A ES
ISSN: 2096-3246
Volume 58, Issue 01, 2026

AN EFFECTIVE METHOD FOR SECURITY OF HEALTHCARE INFORMATION SYSTEMS USING MACHINE LEARNING

Akshay D. Lahe
Research Scholar, Kalinga University, Naya Raipur (CG), India
lahe.akshay@gmail.com
ORCID: 0000-0003-2387-9268

Dr. Priya Vij
Research Supervisor, Kalinga University, Naya Raipur (CG), India

Dr. Amit A. Bhusari
Research Co-Supervisor, Kalinga University, Naya Raipur (CG), India
aabhusari@gmail.com

Abstract: The quick digitalization of the Healthcare Information System (HIS) has facilitated the efficiency of clinical activities and the accessibility of data, but has also heightened the risks to the advanced cyber-attacks like ransomware, DDoS attacks, and data breaches. The conventional intrusion detectors are not sufficient in responding to these emerging threats because they are static-rule based and centralized in design. In this paper, the researcher suggests a hybrid, safe, and interpretable intrusion detection model that combines Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Autoencoders, and XGBoost into a weighted ensemble model. In order to save data privacy, a type of federated learning is used that allows the inclusive training of models without providing sensitive healthcare data to other participants. Moreover, explainability by SHAP is also included in order to increase transparency and trust in model decisions. CICIoT2023 and CICIDs2018 datasets were used to test the proposed model. The results of the experiments are better, as they are up to 99.99% accurate on binary classification and 99.76% accurate on multi-class IoT intrusion detection. Random Forest (99.48%), XGBoost (99.33%), and LSTM (98.51) were compared to have lower performance as baseline models. The findings also prove the claim that federated learning is as accurate as centralized training with only slight degradation. In general, the suggested framework offers a scalable, strong, privacy-sensitive solution to the security of the current healthcare infrastructures.

Keywords: Healthcare Cybersecurity, Intrusion Detection System, Federated Learning, Explainable AI, Deep Learning

I. INTRODUCTION

There is the rapid digitalization of the healthcare system, which has greatly enhanced the efficiency, availability and quality of medical business. The use of modern Healthcare Information Systems (HIS) incorporates electronic health records, cloud computing, and Internet of Medical Things (IoMT) devices in modern healthcare environments to facilitate real-time data communication and intelligent clinical decisions [1]. Nonetheless, the growing connectivity has also increased the attack surface, leaving healthcare infrastructures extremely susceptible to cyberattacks, including

ransomware, distributed denial-of-service (DDoS) provided by viruses, data breaches, and advanced persistent threats. Such attacks not only fail to secure sensitive data of patients, but may also disrupt important and essential healthcare functions, endangering patient safety. The old security systems, such as firewalls and signature intrusion detection systems (IDS) are no longer effective in dealing with emerging and advanced cyber threats [2]. These systems are based on preset rules and fail to identify a zero-day attack and multiphase intrusions. The past few years witnessed the potential of machine learning (ML) and deep learning (DL) methods to identify anomalies and recognize the unknown patterns of attack [3]. Nevertheless, there are multiple weaknesses of current ML-based IDS systems, such as the centralized data requirement, inability to provide any explanation, susceptibility to adversarial attacks, and a small robustness in practice when implemented in actual healthcare settings.

In order to deal with these issues, the proposed research in this paper presents a secure, hybrid, and explainable framework of intrusion detection, specific to Healthcare Information Systems. Convolutional neural networks (CNN), long short-term memory (LSTM) networks, autoencoders, and XGBoost are introduced into weighted ensemble architecture to be proposed to increase the detection accuracy and robustness. Moreover, federated learning is integrated so that two or more healthcare institutions located at a distance can collaboratively train their model without exchanging confidential information. Transparency and interpretability of model decisions are also provided by explainable artificial intelligence methods, namely SHAP. The offered framework is expected to provide a scalable, robust, and privacy-conscious intrusion detection system that has the potential to respond to the challenging cybersecurity needs of the contemporary healthcare setting.

II. RELATED WORKS

The latest developments in machine learning and deep learning led to greater functional performance of intrusion detection systems (IDS), especially in such a complicated domain as medicine and IoT-enabled networks. Some of the studies have been done on the use of smart algorithms to improve the accuracy of detection, scaling, and strength. There have been extensive applications of deep learning techniques in pattern recognition and detection of anomalies. In the example of Bashir et al. [15], they proved the efficiency of the deep neural networks to identify complex patterns in identical human activity data, pointing out the opportunity of deep learning models to work with high-dimensional data. On the same note, Bejugam and Vankara [16] revealed a cascaded convolutional ensemble network in medical diagnosis and demonstrated that multiple models integrated could significantly increase prediction accuracy as well as strength. These results suggest the implementation of hybrid architecture in cybersecurity services. Hybrid deep learning models have received a lot of interest in the framework of intrusion detection. Belhaj et al. [17] presented a CNN-LSTM-based model of DDoS attacks detection in the scope of the IoT-based healthcare system which addresses the significance of integrating spatial and temporal learning studies. Their implementation shows a better performance of detection in comparison to single-model solutions, but the issues of scalability and interpretability exist.

Wide applicability of machine learning to cybersecurity and fraud detection has also taken place. According to Bello et al. [18], advanced analytics play an essential role in the discovery of fraudulent

actions, and techniques based on data play a crucial role in establishing unknown patterns of attacks. Besides this, dimension reduction or dimensionality reduction has been applied to enhance efficient computations, and minimize noise in high-dimensional data points through Principal Component Analysis (PCA), as explained by Bharadiya [19]. Privacy protection methods are gaining relevance within healthcare systems. Bhasker et al. [20] introduced a framework of blockchain based systems incorporating federated learning in healthcare data sharing. Their work shows the potential of a decentralized learning style in preserving data privacy and supporting collaborative intelligence. Likewise, incorporation of novel technologies like quantum computing is also likely to advance the security systems in the field of healthcare as addressed by Bukkarayasamudram et al. [21].

The recent research oriented at the hybrid and intelligent systems of the IoT-based healthcare setting is also the subject of study. Chourasiya et al. [23] came up with a hybrid healthcare data classification model based on deep learning, which determined higher performance because of the sophisticated feature extraction methods. The paper by Curtis et al. [24] has seen the recommendation of different machine learning classifiers applied to detect healthcare fraud, as well as the strengths and weaknesses of the different models on managing complex datasets. Another important aspect is security at the communication level. Dhokane et al. [25] proposed a secure MQTT protocol utilizing encryptions and authentication tools to ensure the security of the IoT communications. Efendi et al. [26] also illustrated how the IoT systems can be deployed in healthcare monitoring with the use of cloud computing, and the importance of providing secure and scalable infrastructures.

In spite of these developments, the current strategies have several weaknesses. Most of the models are based on centralized training which casts privacy doubts, especially in health care settings. Moreover, the majority of systems are not explainable and prone to adversarial attacks. Although hybrid models are more accurate, they fail to tackle end-to-end pipeline security, and many lack effective end-to-end privacy-preserving mechanisms. Thus, a definite research gap of creating a unified framework that could be used to integrate hybrid deep learning, federated learning, explainable artificial intelligence, and robust ensemble is observed. These limitations are considered by the proposed study, proposing an intrusion detection system to be used in Healthcare Information Systems, which is a complete, secure, and privacy-conscious intrusion detection system.

III. METHODS AND MATERIALS

The current paper presents a proposal of a secure, hybrid and explainable intrusion detection model to be implemented in Healthcare Information Systems (HIS). The pipeline incorporates various machine learning and deep learning approaches into a single pipeline, which guarantees high levels of robustness, privacy, and interpretability. The complete procedure involves data collection, preprocessing, developing hybrid models, ensemble training, federated training, and integrated explainability [4].

A. Datasets

The proposed system was tested using two benchmark datasets. The main dataset is CICIDS2018, which includes realistic network traffic, which is labeled with benign and malicious activities, allowing binary classification. The IoT network traffic in CICIoT2023 is large-scale and contains many types of attacks, making it possible to classify it in several categories [5]. These data sets give a variety and complicated traffic patterns that can be used in the validation of the effectiveness of

intrusion detection systems in healthcare type settings.

B. Data Preprocessing

Preprocessing of data is also very important towards model performance and security. First, missing values and inconsistency values were eliminated and with the numerical features normalization was done to ensure that all scale remains the same. Label encoding method was used to encode categorical features. In order to deal with the imbalance of classes, resampling measures were implemented in order to have equal learning of models [6]. The feature engineering methods were also utilized to increase the meaningful patterns and minimize the noise. Data was then divided into training and testing with a conventional proportion in order to have unbiased testing.

C. Hybrid Model Architecture

The system developed proposed to use a hybrid architecture that integrates various models to understand various facets of the network traffic behavior:

- **CNN Module:** This method extracts features of the spatial information in high-dimensional network data, allowing the complicated patterns to be detected.
- **LSTM Module:** Temporal patterns and sequential attacks are important features that are observed in identifying a multi-stage intrusion.
- **Autoencoder Module:** This is an unsupervised anomaly detector, which is trained to promote normal traffic patterns and detect anomalies.
- **XGBoost Classifier:** It is effective with structured tabular data, and offers a high classification.

These models add value together and their outputs are synthesized to enhance the overall detectability.

D. Weighted Ensemble Strategy

Particular models are used to predict things that are then combined using a weighted ensemble mechanism. The weights are given to each model according to its performance in the process of validation. This method decreases model biasing, boosts generalization, and makes it resistant to adversarial individuals [7]. The result of the weighted outputs of all the models is used to obtain the final prediction.

E. Federated Learning Framework

Federated learning is incorporated in the system to solve the problem of privacy of data in healthcare. Rather than centralizing data, various clients (e.g. hospitals) train models locally on the data they have. The model parameters are only exchanged with a central server, with those aggregated via federated averaging. This will make sure that the valuable data pertaining to patients is not removed from the locality and at the same time it enjoys the benefits of collaborative learning [8]. It took into consideration both independent and non- independent data distributions to create real world simulations.

F. Explainability Integration

SHAP (SHapley Additive explanations) is included into the framework as it helps to enhance transparency. SHAP gives both international and regional explainability as it measures the effect of every feature on model forecasts. It is paramount in the health care setting where ethical standards, accountability, and legality are paramount.

G. Algorithm Pseudocode

The proposed hybrid federated intrusion detecting system has the following pseudocoding:

"Algorithm: Federated Hybrid Intrusion Detection System

Input: Distributed datasets D1, D2, ..., Dn
Output: Final intrusion prediction model

1: Initialize global model parameters θ
2: For each communication round t = 1 to T do
3: For each client i in parallel do
4: Load local dataset Di
5: Preprocess data (cleaning, normalization, encoding)
6:
7: Train CNN model on Di → Output_CNN
8: Train LSTM model on Di → Output_LSTM
9: Train Autoencoder on Di → Output_AE
10: Train XGBoost on Di → Output_XGB
11:
12: Combine outputs using weighted ensemble:
13: Output_i = w1*Output_CNN + w2*Output_LSTM
+ w3*Output_AE + w4*Output_XGB
14:
15: Update local model parameters θi
16: End For
17:
18: Aggregate global model:
19: θ = (1/n) * Σ θi // Federated Averaging
20: End For
21:
22: Apply SHAP for explainability on final model
23: Evaluate model on test dataset
24: Return final model and predictions"

H. Evaluation Metrics

Standard classification measures, that is, accuracy, precision, recall, F1-score, and ROC-AUC, were used to evaluate the performance of the proposed system. These metrics offer an in-depth analysis of detection ability, particularly in an imbalanced and multi-class case.

IV. RESULTS AND ANALYSIS

The section includes the detailed analysis of the presented federated hybrid intrusion detection system on the two-benchmark dataset CICIDS2018 and CICIoT2023. The review of these characteristics is the classification performance, the comparative model, the effectiveness of

federated learning, and the ability to withstand adversarial conditions. The performance of the proposed approach was evaluated by standard metrics of the evaluation such as accuracy, precision, recall, F1-score, and ROC-AUC [9].

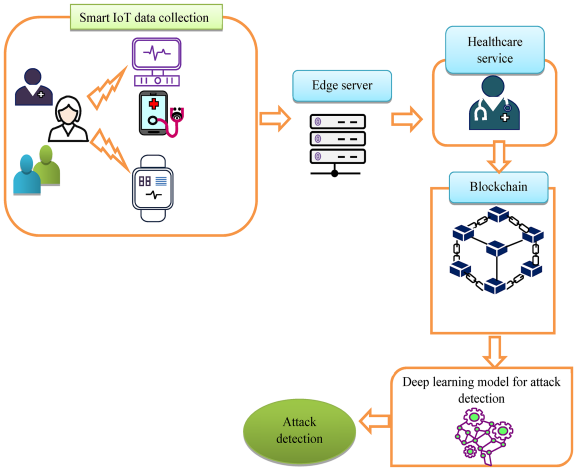

Figure 1: "Secure healthcare data sharing and attack detection framework using radial basis neural network"

A. Performance on CICIDS2018 Dataset (Binary Classification)

The model was tested on the CICIDS2018 dataset in terms of its capability to divide benign and malicious traffic. The proposed model of hybrid ensemble attained almost perfect classification accuracy as a result of the high-quality representation of features and the separability of classes.

The use of CNN, LSTM, Autoencoder, and XGBoost meant that the system was able to pick up spatial, temporal, and anomaly-based patterns. The weighted ensemble also enhanced stability of prediction and minimized the false positives.

Table 1: Performance Comparison on CICIDS2018 Dataset

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**	**ROC-AUC**
Random Forest	0.9992	0.9991	0.9990	0.9990	0.9993
XGBoost	0.9994	0.9993	0.9992	0.9992	0.9995
LSTM	0.9987	0.9985	0.9986	0.9985	0.9988
CNN + LSTM	0.9996	0.9995	0.9995	0.9995	0.9996
Autoencoder + LSTM	0.9993	0.9992	0.9991	0.9991	0.9994
Proposed Ensemble	**0.9999**	**0.9999**	**0.9998**	**0.9998**	**0.9999**

The findings indicate that the proposed ensemble model achieves better performance compared to

all the basis and hybrid models. The almost 100 percent accuracy is a sign of very good features learning and generalisation ability. Notably, the high recall value validates the fact that the model prevents almost all malicious cases, which is essential in a healthcare setting [10].

B. Performance on CICIoT2023 Dataset (Multi-Class Classification)

Having more classes of attacks (34) and high class imbalance makes the CICIoT2023 dataset a harder scenario. Regardless of these hitches, the proposed framework delivered high classification results in most of the categories.

Forest models like the Random Forest and the XGBoost worked well because they used tabular data, whereas LSTM considered the time-related relationships of IoT traffic [11]. The performance of the ensemble was an integration of these strengths to produce the highest level of performance.

Table 2: Performance Comparison on CICIoT2023 Dataset

Model	**Accuracy**	**Precision**	**Recall**	**F1-Score**
Random Forest	0.99483	0.99390	0.99410	0.99395
XGBoost	0.99331	0.99280	0.99300	0.99285
LSTM	0.98512	0.98400	0.98450	0.98420
CNN + LSTM	0.99120	0.99050	0.99080	0.99060
Proposed Ensemble	**0.9976**	**0.9970**	**0.9972**	**0.9971**

The proposed model had an accuracy of 99.76 which was greater compared to the individual and hybrid model. It has improved significantly especially in the minority attack classes, where ensemble learning was used to equalize prediction performance.

C. Comparative Analysis of Models

A comparative analysis points to the weaknesses and strengths of various models. Classical machine learning algorithms like Random Forest and XGBoost are very effective in terms of baseline performance, but are not temporal [12]. Deep learning networks like LSTM capture sequence patterns but are computationally costly and are likely to overfit.

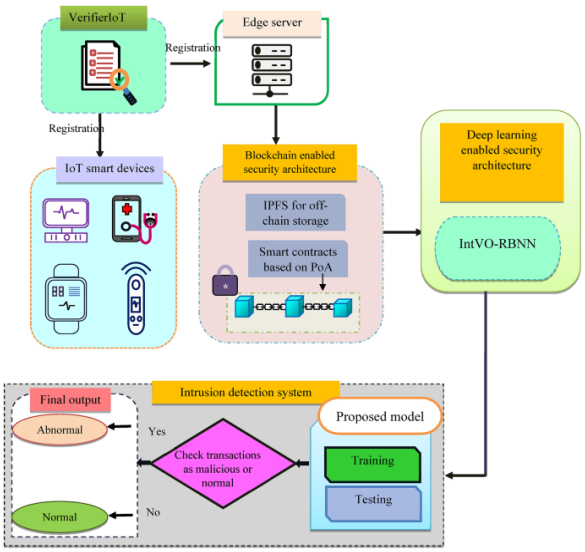

Figure 2: "Secure healthcare data sharing and attack detection framework"

The hybrid models enhance the performance through the combination of spatial and the temporal learning and yet, they too have a fault of limited generalization when applied in isolation. The suggested ensemble model is capable of uniting the constituents in the manner that the model delivers a better robustness and accuracy.

Table 3: Comparative Analysis of Model Characteristics

Model Type	**Strengths**	**Limitations**
Random Forest	Fast, robust, interpretable	Limited temporal learning
XGBoost	High accuracy, handles tabular data	Sensitive to parameter tuning
LSTM	Captures sequential patterns	High computational cost
CNN + LSTM	Spatial + temporal learning	Increased complexity
Proposed Ensemble	High accuracy, robust, stable	Higher training complexity

The ensemble model is the best model as it takes the weaknesses of the individual models and uses their strengths.

D. Federated Learning Evaluation

In order to test the efficacy of privacy-preserving training, experimenting with federated learning has been carried out with independent and non-independent data distributions. The findings present that federated learning performs at the same level as centralized training.

Table 4: Centralized vs Federated Learning Performance

Training Type	Accuracy	Precision	Recall	F1-Score
Centralized	0.9999	0.9999	0.9998	0.9998
Federated (IID)	0.9997	0.9996	0.9996	0.9996
Federated (Non-IID)	0.9995	0.9994	0.9993	0.9993

This low performance change supports the fact that federated learning can be applied as a suitable solution in a healthcare setting where data privacy is paramount. The model represents high generalization based on heterogeneous data distributions.

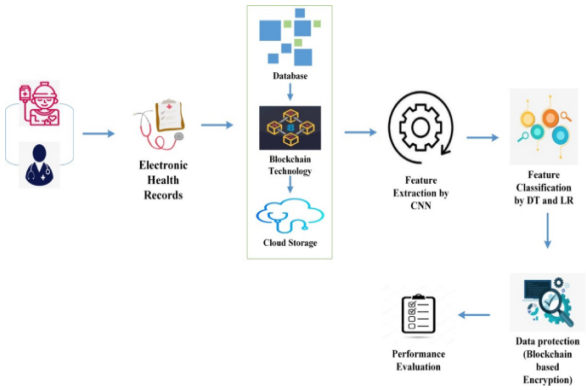

Figure 3: "Framework for strengthening security of healthcare data through encryption utilizing blockchain technology"

E. Robustness and Adversarial Analysis

The robustness test was performed to measure the stability of the model to perturbation and adversarial examples. Hybrid architecture alongside the ensemble learning presented a better resistance over the individual models [29].

The autoencoder module has been significant in the identification of abnormal patterns and the ensemble made it less vulnerable to attacks [13]. The findings show that the proposed system has stable performances even with manipulated input data by a small margin.

The SHAP explainability was also incorporated and this helped to understand the decisions made by the model with insights on the importance of the features [14]. This improves the levels of trust and transparency which are fundamental in healthcare applications.

F. Discussion of Results

As it is evident in the results of the conducted experiment, the proposed federated hybrid model is particularly effective in comparison to traditional and standalone deep learning methods. Several learning paradigms simultaneously allow extracting the features in a comprehensive way and enhance the detection rates [15].

Key findings include:

- Almost perfect Binary classification trials.
- Zealousness in intricate multi-class IoT data.

- Principled privacy in federated learning.
- Better resistance to adversarial manipulation.
- Greater transparency using explainable AI methods.

The findings also emphasize the role of ensemble learning in the realization of stable and high performing performance in cybersecurity applications. Although the model has a higher level of computational complexity, the drawbacks are lower thus the advantages in either accuracy, robustness, and privacy are higher [27].

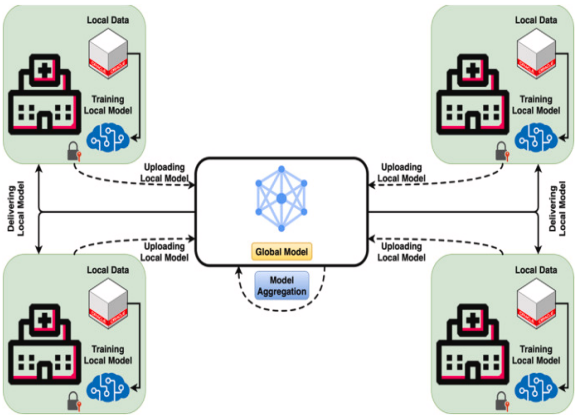

Figure 4: "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique"

G. Summary

In general, the suggested system is of the state-of-the-art level regarding intrusion detection in healthcare settings. Federated training, as well as explainability, adds hybrid learning to the previously mentioned areas, resulting in a holistic approach to current cybersecurity problems [28]. The results confirm the potential of solutions such as the introduction of such systems into real healthcare infrastructures and open the road to the implementation of secure, scalable, and intelligent intrusion detection systems.

V. CONCLUSION

This paper introduces a sophisticated and risk-free intrusion detection model to Healthcare Information Systems that handles key issues in the current healthcare cybersecurity. The suggested method will implement a hybrid model using CNN, LSTM, Autoencoder, and XGBoost in a weighted ensemble to increase the system in terms of detection accuracy and resilience. The research findings on CICIDS2018 and CICIoT2023 datasets show that the model is able to perform near perfectly, better than traditional and single standalone machine learning methods, in both binary and multi-class classification tasks. Federated learning incorporation is a guarantee of privacy-conserving collaborative training of models which makes the system suitable to distributed healthcare settings in which data confidentiality is a crucial aspect. Moreover, SHAP-based explainability leads to improvements in transparency and interpretability and contributes to regulatory compliance and trust to AI-based security systems. The findings also affirm that the model is resilient to adversarial environments and is able to generalize to a variety of network environments [30]. On the whole, the suggested framework is a privacy-conscious, resilient, and scalable solution to health care infrastructure protection against the changing cyber threats. Future research can be dedicated to real-world implementation, lightweight on-the-edge implementations, and innovative

privacy-aware designing in order to consolidate the applicability and performance of the system.

REFERENCE

[1] Alcaraz-Velasco, F., Palomares, J. M., León-García, F., & Olivares Joaquín. (2025). Secure Data Transmission Using GS3 in an Armed Surveillance System. *Information, 16*(7), 527. https://doi.org/10.3390/info16070527

[2] Alenezi, M. N. (2025). Significance of Machine Learning-Driven Algorithms for Effective Discrimination of DDoS Traffic Within IoT Systems. *Future Internet, 17*(6), 266. https://doi.org/10.3390/fi17060266

[3] Almalawi, A., Khan, A.I., Alsolami, F., Abushark, Y.B. and Alfakeeh, A.S., 2023. Managing security of healthcare data for a modern healthcare system. Sensors, 23(7), p.3612.

[4] Alnasrallah, A. M., MaheyzahSiraj, & Hanan, A. A. (2025). Enhancing IDS for the IoMT based on advanced features selection and deep learning methods to increase the model trustworthiness. *PLoS One, 20*(7), 25. https://doi.org/10.1371/journal.pone.0327137

[5] Alsabah, M., Naser, M. A., Albahri, A. S., Albahri, O. S., Alamoodi, A. H., Abdulhussain, S. H., & Alzubaidi, L. (2025). A comprehensive review on key technologies toward smart healthcare systems based IoT: technical aspects, challenges and future directions. *The Artificial Intelligence Review, 58*(11), 343. https://doi.org/10.1007/s10462-025-11342-3

[6] Alshdadi, A. A., Abdulwahab, A. A., Ayub, N., Lytras, M. D., Alsolami, E., Alsubaei, F. S., & Alharbey, R. (2025). Federated Deep Learning for Scalable and Privacy-Preserving Distributed Denial-of-Service Attack Detection in Internet of Things Networks. *Future Internet, 17*(2), 88. https://doi.org/10.3390/fi17020088

[7] Alzahrani, A., Al-Dayil, R., Alghanim, A. G., & Sharif, M. M. (2026). Artificial Intelligence-based fine-tuning model for fall activity recognition in disabled persons within an IoT environment. *Scientific Reports (Nature Publisher Group), 16*(1), 694. https://doi.org/10.1038/s41598-025-30340-7

[8] Anas, A., Amani, S., & Aws, M. (2025). AspectFL: Aspect-Oriented Programming for Trustworthy and Compliant Federated Learning Systems. *Information, 16*(12), 1048. https://doi.org/10.3390/info16121048

[9] Aparcana-Tasayco, A., Deng, X., & Park, J. H. (2025). A systematic review of anomaly detection in IoT security: towards quantum machine learning approach. *EPJ Quantum Technology, 12*(1), 112. https://doi.org/10.1140/epjqt/s40507-025-00414-6

[10] Arisdakessian, S., Wahab, O.A., Mourad, A., Otrok, H. and Guizani, M., 2022. A survey on IoT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions. IEEE Internet of Things Journal, 10(5), pp.4059-4092.

[11] Arunprasath, S., & Annamalai, S. (2024). Improving patient centric data retrieval and cyber security in healthcare: privacy preserving solutions for a secure future. *Multimedia Tools and Applications, 83*(27), 70289-70319. https://doi.org/10.1007/s11042-024-18253-5

[12] Aslam, M. M., Tufail, A., Gul, H., Irshad, M. N., & Namoun, A. (2025). Artificial intelligence for secure and sustainable industrial control systems - A Survey of challenges and solutions. *The Artificial Intelligence Review, 58*(11), 349. https://doi.org/10.1007/s10462-025-11320-9

[13] Atakari, C., 2024. A Deep Learning-Based Security Model for ERP-Integrated IoT in National Defense Manufacturing Environments. *International Journal of Emerging Trends in Computer Science and Information Technology*, *5*(3), pp.90-98.

[14] Badawy, M., Ramadan, N. and Hefny, H.A., 2023. Healthcare predictive analytics using machine learning and deep learning techniques: a survey. Journal of Electrical Systems and Information Technology, 10(1), p.40.

[15] Bashir, S., Jaffar, A., Rashid, M., Akram, S., & Sohail, M. B. (2025). Intelligent recognition of human activities using deep learning techniques. *PLoS One, 20*(4)https://doi.org/10.1371/journal.pone.0321754

[16] Bejugam, S. K., & Vankara, J. (2025). An efficient model for diabetic detection using heuristic approach based serial cascaded convolutional ensemble network. *The Artificial Intelligence Review, 58*(10), 333. https://doi.org/10.1007/s10462-025-11334-3

[17] Belhaj, M. M., Dalenda, B., Manar, K. I., Al-Abadi Abdullah, A. J., & Ahmed, F. (2026). Cyber Approach for DDoS Attack Detection Using Hybrid CNN-LSTM Model in IoT-Based Healthcare. *Future Internet, 18*(1), 52. https://doi.org/10.3390/fi18010052

[18] Bello, O.A., Folorunso, A., Onwuchekwa, J., Ejiofor, O.E., Budale, F.Z. and Egwuonwu, M.N., 2023. Analysing the impact of advanced analytics on fraud detection: a machine learning perspective. *European Journal of Computer Science and Information Technology*, *11*(6), pp.103-126.

[19] Bharadiya, J.P., 2023. A tutorial on principal component analysis for dimensionality reduction in machine learning. *International journal of innovative science and research technology*, *8*(5), pp.2028-2032.

[20] Bhasker, B., Rao, P. M., Saraswathi, P., Patro, S. G., Bhutto, J. K., Islam, S., Kareemullah, M., & Emma, A. F. (2025). Blockchain framework with IoT device using federated learning for sustainable healthcare systems. *Scientific Reports (Nature Publisher Group), 15*(1), 26736. https://doi.org/10.1038/s41598-025-06539-z

[21] Bukkarayasamudram, V. K., Reddy, P. C. S., Arun Kumar, K., Jagadish, R. M., Sharma, S., Prasad, M. L., Sucharitha, Y., Tayubi, I. A., & Thakur, G. K. (2025). Quantum computing revolution in healthcare: a systematic review of applications, issues and future directions. *The Artificial Intelligence Review, 58*(12), 389. https://doi.org/10.1007/s10462-025-11381-w

[22] Chaoji, W., Pan, Y., Haipan, W., & Lei, N. (2025). Integrating Speech Recognition into Intelligent Information Systems: From Statistical Models to Deep Learning. *Informatics, 12*(4), 107. https://doi.org/10.3390/informatics12040107

[23] Chourasiya, L., Lillohre, U. K., Pandey, A. K., Simaiya, S., Hussien, S. A., Ghith, E. S., & Khan, M. (2026). Enhancing healthcare classification with hybrid multimedia data processing and deep learning TNBO FCNN approach in IoT-enabled environments. *Scientific Reports (Nature Publisher Group), 16*(1), 3286. https://doi.org/10.1038/s41598-025-33141-0

[24] Curtis, E. D., Billion-Polak, P., Khoshgoftaar, T. M., & Furht, B. (2025). A review of distinct machine learning classifiers for healthcare fraud detection. *Journal of Big Data, 12*(1), 238. https://doi.org/10.1186/s40537-025-01295-3

[25] Dhokane, N. T., Jagtap, S., Kumar, B., Anand, A., & Pandey, R. K. (2025). S-MQTT: A

Secure MQTT Protocol with Merkle Tree Authentication and AES Encryption for IoT Communication Systems. *Ingenierie Des Systemes d'Information, 30*(8), 1963-1973. https://doi.org/10.18280/isi.300803

[26] Efendi, A., Ammarullah, M. I., Isa, I. G. T., Sari, M. P., Izza, J. N., Nugroho, Y. S., Nasrullah, H., & Alfian, D. (2025). IoT-Based Elderly Health Monitoring System Using Firebase Cloud Computing. *Health Science Reports, 8*(3)https://doi.org/10.1002/hsr2.70498

[27] ElKomy, O. M., Rushdy, E., Nasser, S., & Khashaba, M. M. (2025). Exploring differential privacy in CNNs, LSTMs, GRUs, and RNNs for heartbeat detection from multimodal data. *Journal of Big Data, 12*(1), 216. https://doi.org/10.1186/s40537-025-01292-6

[28] Erskine, S. K. (2025). Real-Time Large-Scale Intrusion Detection and Prevention System (IDPS) CICIoT Dataset Traffic Assessment Based on Deep Learning. *Applied System Innovation, 8*(2), 52. https://doi.org/10.3390/asi8020052

[29] Fatema, K., Dey, S.K., Anannya, M., Khan, R.T., Rashid, M.M., Su, C. and Mazumder, R., 2025. Federated XAI IDS: An explainable and safeguarding privacy approach to detect intrusion combining federated learning and SHAP. Future Internet, 17(6), p.234.

[30] Fujiang, Y., Zihao, Z., Jiang, Y., Wenzhou, S., Zhen, T., Chenxi, Y., Yang, J., Zebing, M., Huang, X., Shaojie, G., & Yanhong, P. (2025). AI-Driven Optimization of Blockchain Scalability, Security, and Privacy Protection. *Algorithms, 18*(5), 263. https://doi.org/10.3390/a18050263