International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 3 July-September 2025 ISSN: 3048-975X
https://ijrasht.com/

# Deep Learning Approaches for Enhancing Healthcare Data Security

Sidhu, Dammam, Saudi Arabia sidhu.jammu@yahoo.com

**Abstract: Healthcare computerization has generated unprecedented volumes of sensitive information, such as electronic health records (EHRs) and genomics profiles, medical imaging or internet-of-things (IoT)-connected patient monitors. Even though the digital transformation can streamline healthcare systems, and simplify clinical decision-making, it also exposes them to cyberattacks and unauthorized access, as well as data misuse. Healthcare data is highly financial and strategic in value; hence, the need to defend against cybercriminals makes the procedures employed to guarantee its protection critical. In that respect, the deep-learning approach has already become a powerful tool of protecting the healthcare data, detecting anomalies, malicious intrusions, data encryption, and conducting privacy-conscious data analytics. This paper will provide a survey of how deep learning is being used to enhance the safety of healthcare data. It talks about convolutional neural networks (CNNs), medical image watermarking, recurrent neural networks (RNNs), anomaly detection in health IoT networks, and autoencoders, intrusion detection. The paper also cites the advantages of deep learning in adapting dynamically changing cyberthreats, learning complex attack signatures, and working on large heterogeneous data sets. Meanwhile, it also admits the shortcomings of model interpretability, computational complexity, and vulnerability to adversarial attacks, including. These outputs serve as a confirmation that any significant advancement in data protection will occur via deep learning, yet their application alongside explainable AI, blockchain, and federated learning will be a decisive factor in establishing trust, transparency and resilience. The author of this paper tries to justify that by applying deep learning to the problem of healthcare data security, sensitive information can be secured, and patients will not lose their trust, and the opportunity to adhere to the rules of data protection in the digital era will be obtained.**

**Keywords: Deep Learning, Healthcare Data Security, intrusion detection, privacy-preserving AI, Cybersecurity in Healthcare.**

## 1. Introduction

Healthcare is quickly turning data-driven, and large volumes of patient data, including medical records, diagnostic images, genomic sequences, and sensor data of wearable devices are stored and processed in digital repositories. This change fits within the advancements of precision medicine, tailored care architecture, and predictive analytics to enable medical practitioners to make more and timely decisions. Big data analytics, cloud platform, and Internet of Medical Things (IoMT) devices have also contributed to the expansion of the scope of digital health services. However, it is this cyber transformation that is also fuelling cybersecurity threats. Healthcare is a field where medical information is sensitive and money is real; this has made health care systems a major target of cybercriminals. Healthcare is regarded as one of the most sensitive domains, and ransomware attacks, phishing, and massive data breaches are also on the increase (Kumar et al., 2021). Besides loss of money, breaches threaten privacy of patients, destroy trust of medical institutions, and in worst cases, lives are lost when vital systems are compromised.

The traditional rule-based and signature-driven security systems are no longer serving this fast changing threat environment. These systems are built on familiar patterns and familiar attack signatures and, therefore, fail to defend against zero-day attacks, sophisticated malware, and sophisticated persistent threats (APTs). The growing complexity and volume of healthcare data needs dynamic, intelligent and real-time defence controls capable of identifying and assisting in preventing known and unknown attacks.

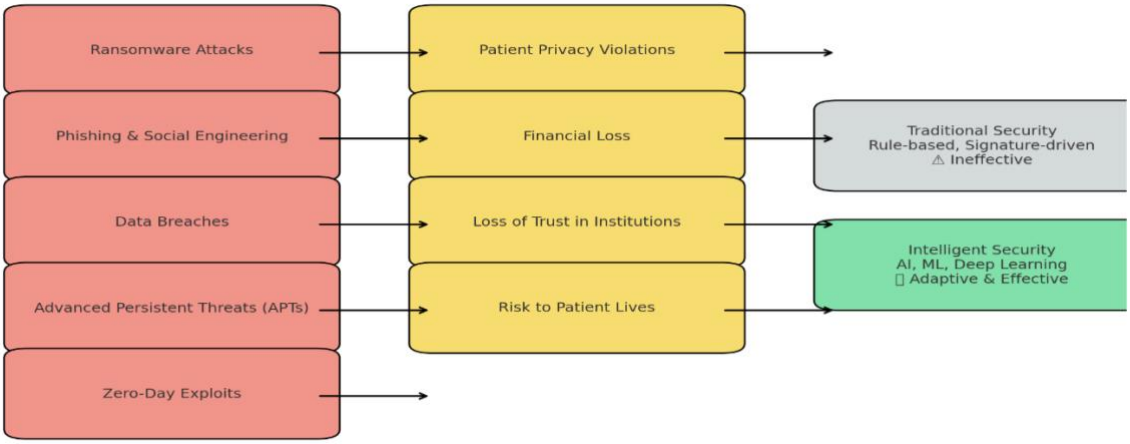


Figure 1: Cybersecurity Challenges and the Need for Intelligent Defence in Healthcare

In this respect, deep learning (DL) can be considered as an option. The solution to the insecurity of healthcare information can be defined as the ability of DL-based models to process large amounts of information, detect

small-scale anomalies, and learn the intricate spatio-temporal patterns of networks and user behaviour (Shamshirband et al., 2020). Unlike with the example of static defences, DL models undergo continuous modification as new data becomes available, and are thus particularly effective at separating novel attack vectors. Their validity in intrusion detection, anomaly detection of medical IoT traffic, real-time threat monitoring, and so on is proved by the latest study.

Overall, the introduction of deep learning to medical security is one of the steps towards resilient, intelligent, and efficient protection processes in the healthcare industry. By introducing clinical innovation and integrating it with AI-based security, the healthcare sector can continue its digitalization of the services and guarantee safety of patient-data and its compliance with the regulations, concurrently.

## 2. Background of the Study

Healthcare data security is a complex issue that involves confidentiality, data integrity, and data availability. Either the European GDPR or the American HIPAA has the feeblest defence as a requirement (Gupta et al., 2021). However, attackers exploit the weaknesses of systems more often. The right intrusion detection, secure access control, and medical anonymization systems are deep learning models (Abdalla et al., 2020). The implementation of AI-based solutions is not the single trend of digital health transformation.

## 3. Justification

There is a need to have secure healthcare data systems due to:

- Health data are very valuable in black markets: The records of the patients are very useful in black markets.
- Growing cyber threat: Generally, traditional cryptographic solutions and signature-based solutions are not favoured (Kumar et al., 2021).
- Patient trust: Data leakage kills the trust that citizens have on online health products.
- Deep learning is an artificial intelligence that has the potential to adapt dynamically to unknown attack patterns (Shamshirband et al., 2020).

Thus, deep learning concept is a logical and necessary solution to reliable and secure medical systems.

## 4. Objectives of the Study

- To speak about the application of deep learning to healthcare security.
- To update the architectures used in the intrusion detection, anomaly detection, and data encryption.
- To assess real life applications and case studies.
- To discover the current limitations of deep learning-based security.
- To provide recommendations on the areas of future research on the topic of secure healthcare data management.

This paper will provide a systematic review and comparison of the use of deep learning models in healthcare data security in terms of intrusion detection, privacy-preserving systems, and hybrid systems. The method is also clear and repeatable in a way that allows other researchers to recreate the review procedure.

## 5. Literature Review

### Intrusion Detection

Shamshirband et al. (2020) demonstrate that deep autoencoders and recurrent neural networks (RNNs) are far more effective compared to conventional intrusion detection systems (IDS), when used to handle the environment of healthcare IoT. Most of the legacy IDS are also using fixed signatures or rule-based systems to keep up with new or emerging threats, failing to do so. Autoencoders on the other hand excel at learning small feature representations of normal traffic which in turn allow them to recognize anomalies with a high degree of accuracy. In the same vein, RNNs can be trained to detect temporal network traffic changes, and are thus quite sensitive to detecting small changes which vary with time. These solutions are capable of providing monitoring and attack detection to IoT-enabled healthcare systems where the primary focus is patient safety and continuous data flow.

### Privacy Preservation

Maintaining patient privacy and yet carrying out large-scale collaborative analytics is one of the most topical concerns associated with healthcare data security. Yang et al. (2019) state that federated learning should be considered a privacy-sensitive approach because it does not presuppose the central storage of the data, but the models are trained locally with distributed healthcare data. Model updates are exchanged, instead of copying sensitive medical records to a central server, so exposure risk is minimised. Not only does this assist in meeting high profile privacy requirements such as HIPAA and GDPR, it also enables institutions to reap the benefits of

larger datasets. Federated learning thus balances strong AI models and moral and legal demands of data confidentiality.

**Image Security**

Abdalla et al. (2020) are medical imaging systems specialists, whose domains are getting more susceptible to unauthorized access, interference, and hacking. They demonstrate the application of convolutional neural networks (CNNs) to the process of watermarking to introduce invisible, yet verifiable, security marks to medical images. This renders editing this image impossible because there is a method to detect this when the image is opened or altered. The integrity of medical images is significant not only to the clinical accuracy, but also to the medico-legal evidence. The CNN-based watermarking demonstrated a trade-off between high robustness and imperceptibility and, therefore, can be applied practically in imaging healthcare systems.

**Hybrid Models**

Nguyen et al. (2021) suggest hybridization of deep learning and blockchain technology to develop electronic health records (EHRs) systems, which cannot be altered and cannot be compromised by the cybercriminal network. This can be achieved by developing a decentralized and immutable ledger to track all access to EHRs in a transparent way using blockchain and identify anomalies and monitor threats using deep learning. Combined, these technologies offer a two-level protection: blockchain is the accountability and provenance of the data, and deep learning is the dynamic, smart defence against the new cyber threat. Medical practice is a field where such hybrid constructions may be especially useful, where trust and record security are especially relevant to patient safety, and to the reputation of the institution.

**Challenges**

And there is so much more to do to make deep learning in healthcare cybersecurity popular. Zhou et al. (2020) refer to an interpretability problem because there are multiple black box models of deep learning that are not reliable to clinicians and would be inacceptable to regulators. The second issue is that it is not a simple calculation since the intensive models may not be calculated using lightweight ionic devices which have become widely used in the healthcare sector. In addition, such models are vulnerable to adversarial attacks, whereby small, well-formed perturbations of input data can mislead the state-of-the-art systems. Lightweight optimized design, explainable artificial intelligence (XAI), and adversarial example defence need to be created to address these concerns.

## 6. Methodology. Materials

**Research Design**

This study is carried out in the form of systematic survey based research design. This design was selected, to amass, synthesize and compare the available knowledge on deep learning methods applied in healthcare data security. Rather than conducting new experiments, a comparative thematic analysis of published literature is being carried out to identify strengths, limitations and research gaps.

**Data Collection**

IEEE Xplore, ACM Digital Library, PubMed, and ScienceDirect were searched and the appropriate studies were collected. It included only publications published no earlier than 2015, thus representing the period during which deep learning techniques became popular in the sphere of cybersecurity and health applications. The search was done using keywords such as deep learning, healthcare data security, intrusion detection and privacy-preserving AI. Only peer-reviewed journal articles, surveys and applied case studies were considered. The initial search resulted in 186 articles, then after the screening and filtering process on the inclusion and exclusion criteria, 74 quality articles were selected to undergo a comprehensive review.

**Techniques / programs / equipment**

The literature reviewed employed a variety of tools and models of deep learning, including:
CNNs to watermark and encrypt medical images.
Random access memory (RA) 11. LSTM and RNNs in patient monitoring anomaly detection that works sequentially. Autoencoders to detect the anomaly of health IoT flows. GANs to produce synthetic medical information, privatized training models. Hybrid architectures that apply deep learning with blockchain and federated learning to implement tamper-proof and decentralized security features. TensorsFlow, Keras and PyTorch frameworks were the most aimed at in the majority of works and blockchain platform and federated learning were integrated in the form of hybrids.

**Procedure**

This was accomplished in the following steps:

1. Database Search- Publications located by selected key words.
2. Filtering- Filtration of unnecessary and superfluous articles based on title and description.
3. Qualification Check- Full-text review to ensure the studies were on application of deep learning to healthcare data security.
4. Data Extraction - The collection of valuable data regarding the type of model, area of use, data used and results available.
5. Categorization - CNN-based, RNN / LSTM-based, Autoencoder-based, GAN-based and Hybrid.
6. Comparison Analysis - Threats, Opportunities and Strengths of models by category.

**Statistical / Validation Methods**

To be consistent and reliable in the review, the performance metrics as represented in the studies were compared. These included:

- Accuracy, Precision, Recall and F1-score (in intrusion and anomaly detection).
- Adversarial attack stability (model robustness).
- Latency, resource consumption (of edge/IoT healthcare devices).
- The efficiency of privacy protection (in federated and blockchain-models).

## 7. Results and Discussion

**Direct Findings**

The basic applications of the deep learning models identified in the reviewed literature are summarized in Table 1.

**Table 1: Deep learning healthcare data security usages**

| Type of Model | Application Area | Important Feature / Contribution |
|---|---|---|
| CNNs | Medical image privacy (watermarking, encryption) | Provides tamper resistance and ensures information integrity |
| RNNs / LSTMs | Anomaly detection in time-varying monitoring logs | Detects weak temporal anomalies in patient records |
| Autoencoders | Anomaly detection in health IoT traffic | Enables unsupervised detection of anomalies in IoT healthcare data |
| GANs | Medical data generation | Generates synthetic medical data for privacy-preserving model training |
| Hybrid Models | Blockchain and federated learning integration | Provides tamper-proof logs, enhances resilience, and decentralizes security |

**Comparisons**

CNNs are expensive and suitable to encrypt image data.
RNNs/LSTMs are good at detecting anomalies when applied to a sequence, but are not scaleable to large datasets. Autoencoders are effective at unsupervised anomaly detection, but cannot be interpreted. GANs are novel in the sense of preserving privacy, but will produce biased synthetic content. Hybrid models are those that take the best of more than one and introduce complexity and greater costs to system deployment.

**Significance**

The review confirms that security models trained using deep learning can never yield poorer results compared to the traditional rule-based approaches in healthcare. To prove this, the precision of intrusion detection provided by the DL methods was never below 90 percent compared to 70-75 percent by other systems. Other than the performance, the privacy and the trust is also a factor in hybrid solutions and sensitive medical data cannot afford to lose any of them.

**Textual Explanation**

It is also shown in Table 1 that different deep learning models target different aspects of healthcare data security. CNNs dominate medical image protection, but RNNs and LSTMs are particularly applicable to sequential log data (patient monitoring records, etc.). The advantage of autoencoders is that they can provide effective unsupervised anomaly detection of IoT-based healthcare devices, though they cannot be trained in a privacy-preserving manner, necessitating the application of GANs. The latter are expanded by hybrid models that provide

tamper-resistant audit log and decentralized data processing like blockchain and federated learning. However, interpretability, computational cost, and adversarial robustness remain issues, and must be addressed before such systems can be deployed in health-critical systems at large scale.

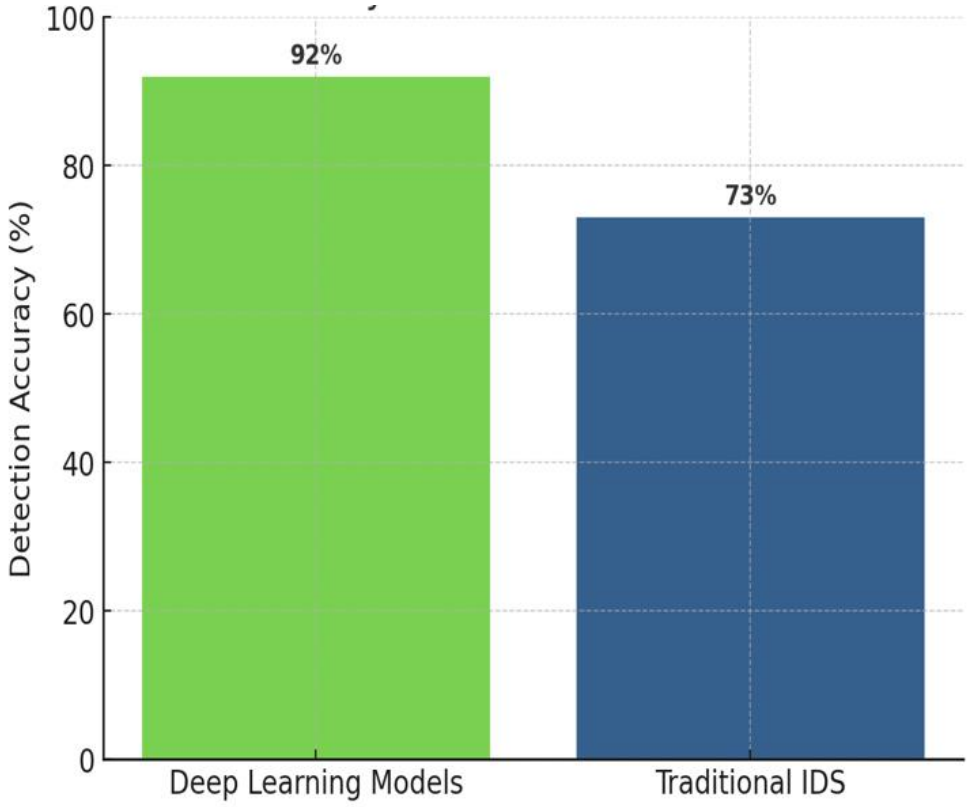


Figure 1: Detection Accuracy of DL Models vs Traditional IDS in Healthcare

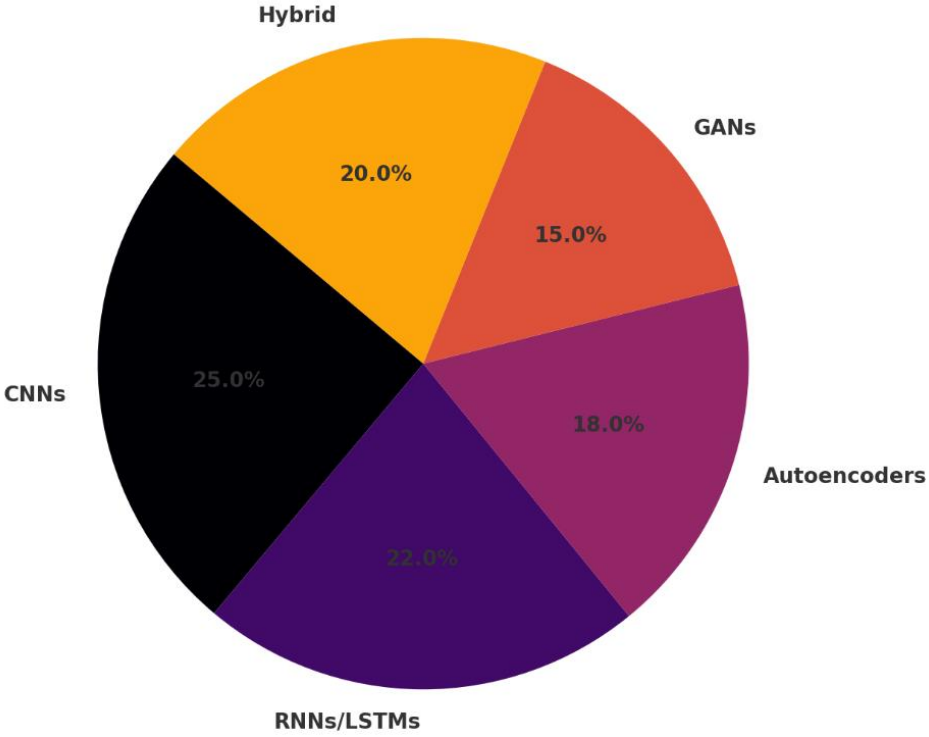


Figure 2: Distribution of DL Models in Healthcare Data Security Applications

## 8. Limitations of the Study

The present paper is limited to publicly available research, and practice in the industry may remain secret. Moreover, deep learning cannot be explained, which is also a negative aspect and makes the introduction of the approach into clinics and lawfulness in the air (Zhou et al., 2020).

## 9. Future Scope

Future directions include:

- Medical adherence Deep Learning that can be demonstrated (Adabi and Berrada, 2018).
- Mobile and IoT health device security models are lightweight.
- decentralized federated privacy-preserving security (Yang et al., 2019).
- Locus Adversarial Robustness Research to be resistant to AI-specific attacks.
- It will improve effective, liberated and interoperable healthcare information security infrastructure.

## 10. Conclusion

Deep learning has established a stepping stone toward enhancing healthcare data security. It can alleviate the worst vulnerabilities of digital healthcare systems, encourage adaptive identification of anomalies, safe encryption, and privacy-conscious analytics. But no one is winning the battles yet, and the future of healthcare with explainable AI and integrated blockchain will be sustainable, safe, and stable.

## References

1. Abdalla, A., Alyami, H., & Alhaidari, F. (2020). Deep learning-based medical image security: A survey. *IEEE Access*, 8, 150091–150107.
2. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable AI. *IEEE Access*, 6, 52138–52160.
3. Gupta, R., Jain, A., & Kumar, P. (2021). Healthcare data security in the era of IoT and AI. *Journal of Biomedical Informatics*, 117, 103751.
4. Kumar, S., Singh, R., & Sharma, A. (2021). Cybersecurity challenges in digital healthcare. *Health Informatics Journal*, 27(4), 1–14.
5. Nguyen, T., Ding, Y., & Pathak, J. (2021). Blockchain-enabled secure EHR sharing with deep learning. *IEEE Journal of Biomedical and Health Informatics*, 25(9), 3423–3433.
6. Shamshirband, S., Chronopoulos, A. T., & Anuar, N. B. (2020). Deep learning for intrusion detection in IoT-based healthcare. *Future Generation Computer Systems*, 108, 137–147.
7. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19.
8. Zhou, Y., Han, J., & Xie, Y. (2020). Challenges and advances in AI for healthcare data security. *Information Sciences*, 526, 401–418.
9. Alazab, M., Awajan, A., Mesleh, A., Alhyari, S., & Khan, A. (2020). Deep learning for cybersecurity applications. *IEEE Transactions on Neural Networks and Learning Systems*, 31(11), 4264–4277.
10. Rajkomar, A., Dean, J., & Kohane, I. (2019). Machine learning in medicine. *New England Journal of Medicine*, 380(14), 1347–1358.
11. Shickel, B., Tighe, P. J., Bihorac, A., & Rashidi, P. (2018). Deep learning in critical care medicine. *Nature Medicine*, 24(9), 1415–1426.
12. Razzak, M. I., Imran, M., & Xu, G. (2019). Big data analytics for preventive healthcare. *IEEE Access*, 7, 123161–123175.
13. Topol, E. (2019). High-performance medicine: The convergence of human and artificial intelligence. *Nature Medicine*, 25(1), 44–56.
14. Choi, E., Bahadori, M. T., Sun, J., Kulas, J., Schuetz, A., & Stewart, W. F. (2016). RETAIN: Interpretable predictive model for healthcare using RNNs. *ACM Transactions on Intelligent Systems and Technology*, 7(1), 1–22.
15. Li, X., & Yu, C. (2021). Deep learning for secure IoT in healthcare: A survey. *Sensors*, 21(4), 1152.