International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5298 - 5306
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0693

A Novel Approach for Health Care Data Security employing Deep Learning Algorithms Compatible with HIPAA

Saranya D[1], Srinidhi G A[2]
[1]Research Scholar, Department of Electronics and Communication, SSIT, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
[2]Research Supervisor, Department of Electronics and Communication, SSIT, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
Emails: *sharanyadamodharan@gmail.com[1] srinidhiga@ssit.edu.in[2]*

Abstract
This paper presents a novel framework for securing healthcare data using deep learning techniques while maintaining compliance with the Health Insurance Portability and Accountability Act (HIPAA). The proposed approach combines advanced encryption methodologies with neural network-based anomaly detection to protect sensitive patient information. We introduce a hierarchical security model that employs autoencoders for data compression and reconstruction, adversarial networks for threat detection, and federated learning for privacy-preserving model training. Experimental results demonstrate that our approach achieves 99.3% accuracy in detecting unauthorized access attempts while maintaining system performance. The framework successfully addresses the unique challenges of healthcare environments by providing robust security measures without compromising data accessibility for authorized personnel. This research contributes to the growing field of AI-enhanced cybersecurity specifically tailored for healthcare institutions handling protected health information (PHI).

Keywords: *Adversarial networks; Deep learning; Federated learning; HIPAA compliance; Privacy-preserving AI*

1. Introduction
Healthcare organizations are grappling with the challenge of protecting patient-specific data, as well as providing unhindered access for healthcare providers. The Health Insurance Portability and Accountability Act (HIPAA) imposes strict rules on the protection of Personal Health Information (PHI) such as proper administrative, physical and technical safety measures (Office for Civil Rights, 2013). Given the average cost of a data breach in 2023, which stood at $9.42 million per incident it is now crucial that more advanced security strategies are put in place (IBM Security, 2024). While these are still essential components of security, they are no longer enough to protect against the latest cyber threats faced by healthcare organizations. Deep learning technologies hold promises for this as well, by allowing systems to learn complex patterns in data access and use that can reveal malicious usage that may not be caught by traditional methods (Berman et al. (2019). In this paper, the authors present a novel framework that can be used to leverage the use of deep learning algorithms to improve healthcare.
Data security with HIPAA compliance. We have combined several important challenges into our solution:

- Securing sensitive patient data against unauthorized access
- Detecting anomalous patterns that may indicate security breaches
- Preserving data utility for legitimate healthcare operations
- Ensuring HIPAA compliance throughout all security processes
- Minimizing computational overhead to maintain system performance

The rest of the material is organized as follows in this document: Section II reviews the relevant work. In Section 3, we outline our framework and methodology. Experimental results and performance evaluation are given in Section 4. HIPAA compliance considerations are discussed in Section 5. Finally, Section 6 provides implications and directions for

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5298 - 5306
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0693

future research.

2. Related Work

2.1.HIPAA Security Requirements

The Security Rule of HIPPA sets standards for the security of ePHI that includes the "Security Rule" of the three known elements of security, which are privacy, reliability and accessibility (HHS, 2023). Access control, audit controls, integrity controls and transmission security are critical requirements. Recent updates have highlighted the significance of the risk analysis and management processes to deal with the new set of cyber threats (Marron/NIST, 2024).

2.2.Deep Learning in Cybersecurity

The use of deep learning in cybersecurity has also been picking up steam. CNNs have been successful in detecting malware and RNNs perform well in detecting temporal patterns in network traffic that could indicate intrusions (Muzaffar et al., 2022); Vinayakumar et al., 2019). Generative Adversarial Networks (GANs) have been used to simulate possible scenarios of attacks, thereby enhancing the defense measures (Lin et al., 2022).

2.3.Privacy-Preserving Machine Learning

New developments in privacy-preserving machine learning methods are especially applicable to the field of healthcare. One of the ways to train a model across multiple decentralized data sources without sharing raw patient data is called federated learning (McMahan et al., 2017). Some methods used to achieve differential privacy are to add calibrated noise to the data that could reveal information about an individual record without sacrificing the overall statistical value of the data (Dwork and Roth, 2014). One of the most significant challenges for secure analysis of sensitive healthcare information is that of computations on encrypted data, which is a promising approach enabled by homomorphic encryption (Acar et al., 2018).

2.4.Healthcare-Specific Security Solutions

There has been previous work that has investigated specific types of security solutions for healthcare applications. Shi et al. (2020) presented a blockchain system to secure sharing of electronic health records (EHRs). Jayabalan & O'Daniel (2016) have proposed a context-aware access control system that takes the clinical workflow into account when granting access to information. These methods all have merits in the field of healthcare data security but do not generally have the adaptive learning features associated with deep learning models.

3. Proposed Framework

We present a holistic security framework known as HIPAA-Guard that integrates different deep learning components to provide a holistic security solution for healthcare data systems. We have drawn the architecture of our framework in figure 1. The system consists of four parts: (1) an autoencoder-based anomaly detection, (2) a multi-layered security system, (3) a database of potential security issues and (4) a real-time system that notifies security staff.

3.1.System Architecture

The HIPAA-Guard is a multi-layered security system that's placed between health care data repositories and end-users. The following table (Table 1) shows the key components and their respective functions. As shown in Table 2 HIPAA Requirements and Corresponding System Features

Table 2 HIPAA Requirements and Corresponding System Features

COMPONENT	TECHNOLOGY	FUNCTION	HIPAA ALIGNMENT
Access Monitoring	BiLSTM Network	Analyzes temporal patterns in data access requests	Technical Safeguards (Access Control)
Threat Detection	Variational Autoencoder	Identifies anomalous access patterns	Technical Safeguards (Audit Controls)

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5298 - 5306
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0693

Intrusion Response	Reinforcement Learning	Determines optimal response to potential threats	Technical Safeguards (Security Incident Procedures)
Data Encryption	Quantum-Resistant Algorithms	Secures data at rest and in transit	Technical Safeguards (Transmission Security)
Federated Training	Secure Aggregation Protocol	Enables privacy-preserving model updates	Administrative Safeguards (Risk Analysis)
Compliance Verification	Rule-Based Expert System	Ensures all operations meet HIPAA requirements	Administrative Safeguards (Evaluation)

3.2.Deep Learning Components

3.2.1. Anomaly Detection with Variational Autoencoders

We use Variational Autoencoders (VAEs) for detecting abnormal access patterns, which could be an indicator of security breach. VAEs learn a compressed model of normal data access patterns and can identify deviations when they are running. The model architecture uses an encoder network which is used to map the input data to a latent space, and a decoder network which is used to reconstruct the original input data from the latent space. The encoder takes an input vector x that denotes a given data access event (with user ID, time, place, type of data accessed, etc.) and outputs the parameters of a multivariate normal distribution, namely μ and σ. A latent vector $\vec{z}$ is drawn from this distribution and fed into the decoder which decodes to output $\hat{\vec{x}}$. Loss function is a combination of reconstruction error and KL-divergence:

$$L(\vartheta, \phi) = -E_{z\sim q\phi(z|x)}[\log p\vartheta(x|z)] + D_{KL}(q\phi(z|x)||p(z))$$

Where θ and ϕ are the parameters of the decoder and encoder networks respectively, $q_{\phi}(z|x)$ is the encoded distribution, and $p(z)$ is the prior distribution (typically a standard normal distribution). For each access, a reconstruction error is measured and searching for any anomalies is attempted. Events that have reconstruction errors that pass a dynamically determined threshold are flagged for additional investigation. Input: Access event vector x, VAE model (encoder E, decoder D), threshold τ Output: Binary classification (normal/anomalous)

- Encode input: μ, σ = E(x)
- Sample latent vector: z ~ N(μ, σ)
- Reconstruct input: x̂ = D(z)
- Calculate reconstruction error: e = ||x - x̂||²
- If e > τ:
- Return "Anomalous" Else:
- Return "Normal"
- Update threshold τ based on recent error distribution

3.2.2. Threat Modeling with Generative

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5298 - 5306
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0693

Adversarial Networks

To simulate possible attack vectors of healthcare data systems,GANs are used. The problem is that the generator network G is attempting to create fake access patterns that can trick the[1-5] discriminator network D which has been trained to recognize the legitimate access patterns from the synthetic access patterns. The "training goal" is in the minimax game expression:

minG maxD Ex~pdata(x)[log D(x)] + Ez~pz (z)[log(1 − D(G(z)))]

Where $p_{data}(x)$ represents the distribution of legitimate access patterns and $p_z(z)$ is a prior noise distribution. This adversarial training process strengthens the system's ability to detect novel attack patterns.

3.2.3. User Behavior Modeling with BiLSTM Networks

Temporal patterns of user interaction with healthcare data systems are captured using Bidirectional Long Short-Term Memory (BiLSTM) networks. BiLSTM: get complex dependency and context; access sequences forward and backward.

For a sequence of user activities $X = (x_1, x_2, ..., x_T)$, the BiLSTM computes:

$$ht = LSTM(xt, ht−1)\ ht = LSTM(xt, ht+1)\ ht = [ht, ht]$$

The last hidden states are fed into all-to-all layers, which generate a user behavior profile. Any departure from a “profile” activates security warnings. The process of user behaviour profiling is described in Algorithm 2.

Algorithm 2: BiLSTM User Behavior Profiling

Input: User activity sequence X = (x_1, x_2, ..., x_t), BiLSTM model M, threshold δ Output: Anomaly score for current activity

- Extract sequence features: For each timestep t in X:
- Extract user ID, action type, resource accessed, timestamp
- Convert categorical features to embeddings
- Normalize numerical features
  Concatenate to form feature vector x_t
- Process sequence through BiLSTM:
  Forward pass: h_f = LSTM_forward(X)
  Backward pass: h_b = LSTM_backward(X)
  Concatenate: h = [h_f, h_b]
- Generate user profile vector p = FCN(h)
- Retrieve historical profile p_hist for user
- Calculate profile deviation: d = cosine_distance(p, p_hist)
- Update historical profile using exponential moving average: p_hist = α * p + (1-α) * p_hist
- Return d as anomaly score

3.3.Privacy-Preserving Federated Learning

For patient privacy and security models in healthcare institutions, we use a federated learning approach. Local models are trained locally and only updates to the model are shared, rather than having sensitive information centralized. Secure aggregation protocols are used to prevent that individual updates could be reverse engineered to expose PHI. The federated learning process follows Algorithm 3.

Algorithm 3: Privacy-Preserving Federated Learning

Input: Global model parameters θ, learning rate η, number of communication rounds T Output: Updated global model parameters θ [6 – 10]

- Initialize global model parameters θ_0
- For each round t = 1 to T:
  Select subset of healthcare institutions St
  For each institution k in St:
- Download global model θt-1
- Perform local training:
- $\theta_k t = \theta t\text{-}1 - \eta \nabla L(\theta t\text{-}1, D_k)$ // D_k is local data
- iii. Apply differential privacy mechanism: $\theta_k \tilde{} t = \theta_k t$ + noise
  Securely aggregate updates:
- $\theta t = \theta t\text{-}1 + (1/|St|) * \sum_{k \in St} (\theta_k \tilde{} t - \theta t\text{-}1)$
- Return θT

Secure aggregation protocol prevents one participating institution from knowing the training data or updates to the model of another, thus maintaining patient anonymity, but gaining from the collective knowledge[11 – 13].

3.4.HIPAA Compliance Verification Layer

A rule-based expert system continually ensures all security operations adhere to HIPAA requirements. It

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5298 - 5306
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0693

is a set of rules that are already defined and aligned with HIPAA provisions that will track any data access, processing, or transmission. Table 2 provides an overview of the major requirements of HIPAA and how they are related to system functions. As shown in Table 2 HIPAA Requirements and Corresponding System Features

Table 2 HIPAA Requirements and Corresponding System Features

HIPAA REQUIREMENT	SYSTEM FEATURE	IMPLEMENTATION
Access Control (§164.312(a) (1))	Role-based access with ML verification	BiLSTM user behavior models verify access patterns match role expectations
Audit Controls (§164.312(b))	Comprehensive logging with anomaly detection	All access events analyzed by VAE model; anomalies flagged for review
Integrity (§164.312(c)(1))	Checksum verification with tamper detection	ML models detect unauthorized modifications to data based on historical patterns
Person or Entity Authentication (§164.312(d))	Multi-factor authentication with behavioral biometrics	BiLSTM analyzes typing patterns and system interaction behaviors
Transmission Security (§164.312(e)(1))	End-to-end encryption with integrity verification	Quantum-resistant encryption with ML-based integrity checking
Risk Analysis (§164.308(a)(1) (ii)(A))	Continuous threat modeling	GAN-based simulations of potential vulnerabilities
Security Incident Procedures (§164.308(a)(6))	Automated incident response	Reinforcement learning determines optimal response to detected threats

4. Experimental Results

4.1.Dataset and Implementation

We tested HIPAA-Guard with a synthetic dataset, with access events corresponding to 2.3 million access events from five healthcare institutions over six months. The data consisted of real-life access scenarios representing different roles (physicians, nurses, administrative) and simulated attack scenarios based on known hacking incidents within the healthcare field.

Implementation details:

- VAE: 4 encoding layers (256, 128, 64, 32 neurons) with ReLU activation BiLSTM: 2 bidirectional layers with 128 units each

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5298 - 5306
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0693

- GAN: Generator with 4 transpose convolutional layers, discriminator with 4 convolutional layers
- Training: Adam optimizer, learning rate 0.001, batch size 128

4.2.Security Performance Evaluation

Table 3 shows a comparison of the performing of HIPAA-Guard with baseline security approaches about various measures.

Table 3 Security Performance Comparison

Security Approach	Detection Accuracy	False Positive Rate	False Negative Rate	Mean Time To Detect
Traditional Rule-Based	83.7%	8.2%	7.9%	42.6
Single ML Model	91.2%	5.3%	3.5%	15.2
Ensemble Methods	95.8%	2.9%	1.3%	8.7
HIPAA-Guard	99.3%	0.4%	0.3%	3.2

HIPAA-Guard outperformed all in terms of the minimisation of false positives (which can negatively affect healthcare operations) and false negatives (which are a security risk).

4.3.Performance Against Attack Vectors

We tested HIPAA-Guard against typical attack methods used when attacking healthcare systems. Table 4 shows the detection rates for different attacks.

Table 4 Attack Vector Detection Performance

ATTACK VECTOR	DESCRIPTION	DETECTION RATE
Credential Theft	Unauthorized use of legitimate credentials	99.7%
Insider Threats	Authorized users accessing inappropriate data	98.9%
Phishing Attacks	Social engineering to gain system access	99.5%
Ransomware	Malicious encryption of healthcare data	99.8%
API Vulnerabilities	Exploitation of insecure API endpoints	97.6%
Database Injection	SQL injection and similar attacks	99.9%
Zero-day Exploits	Previously unknown vulnerabilities	92.3%

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5298 - 5306
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0693

The relatively lower performance against zero-day exploits is a challenge that is shared by all security systems, but the adaptive learning capabilities of HIPAA-Guard allow it to readily detect and counter new attacks.

4.4.System Performance and Scalability

We evaluated the computational effect of HIPAA-Guard on the healthcare data system. Table 5 shows performance measures, As shown in Table 5 System Performance Metrics.

Table 5 System Performance Metrics

DEPLOYMENT SCENARIO	AVERAGE LATENCY	CPU UTILIZATI	MEMORY USAGE (GB)	TRANSACTIONS PER
Small Clinic (50 users)	12.3	6.2%	2.8	850
Medium Hospital (500	18.7	12.5%	8.3	3,250
Large Healthcare System (5,000+ users)	27.6	22.8%	24.6	12,800

The difference in the use of resources shows very good scalability properties, which makes HIPAA-Guard suitable for healthcare institutions of different sizes.

5. Hipaa Compliance Analysis

5.1.Technical Safeguards Alignment

HIPAA-Guard directly meets the Technical Safeguards required by the HIPAA Security Rule. Table 6 associates specific system capabilities with the HIPAA requirements.

Table 6 Technical Safeguards Implementation

HIPAA SAFEGUARD	HIPAA-GUARD IMPLEMENTATION	COMPLIANCE EVIDENCE
Access Control (§164.312(a))	ML-enhanced role-based access control	99.3% accuracy in identifying inappropriate access attempts
Audit Controls (§164.312(b))	Comprehensive logging with ML analysis	Complete audit trail with anomaly detection
Integrity Controls (§164.312(c))	Blockchain-based data integrity verification	Zero undetected tampering incidents in testing
Person/Entity Authentication (§164.312(d))	Multi-factor with behavioral verification	99.7% accuracy in user authentication
Transmission Security (§164.312(e))	Quantum-resistant encryption	No data exposure during simulated interception attempts

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 08 August 2026
Page No: 5298 - 5306
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0693

5.2.Administrative Safeguards Support

Administrative safeguards are policies and procedures; HIPAA-Guard adds technological assistance in effectively implementing the administrative requirements of HIPAA. Key features include:

- Risk Analysis: The GAN-based threat modeling component continuously simulates potential vulnerabilities, supporting ongoing risk assessment.
- Risk Management: Automated responses to detected threats help mitigate identified risks promptly.
- Sanction Policy: The system provides evidence for enforcing sanctions by documenting policy violations with high accuracy.
- Information System Activity Review: Advanced analytics and visualization tools facilitate the review of system activity.

5.3.Privacy Rule Considerations

HIPAA-Guard supports Privacy Rule compliance through:

- Minimum Necessary Principle: ML models learn appropriate access patterns for different roles, flagging access to information beyond what is necessary.
- Disclosure Tracking: All disclosures of PHI are automatically logged and classified.
- Patient Rights: The system facilitates tracking of patient consent and authorization.

Conclusion And Future Work

In this paper, a novel framework named HIPAA-Guard, which utilizes deep learning algorithms to improve healthcare data security while adhering to HIPAA compliance, was presented. Experimental results show that it works significantly better than the conventional security method with accuracy of 99.3% and very low false positive/false negative rate.

Key contributions include:

- A hybrid security system that integrates VAEs, GANs and BiLSTMs.
- Opportunities for security enhancements across institutions using a privacy-preserving federated learning approach
- Mechanisms for verifying compliance specific to HIPAA
- Detailed analysis of the overall performance, on different attacks vectors
- Future research directions include:
- Researching quantum-resistant cryptographic methods that are coupled with deep learning.
- Creating explainable AI elements to help security teams offer clear explanations for their decisions
- Expanding it to cover international healthcare data protection laws
- Investigating transfer learning approaches to improve detection of zero-day exploits

References

[1]. Office for Civil Rights. (2013). HIPAA administrative simplification: Regulation text. U.S. Department of Health and Human Services.

[2]. IBM Security. (2024). Cost of a data breach report 2024. Ponemon Institute.

[3]. Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). A survey of deep learning methods for cyber security. Information, 10(4), 122. https://doi.org/10.3390/info10040122

[4]. U.S. Department of Health and Human Services, Office for Civil Rights. (2023). HIPAA security rule guidance materials. https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

[5]. Marron, J. (2024). Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A cybersecurity resource guide (NIST Special Publication 800-66 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-66r2

[6]. Muzaffar, A., Ragab Hassan, H., Lones, M. A., & Zantout, H. (2022). An in-depth review of machine learning based Android malware detection. Computers & Security, 121, 102833. https://doi.org/10.1016/j.cose.2022.102833

[7]. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning

approach for intelligent intrusion detection system. IEEE Access, 7, 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334

[8]. Lin, Z., Shi, Y., & Xue, Z. (2022). IDSGAN: Generative adversarial networks for attack generation against intrusion detection. In Advances in knowledge discovery and data mining (pp. 79–91). Springer. https://doi.org/10.1007/978-3-031-05981-0_7

[9]. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (Vol. 54, pp. 1273–1282). Proceedings of Machine Learning Research.

[10]. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3–4), 211–407. https://doi.org/10.1561/0400000042

[11]. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 51(4), Article 79, 1–35. https://doi.org/10.1145/3214303

[12]. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97, 101966. https://doi.org/10.1016/j.cose.2020.101966

[13]. Jayabalan, M., & O'Daniel, T. (2016). Access control and privilege management in electronic health record: A systematic literature review. Journal of Medical Systems, 40(12), 261. https://doi.org/10.1007/s10916-016-0589-z