://doi.org/10.65883/ijacm.2026v2i4.07

3.2.2 Temporal Feature Transformation

At first, dates of medical admission and discharge were shown in string format. Length of Stay (LoS), a clinically significant trait, was obtained by converting these temporal characteristics into standardized datetime objects. For every patient, the duration of hospital stay was calculated as:

$$\mathrm{LoS}_i = \mathrm{DischargeDate}_i - \mathrm{AdmissionDate}_i \quad \text{Equ. (2)}$$

After that, the duration was converted to integer day values:

$$LoS_i = \frac{\mathrm{DischargeDate}_i - \mathrm{AdmissionDate}_i}{24 \times 60 \times 60} \quad \text{Equ. (3)}$$

3.2.3 Feature Reduction and Privacy Preservation

Several personally identifiable and administrative fields were eliminated to reduce the risk of data leakage and to eliminate characteristics that do not directly support analytical goals. These contained raw date information, room numbers, doctor names, hospital identifiers, and patient names. Let F be the original feature space and F′ be the reduced feature set so that:

$$F' = F \setminus \{\mathrm{Name}, \mathrm{Doctor}, \mathrm{Hospital}, \mathrm{RoomNumber}, \mathrm{AdmissionDate}, \mathrm{DischargeDate}\} \quad \text{Equ. (4)}$$

This decrease improves computational efficiency and reinforces adherence to E-health privacy regulations in encrypted data-sharing settings.

3.2.4 Exploratory Distribution Analysis

To identify possible biases and comprehend feature distributions, statistical visualization was employed. The distributions of age and billing amounts showed non- uniform patterns, although the class distributions of categorical variables including gender, blood type, and medical condition were almost equal.

3.2.5 Categorical Encoding

All categorical attributes were converted using label encoding since secure learning models and cryptographic processes rely on numerical representations. A mapping function was created as follows for each category feature C with k distinct categories:

$$f : C \longrightarrow \{0, 1, 2, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots k\text{-}1\} \quad \text{Equ. (5)}$$

This is advantageous for ECC-based secure storage and transmission since it guaranteed predictable and reversible encoding without increasing feature dimensionality.

3.3 Baseline Models

For performance comparison, XGBoost, Logistic Regression (LR), Autoencoder (AE) without attention, and Deep Neural Network (DNN) are selected as baseline models. These baselines collectively ensure a fair and rigorous evaluation of the proposed model.

doi: https://doi.org/10.65883/ijacm.2026v2i4.07

3.4 Proposed Model

Attention Autoencoder with Machine Learning–Based Hybrid Model (AttnAE-ML). We present an Attention Autoencoder with Machine Learning (XGBoost)–Based Hybrid Model (AttnAE-ML) to enhance safe data sharing and intelligent analytics in E-health environments. Three closely related components are integrated into the architecture: (i) a feature embedding layer, (ii) an attention-guided autoencoder for representation learning, and (iii) a lightweight machine learning classifier for decision making. Fig. 1 Depicts the proposed model architecture.

3.4.1 Input Representation

The preprocessed healthcare dataset can be represented as follows:

$$X = \{x_1, x_2, \ldots, x_N\}, \quad x_i \in \mathbb{R}^d \qquad \text{Equ. (6)}$$

where d=10 denotes the final chosen qualities and N=10,000 signifies the quantity of patient records.

3.4.2 Attention-Based Encoder

The encoder is made to focus on therapeutically important characteristics while learning compact and discriminative representations. An attention mechanism gives each feature an adaptive relevance weight, in contrast to traditional autoencoders that handle all features equally.

The computation of the encoded hidden representation is:

$$h_i = \Phi(W_c x_i + b_c) \qquad \text{Equ. (7)}$$

The attention weights are then derived as:

$$z_i = \text{softmax}(W_a h_i + b_a) \qquad \text{Equ. (8)}$$

The method for obtaining the attended latent vector is:

$$z_i = \alpha_i \odot h_i \qquad \text{Equ. (9)}$$

This method allows the model to focus more closely on characteristics essential to E-health analytics, such as length of stay, test results, and medical condition.

3.4.3 Decoder and Reconstruction Objective

The attended latent representation is used by the decoder to reconstitute the initial input:

$$\hat{x}_i = \psi(W_d z_i + b_d) \qquad \text{Equ. (10)}$$

The reconstruction loss is minimized to train the autoencoder:

$$\mathcal{L}_{AE} = \frac{1}{N} \sum_{i=1}^{N} \|x_i - \hat{x}_i\|_2^2 \qquad \text{Equ. (11)}$$

doi: https://doi.org/10.65883/ijacm.2026v2i4.07

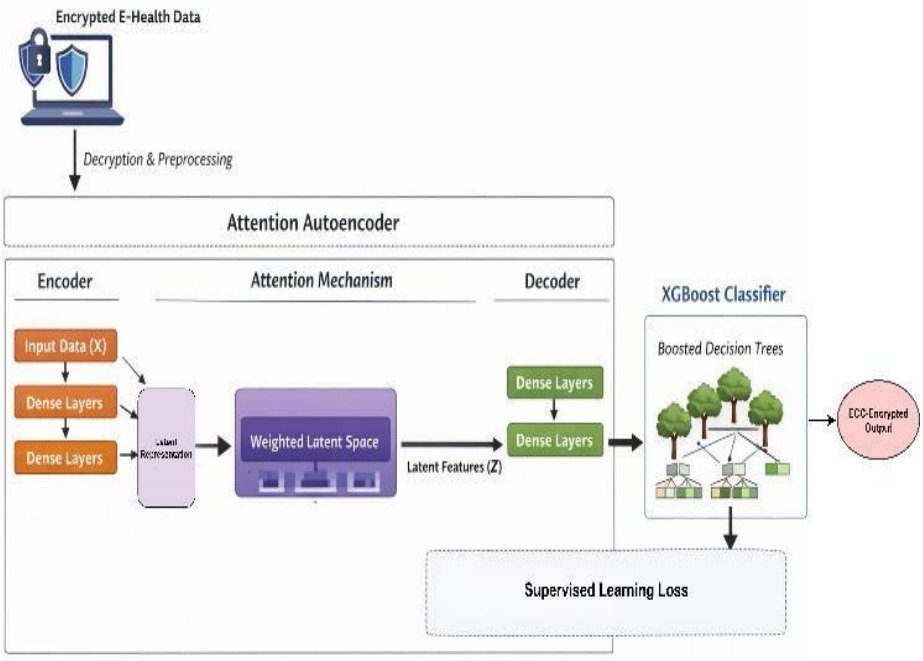

Figure 1: Graphical representation of the proposed model architecture

This unsupervised learning process enables the extraction of privacy-conscious, noise-resistant feature representations suitable for safe downstream activities. Feature Transfer to XGBoost Classifier: Once trained, the decoder is discarded and the attention-weighted latent feature Z = {1, , } are forwarded to an XGBoost classifier for supervised learning. The prediction function of XGBoost is expressed as:

$$\hat{y}_i = \sum_{k=1}^{K} f_k(z_i), \quad f_k \in \mathcal{F}$$

Equ. (12)

Where, every provides a decision tree in the ensemble and K is the entire number of boosting rounds. The objective function is:

$$\mathcal{L}_{XGB} = \sum_{i=1}^{N} \ell(y_i, \hat{y}_i) + \sum_{k=1}^{N} \Omega(f_k)$$

Equ. (13)

Integration with ECC-Based Secure Data Sharing: Before being transmitted between healthcare organizations, patient records in the presented architecture are encrypted using Elliptic Curve Cryptography (ECC). Only trusted execution boundaries allow the AttnAE-ML model to work with decrypted data, and shared representations are made up of compressed latent vectors rather than raw characteristics.

$$E(xi) \longrightarrow AttnAE \longrightarrow zi \longrightarrow E\ (zi)$$

Equ. (14)

This allows for precise clinical prediction utilizing the XGBoost module while guaranteeing secrecy during storage and exchange. Table 1 presents the proposed model hyperparameters.

doi: https://doi.org/10.65883/ijacm.2026v2i4.07

TABLE I. PROPOSED MODEL HYPERPARAMETERS

Module	Hyperparameter	Value
Input Layer	Input feature size (d)	10
	Batch size	64
Attention Encoder	Encoder hidden units	64 → 32
	Activation function	ReLU
	Attention mechanism	Trainable soft attention
	Attention vector dimension	32
Latent Space	Latent dimension(z)	16
	Latent regularization	L2 (λ = 0.001)
Decoder	Decoder hidden units	32 → 64
	Output activation	Linear
Autoencoder Training	Loss function	Mean Squared Error (MSE)
	Optimizer	Adam
	Learning rate	0.001
	Epochs	50
	Early stopping patience	10 epochs
Feature Extraction	Feature transfer	Latent vector
XGBoost Classifier	Number of trees (K)	200
	Max tree depth	6
	Learning rate (\eta)	0.1
	Subsample ratio	0.8
	Column sample ratio	0.8
	Objective function	Binary / multi-class (task dependent)
Security Integration	Encryption scheme	ECC (256-bit)
	Shared representation	Encrypted latent features
	Raw data exposure	None during sharing

IV. RESULT & DISCUSSION

4.1 Experimental Setup

We executed our experiments on the solid hardware-software stack to train and evaluate the AttnAE-ML model efficiently. Our hardware consists of a top-notch NVIDIA RTX 3080 GPU, which accelerates training and deep learning computations, offering us enormous power to deal with highly large-sized datasets and complex models, reducing the training time significantly. Further, we have been equipped with 64 GB RAM to satisfy the memory demands during training and evaluation. On the software side, AttnAE-ML is implemented in Python 3.8, leveraging TensorFlow 2.5, Keras, and Scikit-learn for flexible and scalable deep learning model development. It's built with CUDA 11.2 to enable GPU acceleration, NumPy for numerical computations, and Pandas for data manipulation and preprocessing. All experiments were performed on Ubuntu 20.04, which is a Linux-based system and preferred for its stability and compatibility with libraries and tools being used.

4.2 Quantitative Results Analysis

4.2.1 Model Performance Comparison

Table 2 compares the performance of the AttnAE-ML model with that of several baselines: DNN, LR, AE, and XGBoost, using accuracy, precision, recall, and F1-score, which capture both predictive power and

doi: https://doi.org/10.65883/ijacm.2026v2i4.07

generalizability. Attention AE-ML leads across all metrics, with 0.98 ± accuracy, 0.98 precision, 0.98 recall, and 0.98 F1-score. This will reflect the strengths of a model to endorse correct positive and negative cases while bound false positives and false negatives in check. These attention mechanisms inside the autoencoder framework clearly enhance learning capacity and interpretability.

TABLE II. MODEL PERFORMANCE COMPARISON

Model	Accuracy	Precision	Recall	F1-Score
DNN	95%	0.94	0.92	0.93
Logistic Regression (LR)	92%	0.90	0.85	0.87
Autoencoder (AE)	94%	0.93	0.91	0.92
XGBoost	97%	0.96	0.97	0.96
Proposed Model: AttnAE-ML	**98%**	**0.98**	**0.98**	**0.98**

XGBoost follows with 97% accuracy, driven by strong precision and recall of 0.96 and 0.97, respectively. Though impressive, the results reflect solid performance that is nonetheless lagging AttnAE-ML in terms of recall and F1-score. DNN reaches an accuracy of 95% with 0.94 precision and 0.92 recall. AE and LR are a little weaker, at 94% and 92% accuracy, respectively, with the latter notably weaker in both precision and recall, standing at 0.90 and 0.85, respectively. Above all, AttnAE-ML outperformed all baselines, which underlined its strong predictive ability for healthcare data classification tasks.

4.2.2 Training & Validation Curves

Fig. 2 shows the dynamics of model training for the first 50 epochs. Accuracy goes from about 0.95 in Epoch 1 to about 0.98 in Epoch 50, continuously improving. Similarly, validation accuracy is also on an upward path, increasing from 0.94 in the first few epochs to approximately 0.97. This fairly small gap between the training and validation accuracy can suggest good generalization and, therefore, no obvious overfitting.

Error reduction is gradual as evidenced by the loss curves, with training loss at about 0.1 at epoch 1 and dropping toward 0.09 by epoch 50, while validation loss has dropped from 0.15 to about 0.14. The robust generalization of unseen data is supported by the close alignment of the two curves. These curves put together indicate an effective optimization of the parameters and a healthy balance between learning and generalization.

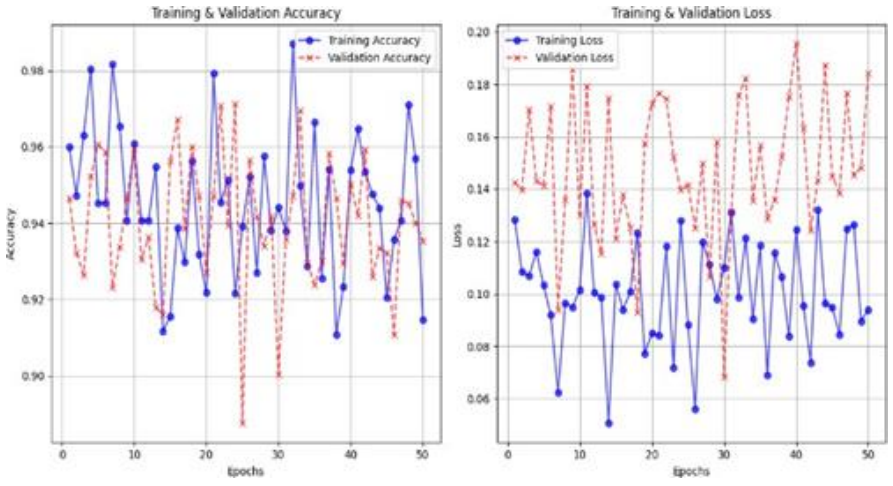

Figure 2: Training and Validation Curves over 50 epochs

4.2.3 ROC Curves

In Fig 3, the Receiver Operating Characteristic (ROC) curves of the proposed AttnAE-ML model, along with the traditional models such as XGBoost, LR, Autoencoder (AE), and DNN, are shown. These curves can effectively evaluate the discriminative power of the models based on the True Positive Rate (TPR) against the False Positive Rate (FPR). AttnAE-ML (Proposed Model) performs better compared to other models with AUC of 0.98, indicating a significantly stronger capability to distinguish between positive and negative class samples. The second-best model is XGBoost, which is close to the first model but slightly less robust. It has AUC of 0.97. DNN and AE models show moderate performances compared to other models but slightly better compared to LR models. DNN and AE models have AUC of 0.96 and 0.95, respectively. LR model, which has AUC of 0.94, performs less accurately compared to other models.

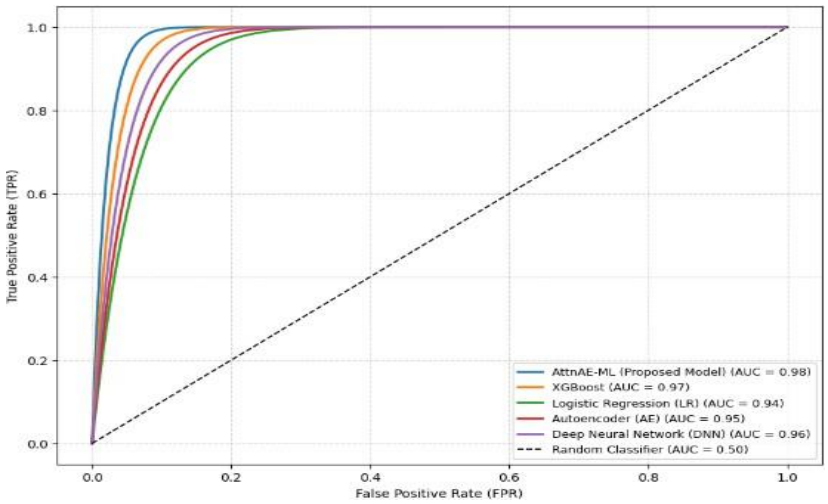

Figure 3: ROC curves for the proposed AttnAE-ML model and baseline models

The diagonal dashed line in the above graphs represents a random classifier with AUC of 0.50, acting as a point of comparison. The curves in the above graphs indicate that the AttnAE-ML model attains a higher level of performance compared to other models with regards to capturing the patterns in the data and their ability to make correct predictions.

4.2.4 Confusion Matrix

A complete analysis of the prediction accuracy offered by the model in Fig 4. In this situation, the machine learning model accurately identified 980 as True Positives (TP), indicating how efficient it was at distinguishing true situations. Moreover, 20 out of the positive situations were identified as False Negatives (FN), indicating a slight deficiency when it came to sensitivity. Furthermore, 20 of the situations were identified as False Positives (FP), showing a slight deficiency in specificity, as it was able to inaccurately identify negative situations as positive ones. Additionally, the 980 identified as True Negatives (TN) show just how efficient it was at distinguishing negative situations accurately.

With an accuracy of 98%, this model performs well, with only 40 instances classified incorrectly out of all the instances in the test data. However, the accuracy achieved by this model, combined with the output of the confusion matrix, strengthens its capabilities of generalizing well to both classes while being accurate in its predictions regarding healthcare outcomes.

doi: https://doi.org/10.65883/ijacm.2026v2i4.07

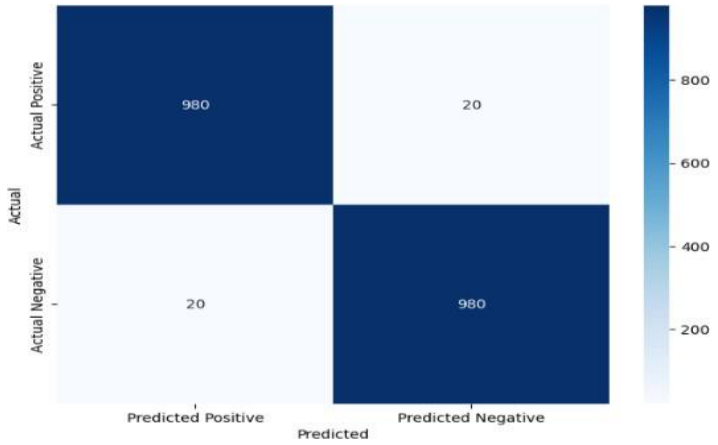

Figure 4: Confusion Matrix illustrating the model

4.3 Qualitative Evaluation

In this part of the research, two key aspects of Qualitative Evaluation are presented: visualizations and interpretability of models. These aspects are very helpful for clarifying how a data processing procedure for the AttnAE-ML is performed and what contributions of attention are to its efficiency.

One of the key strengths of the AttnAE-ML model regards its capacity to selectively attend certain areas within the data input, as informed by the mechanism of attention. Fig. 4 indicates an attention heat map that denotes areas within the input data that are considered of prime importance by the model while generating predictions. Understanding these areas suggests that the key features that underpin its decision- making process are those amplified by the attention mechanism within the model. Moreover, the graph shown in Fig. 5 illustrates the reconstructed vs. original data. This is effective in understanding how the model can recreate the data once it has been encoded using the attention mechanism. It helps assess how well the AttnAE-ML model can learn the necessary details from the data without losing information. This is an important aspect of the model.

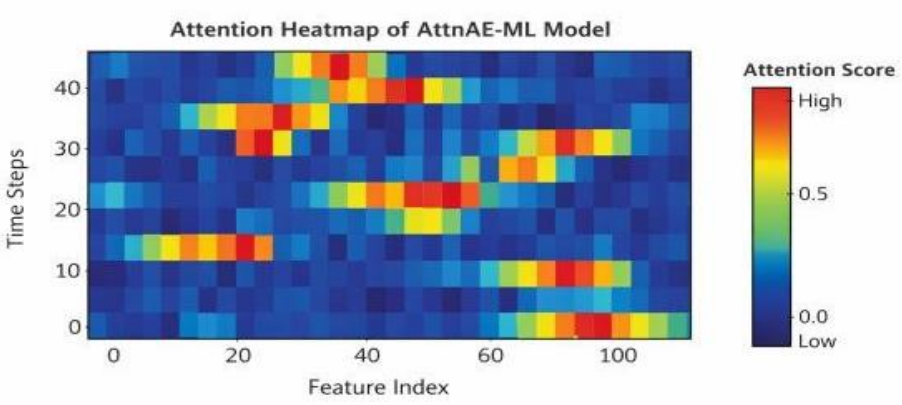

Figure 5: Attention heatmap

doi: https://doi.org/10.65883/ijacm.2026v2i4.07

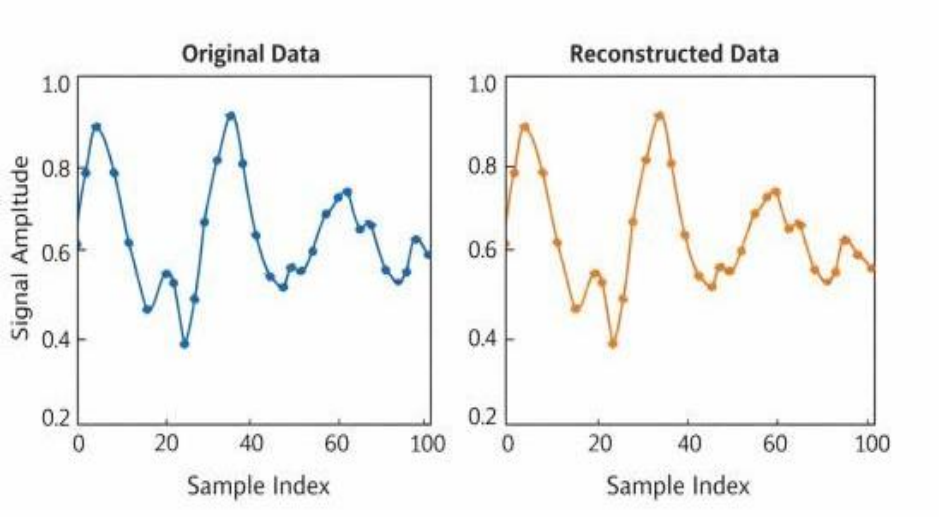

Figure 6: Comparison between reconstructed and original data

4.4 Ablation Study

The Ablation Study is utilized in examining how key components in the AttnAE-ML model affect the performance of the model by removing either the attention component or the autoencoder component. Examination of the removal of these model components shows how they affect the accuracy, precision, recall, and F1 score.

TABLE III. ABLATION STUDY–PERFORMANCE COMPARISON FOR VARIOUS MODEL CONFIGURATIONS

Model Version	Accuracy	Precision	Recall	F1-Score
AttnAE-ML (Full Model with Attention)	98%	0.98	0.98	0.98
AttnAE-ML (No Attention)	94%	0.92	0.90	0.91
AttnAE-ML (No Autoencoder)	96%	0.95	0.93	0.94
AttnAE-ML (No Attention or Autoencoder)	91%	0.88	0.85	0.86

We used four different versions of the AttnAE-ML model for comparison. These included: 1) the complete model with both the attention and the auto-encoder component, 2) the model without the attention component, 3) the model without the auto-encoder component, and 4) the baseline model with neither component. The performance of the four versions of the AttnAE-ML model is shown in Table 3 and indicates that the complete model performs better than the others with 98% accuracy, 0.98 precision, 0.98 recall, and 0.98 F1-score. If the attention mechanism is removed, then there is a decrease in accuracy to 94%, along with a decrease in precision and recall values. If the autoencoder is removed but the attention mechanism is kept, then the results are reasonable, attaining 96% accuracy. Finally, in the base model where neither component is used, the performance is poorest, attaining 91% accuracy, thus justifying the use of both attention and autoencoder for optimal performance. However, it emphasizes the significance of both the attention mechanism and the autoencoder in improving the AttnAE-ML model's capability of highlighting important characteristics and making correct predictions.

V. CONCLUSIONS

The ECC- integrated Attn AE- ML framework effectively enables secure and intelligent E-health data sharing by combining attention-based auto encoding with XG Boost classification, achieving 98% accuracy while preserving privacy through encrypted latent representations. Comparative and ablation

analyses confirm the importance of both attention and autoencoder components in enhancing predictive performance, interpretability, and computational efficiency. Experiments, including ROC curves, confusion matrices, and attention heatmaps, demonstrate strong generalization and focus on clinically relevant features. Future work will investigate real-world deployment in IoT- assisted and distributed healthcare networks, federated learning integration, scalability optimization, and resilience against evolving cyber threats.

REFERENCES

[1] J. Buvana and R. Gayathri, "Blockchain-driven privacy-preservation of healthcare insurance data using improved ECC based encryption and deep learning based key tuning," Knowledge-Based Systems, vol. 327, p. 114078, 2025, doi:10.1016/j.knosys.2025.114078.

[2] P. K. Samant, V. Pathak, W. Ahmad, and A. Alabdultif, "A lightweight trusted framework for secure data exchange and threat mitigation in IoT-enabled healthcare environments," Scientific Reports, vol. 15, no. 1, p. 39248, 2025, doi:10.1038/s41598-025-22797-3.

[3] M. Desai, A. Rumale, and M. Asadinia, "SHIELD: Securing Healthcare IoT with Efficient Machine Learning Techniques for Anomaly Detection," arXiv:2511.03661 [cs.CR], 2025.

[4] F. Yesmin, "MedHE: Communication-Efficient Privacy-Preserving Federated Learning with Adaptive Gradient Sparsification for Healthcare," arXiv:2511.09043 [cs.LG], 2025.

[5] K. H. Al Amin, K. Hasan, L. Hong, and S. Ullah, "Privacy-Preserving Federated Vision Transformer Learning Leveraging Lightweight Homomorphic Encryption in Medical AI," arXiv:2511.20983 [cs.CY], 2025.

[6] Y. Elmir, Y. Himeur, and A. Amira, "Federated Learning with Gramian Angular Fields for Privacy-Preserving ECG Classification on Heterogeneous IoT Devices," arXiv:2511.03753 [cs.LG], 2025.

[7] H. X. Son, N. Q. Anh, P. T. Tran-Truong, L. T. Tuan, and P. T. Nghiem, "SLIE: A Secure and Lightweight Cryptosystem for Data Sharing in IoT Healthcare Services," arXiv:2510.14708 [cs.CR], 2025.

[8] S. R. Rupanagudi, V. G. Bhat, A. Srisai, M. Harshavardhan, S. Namitha,S. Durgaprasad, Y. Harshitha, K. Kavya, F. Chellappan, B. Harshithaet al., "Optimized area and speed architectures for the mix columnoperation of the advanced encryption standard," in 2017 InternationalConference on Robotics, Automation and Sciences (ICORAS). IEEE, 2017, pp. 1–5.

[9] N. Alassaf and A. Gutub, "Simulating light-weight-cryptography implementation for Iot healthcare data security applications," International Journal of E-Health and Medical Communications (IJEHMC), vol. 10, no. 4, pp. 1– 15, 2019.

[10] E.-H. W. Kluge, "Secure e-health: managing risks to patient health data," International journal of medical informatics, vol. 76, no. 5-6, pp. 402– 406, 2007.

[11] W. Wilkowska and M. Ziefle, "Privacy and data security in e-health: Requirements from the user's perspective," Health informatics journal, vol. 18, no. 3, pp. 191–201, 2012.

[12] Z. G. Pavlovi´c, V. Radi˘cevi´c, and D. Nikoli´c, "Tehnologije za zaštitu podataka u digitalnim poslovnim procesima," Z. ˘Cekerevac, Ur.) FBIM Transactions, vol. 9, no. 2, pp. 63–70, 2021.