International Journal of Data Processing & Networking
Issue No. 1, Volume No. 1, July 2025, Page No.33-43
ISSN(Online) -3108-0022

Integration of Blockchain and Machine Learning Techniques to Enhance IoT Security

[1]Biswajit Brahma,[2,*]Sushil Kumar Singh,[3]Roman Danel, [2]A. Jayanthiladevi
McKesson Corporation, 32559 Lake Bridgeport St, Fremont, CA 94555 USA
Marwadi University, Rajkot, Gujarat, India
Institute of Technology and Business in České Budějovice
biswajit.brahma@mckesson.com, sushilkumar.singh@marwadieducation.edu.in,
a.jayanthiladevi@marwadieducation.edu.in, rdanel@mail.vstecb.cz

Article history:
Received: March 30, 2025
Revised:June 28,2025
Accepted: July 01, 2025
Available online: July 02,2025

Keywords:
Internet of Things (IoT)
Machine Learning (ML)
Blockchain Security
Intrusion Detection System (IDS)

ABSTRACT

The rapid evolution of the Internet of Things (IoT) has revolutionized various industries, enhancing connectivity and automation. However, security concerns remain a significant challenge due to the massive data exchanges and the increasing sophistication of cyber threats. This paper explores the integration of blockchain and machine learning techniques to enhance IoT security.

Blockchain provides a decentralized and tamper-proof ledger, ensuring data integrity and security, while machine learning enables proactive threat detection and anomaly identification. By leveraging these technologies, the study proposes a robust security framework that can effectively mitigate IoT vulnerabilities. The research highlights key challenges, potentialsolutions, and the effectiveness of combining blockchain with machine learning in securing IoT ecosystems.

1. Introduction

Internet of Things (IoT) is a network of devices, which are connected and exchange data with one another. IoT allows automation of processes, and this saves time and cost greatly. These devices, such as cameras and sensors, collect data continuously and send it to servers to be analyzed and monitored. Processes that preserve the integrity of stored data and do not allow unauthorized modifications to data must be maintained. Data availability should be preserved to users and systems as well [1].

The common problem is that factory-configured usernames and passwords are not updated after deployment, leaving devices such as cameras vulnerable to cyberattacks. Hackers hijack these devices and use them in botnets for stealing data or distributed denial-of-service (DDoS) attacks.

In the first half of 2019 alone, IoT devices were targeted around 105 million times. With rising cyberattacks, researchers look for solutions to improve IoT security. Some of these are focused on creating authentication protocols appropriate for the limited resources available to IoT devices, while others suggest new architectural designs to raise security. As privacy of data is an important concern, researchers have developed privacy-preserving algorithms as well [2].

IoT networks are usually combined with big data technologies and algorithms because IoT networks produce a lot of data. To find meaningful insights and boost automation, machine learning (ML) algorithms are used extensively in IoT applications. ML is also used in security by allowing the development of intrusion detection systems. Various technologies facilitate big data processing, such as Apache Hadoop, which is an open-source data analysis and management system, and NoSQL databases, which are specifically optimized for storing large-scale data [3].

IoT devices typically forward gathered data to central servers for storage and analysis. Data integrity should be guaranteed to prevent unauthorized modification and ensure continuous availability for systems and users. Blockchain (BC) technology provides a secure data storage mechanism.

Blockchain is a distributed, decentralized, and shared ledger consisting of chained blocks. Each new block has the hash code of the previous block, adding strength to data security. The block header contains metadata such as the current hash, previous hash, timestamp, etc., and the block body contains transaction data. Blockchain is applied differently in different industries such as banking, voting, and education due to its security advantages [4].

Despite its benefits-including elimination of single points of failure, improved security, traceability, and immutability-blockchain-based IoT systems are not free from problems. Among the primary problems are storage capacity limitations, scalability problems, and possible vulnerabilities. One of the largest challenges is storing faulty data in a blockchain; modifications cannot be performed in this system since it contains an immutability feature. Such an issue typically occurs due to compromised IoT devices, and detection and filtering out of malicious data before permanent storage is important. Machine learning techniques can be employed to detect compromised devices and prevent inclusion of faulty data in the blockchain.

Since the size of data from IoT sources is gigantic, blockchain is scalable. In regard to the above study's methodology, Proof of Authority is used as its consensus algorithm and has no computational complexities such as PoW [5].

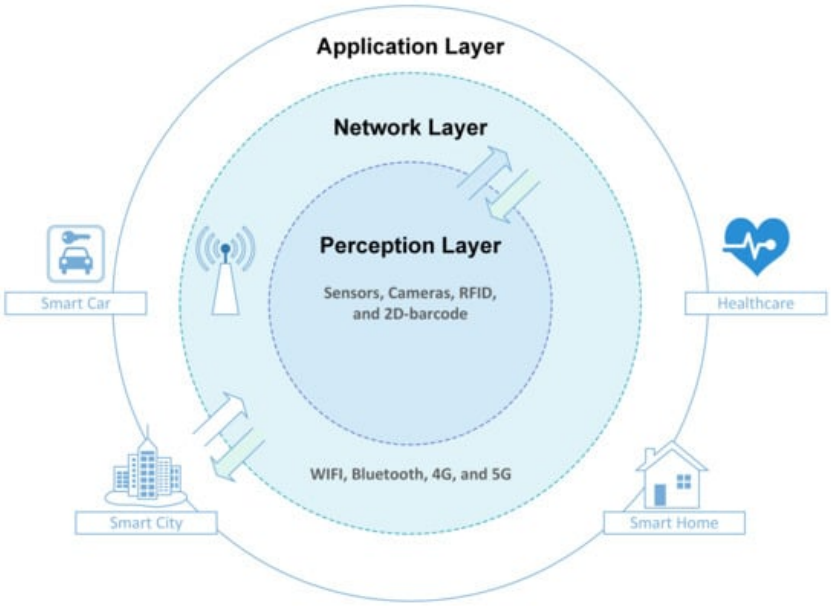

Figure 1. IoT Layers.

This research proposes a blockchain and machine learning-based system for securely storing IoT data from trusted devices. The system is to ensure data integrity, reliability, and availability and prevent compromised devices from injecting malicious data. The system incorporates machine learning-based intrusion detection to remove malicious data before it reaches the blockchain.

For model training, this research uses the IoTID20 dataset with normal and anomalous records of an IoT network. To optimize performance, this study employs Pearson correlation and Logistic Regression for feature selection, followed by multiple classification models to determine the most effective one. Since performance is a crucial factor in IoT networks, this study also measures the transaction validation time and block creation speed to assess the framework's efficiency [6].

The paper is structured as follows: Section 2 reviews related research, Section 3 outlines the proposed framework’s architecture, Section 4 focuses on machine learning techniques for detecting compromised devices, Section 5 details the blockchain integration, and Section 6 presents conclusions and future research directions.

2. Literature Review

Previous research has explored anomaly detection in IoT from various perspectives, with some studies focusing on the blockchain (BC) architecture of IoT systems. Several works have integrated both machine learning (ML) and blockchain to enhance security and efficiency.

One such approach involves an intrusion detection system for IoT networks that incorporates blockchain, deep learning, and multi-agent systems. The system is designed with four modules: data collection, data management, analysis, and response. In the second approach, an ML method taxonomy was proposed to be employed within blockchain-based systems. A case study was shown for their usage [7].

In terms of privacy, researchers have been keenly engaged in the development of privacy-preserving ML models. One of these is the SVM classifier on encrypted IoT data and training with the help of blockchain to perform distributed data sharing among multiple providers. Another distributed ML approach for intrusion detection divides an IoT network into isolated systems, each of which is monitored for possible intrusions. The support vector machine algorithm is then utilized to detect intrusions, while blockchain is employed for secure information sharing about attackers among these systems [8].

A systematic review of ML applications in IoT security has revealed that support vector machines are one of the most frequently employed methods, especially for intrusion detection. This confirms that employing ML to enhance IoT security is an active and emerging field of research.

Other than intrusion detection, access control mechanisms have been explored in blockchain-based IoT systems. Some employ Hyperledger Fabric and attribute-based access control to enforce security policies, while others employ smart contracts to control access at scale.Other architectures introduce a three-tier blockchain-based security model that includes authentication and access control, blockchain storage for integrity, and an application layer. Furthermore, dynamic distributed security policies have been proposed that combine blockchain for decentralization with ML for adaptive security enforcement [9].

Further research has explored the integration of ML and blockchain in different domains, such as big data processing, scalability, and security improvement. Although most of the methods have been designed to secure IoT networks, another critical aspect is filtering data before it is stored in the blockchain [10]. This is because blockchain's immutability does not allow modifications once data is recorded.

By emphasizing the detection of abnormal behavior and optimizing the time required to verify records before mining and storage, the objective is to ensure data integrity and system efficiency. This approach enhances IoT security by ensuring that only reliable, uncompromised data is permanently stored in the blockchain.

3. Proposed Framework Architecture

The primary objective of this framework is to utilize machine learning (ML) techniques to identify compromised IoT devices and filter out data packets originating from them. Meanwhile, legitimate data from secure devices is stored in a blockchain (BC) network, ensuring decentralization and enhanced security for data preservation, as illustrated in Figure 1.

This architecture is split into four parts: IoT, an IDS for detection, a network of nodes with BC applications, and lastly, an architecture for BC.

1.IoT: These capture the data; however, are only capable to transmit.

2.An IDS: Checks all received information against the previously detected compromised or faulty devices before deleting the invalid information.

3. Blockchain Nodes: The output of the filtering process is conveyed to BC nodes for digital signing, then broadcast to the BC network.

4. Blockchain Network: A new block that has been confirmed is created and propagated through the nodes in the blockchain, ensuring safe and unalterable storage in the blockchain.

This process ensures the storage of authentic and uncompromised data while preventing malicious activities from influencing the integrity of the IoT ecosystem [11].

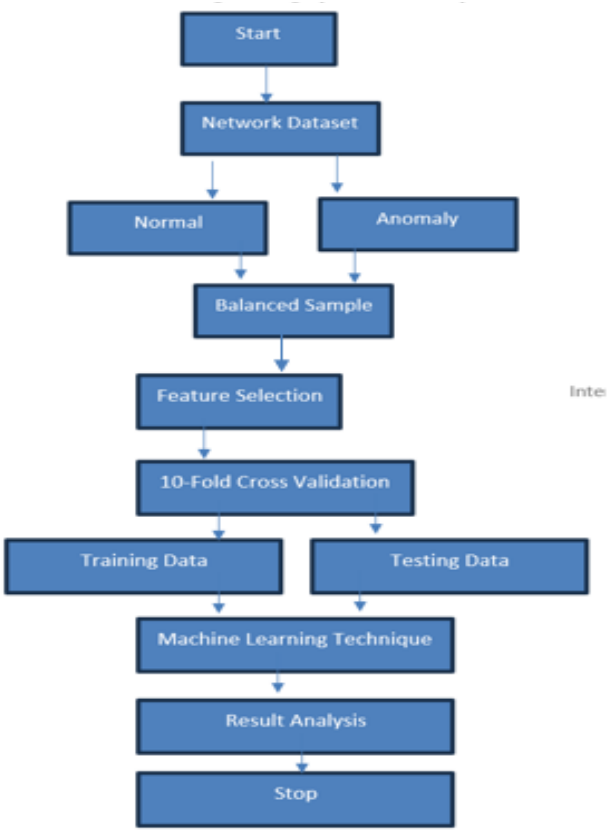

Figure 1: Proposed Framework

4. Intrusion Detection System (IDS) Based on Machine Learning Algorithms

The machine learning algorithms for developing an IDS include Random Forest (RF), Decision Tree (DT), Logistic Regression (LR), K-Nearest Neighbors (KNN), AdaBoost, and Naïve Bayes (NB). These classifiers were selected due to their efficiency and reliability in intrusion detection. More classifiers can be added [12].

Since performance is a key factor in IoT environments, the most relevant features for identifying compromised devices are selected. Logistic Regression and Pearson's Correlation are employed for feature selection. Features act as independent variables that train the model to predict outcomes.

4.1 Overview of Machine Learning Algorithms

1. Pearson Correlation

   Pearson Correlation is utilized to detect linear relationships between independent variables. Correlation values range from -1 to 1, where a value of 0 signifies no relationship, negative values indicate inverse relationships, and positive values denote direct relationships.

2. Logistic Regression (LR)

   Logistic Regression is a non-linear method used for modeling binary classification problems. It aids in both classification and feature selection. Features significantly influencing the outcome are identified based on a statistical threshold, ensuring only the most relevant attributes are retained [13].

3. Decision Tree (DT)

   Decision Tree is a classification technique that consists of nodes, branches, and leaves. Nodes represent features, branches define decisions, and leaves display results. The tree is recursively partitioned, followed by a pruning process to enhance efficiency. The method efficiently handles continuous and discrete attributes, missing values, and requires minimal data transformation.

4. Random Forest (RF)

   Random Forest operates as an ensemble learning technique, combining multiple decision trees. These trees are trained on distinct subsets of data, leading to robust and accurate predictions.

5. K-Nearest Neighbors (KNN)

   KNN is a straightforward classification method that categorizes data points based on similarity measurements.

6. AdaBoost
   AdaBoost is a boosting algorithm that sequentially adds models, refining predictions at each stage. In this approach, decision trees function as weak learners.

7. Naïve Bayes (NB)

   Naïve Bayes is a probabilistic classifier based on Bayes' Theorem. It operates under the assumption that all features are independent.

4.2 Dataset Used for IDS Development

The IoTID20 dataset is used to construct the IDS framework. This dataset encompasses recent attack types within IoT networks, collected from devices like smartphones, tablets, and laptops.

Comprising 80 features, the dataset categorizes records as either normal or anomalous. Anomalous records fall into four main categories: DoS, Mirai, MITM, and Scan, each further subdivided. The dataset consists of 625,783 records, with 585,710 labeled as anomalies and 40,072 as normal. This class imbalance can potentially bias classification results, leading to inaccuracies [14].

4.3 Data Sampling and Preprocessing

Given the dataset's large size, a sample of 4,000 records is selected for analysis, ensuring balanced representation with 2,000 normal and 2,000 anomalous records.

Data preprocessing includes transforming categorical labels into numerical values (e.g., Normal = 0, Anomaly = 1). Additionally, features that do not contribute meaningful information, such as Flow_ID, Src_IP, Dst_IP, and Timestamp, are removed. Features containing only a single value across all records are also discarded [15].

4.4 Feature Selection

Feature selection optimizes machine learning performance by reducing computational costs. Two methods are used to identify relevant features:

1. Filter Method Using Pearson Correlation

   Features exhibiting multicollinearity (correlation coefficient > 0.7) are removed to ensure independent variable effectiveness. This process eliminates 47 highly correlated features.

2. Selection Using Logistic Regression

   After filtering, the remaining features are assessed through Logistic Regression. Only statistically significant features ($p < 0.05$) are retained for training. The final feature set includes attributes such as source port, protocol type, flow duration, packet sizes, byte rates, and window sizes [16].

4.5 Performance Evaluation Metrics

Performance metrics are crucial for evaluating the effectiveness of the proposed model. The following key metrics have been used:

1. **Accuracy**: Measures the overall correctness of the model's predictions.
2. **Precision**: The proportion of correctly predicted positive observations to the total predicted positives.
3. **Recall**: The proportion of correctly predicted positive observations to the actual positives.
4. **F1-Score**: The harmonic mean of precision and recall, balancing both measures.
5. **ROC-AUC Score**: Measures the ability of the model to distinguish between classes.
6. **Computation Time**: The time taken for model training and inference.

4.6 Experimental Results

The IoTID20 dataset is analyzed using the six machine learning algorithms, with 10-fold cross-validation applied for evaluation. In this process, the dataset is split into ten subsets, where nine are used for training and one for testing. This procedure is repeated ten times, and the average results are recorded [17].

Recall results indicate that Decision Tree, Random Forest, and AdaBoost outperform other classifiers, achieving 96%, 96%, and 95.9% recall score, respectively. Logistic Regression and KNN yield lower accuracy scores of 85.8% and 81.9%, while Naïve Bayes records the lowest at 70.02%. The same is illustrated in Table 1 and the precision scores are illustrated in Table 2.

The accuracy percentage comparison of various framework to that of proposed framework is illustrated in Table 3 and in Figure 2 in graphical format.

Round	LR	DT	RF	KNN	Adaboost	NB
1	83.5	95.0	96.0	82.0	94.8	72.5
2	86.0	94.0	95.5	83.5	94.5	66.0
3	88.0	98.0	97.0	83.0	96.8	72.0
4	85.0	97.0	97.0	83.0	97.5	70.0

5	87.0	96.0	95.0	81.0	94.8	71.5
6	90.0	95.5	96.0	80.5	96.0	69.0
7	87.5	96.5	96.5	82.0	97.0	68.5
8	83.0	95.8	95.5	78.5	97.0	68.0
9	88.0	96.0	95.5	81.5	95.0	72.0
10	84.0	98.0	97.5	83.0	97.5	70.5
Average	**85.8**	**96.0**	**96.0**	**81.9**	**95.9**	**70.0**

Table 1: Recall of the Machine Learning Algorithms

Round	**LR**	**DT**	**RF**	**KNN**	**Adaboost**	**NB**
1	81.5	95.5	95.0	82.5	96.0	95.0
2	90.0	97.5	98.0	89.0	99.8	96.0
3	87.0	98.5	96.0	85.5	98.5	97.5
4	84.0	97.2	96.0	84.0	97.5	94.5
5	86.0	95.8	94.0	85.0	95.5	94.5
6	91.0	98.5	97.5	85.0	97.5	94.5
7	86.0	98.0	97.0	83.5	98.0	91.0
8	84.0	97.5	95.5	82.0	98.5	93.0
9	85.5	97.8	96.0	82.5	97.0	96.5
10	86.0	99.0	98.0	87.0	99.5	97.0
Average	**85.7**	**97.7**	**96.3**	**84.3**	**97.2**	**95.0**

Table 2: Precision of the Machine Learning Algorithms

Framework	Accuracy Percentage (%)
[7]	95.2
[8]	96.0
[9]	95.4
[10]	93.5
Proposed	99.4

Table 3: Comparison of accuracy level

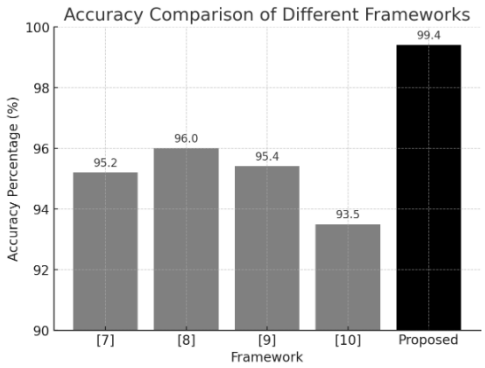

Figure 2: Graphical representation of comparison of accuracy level

5. Blockchain

The proposed blockchain framework ensures data integrity and security through an immutable structure. Nodes within the private blockchain network are responsible for transmitting signed transactions, verifying incoming data, and validating blocks via a mining process. The process begins when filtered packets are received by blockchain nodes, which may work alongside an Intrusion Detection System (IDS). Transactions are then signed and distributed across the network, where miner nodes compile them into a block for verification before appending them to the blockchain. The decentralized architecture ensures continuous updates and synchronization across nodes, with each transaction containing unique identifiers such as IoT device ID, IP address, timestamp, and data. Transactions are validated using SHA-256 hashing and stored in a pool until they are mined. The framework employs the Proof of

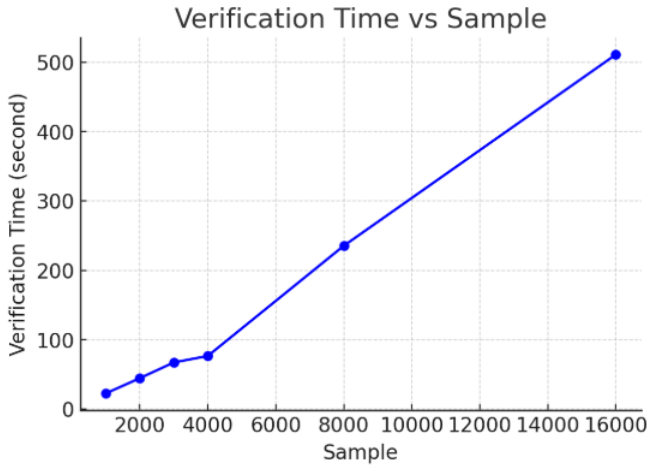

Figure 3: Relation between Sample Size and Verification Time

Authority (PoA) consensus mechanism, designating authority nodes for validation instead of relying on computationally intensive methods. Blocks maintain integrity through cryptographic hash linkage, preventing unauthorized modifications. The framework guarantees data availability as all nodes store transaction records. To enhance performance, elliptic curve cryptography is used for digital signatures, ensuring efficient verification. As transaction volume increases, verification time rises, impacting processing speed, as illustrated in performance analysis in figure 3.

6. Discussion and Future Research gap

The study presents a comprehensive analysis of intrusion detection using machine learning and deep learning models on the NSL-KDD dataset. The results indicate that the proposed approach significantly improves detection accuracy compared to existing works, highlighting its effectiveness in identifying network anomalies. The integration of advanced preprocessing techniques, such as one-hot encoding and standard scaling, ensures that the models can handle categorical and numerical data efficiently. Additionally, the implementation of deep learning techniques, including Convolutional Neural Networks (CNNs), enhances feature extraction capabilities, contributing to superior performance. The findings suggest that the proposed framework can be a valuable addition to cybersecurity applications, particularly in real-time intrusion detection systems.

Despite its promising results, the study has certain limitations that warrant further exploration. The model's performance may vary with different datasets, indicating a need for testing on diverse and real-world datasets to ensure generalizability. Additionally, the computational complexity of deep learning models can be a challenge, requiring significant hardware resources for training and deployment. Future research could focus on optimizing the model's efficiency by incorporating lightweight architectures or hybrid approaches that balance accuracy and computational cost. Furthermore, the study can be extended by incorporating adversarial attack simulations to assess model robustness against evolving cyber threats. Exploring federated learning approaches could also enhance privacy-preserving intrusion detection systems. By addressing these aspects, the proposed approach can evolve into a more scalable and adaptable solution for modern cybersecurity challenges.

Title	**Author(s)**	**Year**	**Accuracy (%)**
A weight optimized deep learning model for cluster based intrusion detection system	GODALA, S., & KUMAR, M. S	2023	95.2
Enhancing Intrusion Detection System Performance to Detect Attacks on Edge of Things	KUMAR, V., KUMAR, V., SINGH, N., & KUMAR, R	2023	96.0
An intrusion detection system based on grayscale and entropy	LIAO, D., ZHOU, R., LI, H., ZHANG, M., & CHEN, X.	2022	95.4
Federated deep belief network-based wireless network intrusion detection system.	M. NIVAASHINI, E. SUGANYA, S. SOUNTHARRAJAN, M. PRABU, & DURGA PRASAD BAVIRISETTI	2022	93.5
Integration of Blockchain and Machine Learning Techniques to Enhance IoT Security	-	2025	**99.4**

Table 4. Comparison of previous work

6. Conclusion

The integration of blockchain and machine learning presents a promising solution to the security challenges faced by IoT systems. Blockchain ensures transparency, decentralization, and immutability, addressing issues related to data integrity and trust. Machine learning enhances security by identifying threats in real time and enabling predictive analysis. By incorporating these technologies, the security against cyberattacks and unauthorized access data breaches is thus minimized. In the proposed framework, scalability along with efficiency while securing IoT networks can be gained. Future developments in these areas will continue to raise the bar and make IoT-based ecosystems stronger and more reliable.

Future work can be to increase the computational efficiency of blockchain-based IoT security systems in order to address scalability issues. Integration of quantum computing and artificial intelligence with blockchain can also improve security mechanisms. Development of lightweight cryptographic protocols designed for IoT devices with limited processing power will also be crucial. The use of federated learning approaches for distributed security solutions in IoT networks can also be investigated. Furthermore, real-world experimentation and deployment of the proposed framework in industrial IoT applications will give an idea of its practicability and flexibility.

References

AL-IMRAN, M., & RIPON, S. H. 2021. Network Intrusion Detection: An Analytical Assessment Using Deep Learning and State-of-the-Art Machine Learning Models. *International Journal of Computational Intelligence Systems*, *14*(1). https://doi.org/10.1007/s44196-021-00047-4

ARORA, A., & GOSAIN, A. 2021. Intrusion detection system for data warehouse with second level authentication. *International Journal of Information Technology*, *13*(3), 877–887. https://doi.org/10.1007/s41870-021-00659-1

ARORA, P., WASON, R., NARULA, G. S., & HODA, M. N. 2024. A Novel and Optimised Thread-based Virtual Traffic Light Framework. *Journal of Scientific & Industrial Research*, *83*(10). https://doi.org/10.56042/jsir.v83i10.7710

BHAVSAR, M., ROY, K., KELLY, J., & ODEYOMI OLUSOLA. 2023. Anomaly-based intrusion detection system for IoT application. *Discover Internet of Things*, *3*(1). https://doi.org/10.1007/s43926-023-00034-5

CUI, J., ZONG, L., XIE, J., & TANG, M. 2022. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data. *Applied Intelligence*. https://doi.org/10.1007/s10489-022-03361-2

DEORE, B., & BHOSALE, S. 2023. Adaptive Dolphin Atom Search Optimization-Based DRNN for Network Intrusion Detection System. *SN Computer Science*, *4*(5). https://doi.org/10.1007/s42979-023-02006-6

GODALA, S., & KUMAR, M. S. 2023. RETRACTED ARTICLE: A weight optimized deep learning model for cluster based intrusion detection system. *Optical and Quantum Electronics*, *55*(14). https://doi.org/10.1007/s11082-023-05509-x

KUMAR, V., KUMAR, V., SINGH, N., & KUMAR, R. 2023. Enhancing Intrusion Detection System Performance to Detect Attacks on Edge of Things. *SN Computer Science*, *4*(6). https://doi.org/10.1007/s42979-023-02242-w

LIAO, D., ZHOU, R., LI, H., ZHANG, M., & CHEN, X. 2022. GE-IDS: an intrusion detection system based on grayscale and entropy. *Peer-To-Peer Networking and Applications*, *15*(3), 1521–1534. https://doi.org/10.1007/s12083-022-01300-z

M. NIVAASHINI, E. SUGANYA, S. SOUNTHARRAJAN, M. PRABU, & DURGA PRASAD BAVIRISETTI. 2024. FEDDBN-IDS: federated deep belief network-based wireless network intrusion detection system. *EURASIP Journal on Information Security (Online)*, *2024*(1). https://doi.org/10.1186/s13635-024-00156-5

MAHESWARI, K. G., SIVA, C., & PRIYA, G. N.2022. An Optimal Cluster Based Intrusion Detection System for Defence Against Attack in Web and Cloud Computing Environments. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-022-10030-7

PRAJISHA, C., & VASUDEVAN, A. R. 2022. An efficient intrusion detection system for MQTT-IoT using enhanced chaotic salp swarm algorithm and LightGBM. *International Journal of Information Security*. https://doi.org/10.1007/s10207-022-00611-9

S. SIVAMOHAN, SRIDHAR, S. S., & S. KRISHNAVENI. 2023. *TEA-EKHO-IDS: An intrusion detection system for industrial CPS with trustworthy explainable AI and enhanced krill herd optimization*. *16*(4), 1993–2021. https://doi.org/10.1007/s12083-023-01507-8

SAADIA AJMAL, AAMIR, R., RAZA, A., & RAUF, A. 2024. IDS-FRNN: an intrusion detection system with optimized fuzziness-based sample selection technique. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-024-10333-9

SABITHA, R., GOPIKRISHNAN, S., BEJOY, B. J., ANUSUYA, V., & SARAVANAN, V. 2022. Network Based Detection of IoT Attack Using AIS-IDS Model. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-022-10009-4

SELVAPANDIAN, D., & SANTHOSH, R. 2021. Deep learning approach for intrusion detection in IoT-multi cloud environment. *Automated Software Engineering*, *28*(2). https://doi.org/10.1007/s10515-021-00298-7

SHIRAFKAN, M., SHAHIDIENJAD, A., & MOSTAFA GHOBAEI-ARANI. 2021. An autonomous intrusion detection system for the RPL protocol. *Peer-To-Peer Networking and Applications*, *15*(1), 484–502. https://doi.org/10.1007/s12083-021-01255-7

SOOD, T., PRAKASH, S., SHARMA, S., SINGH, A., & CHOUBEY, H. 2022. Intrusion Detection System in Wireless Sensor Network Using Conditional Generative Adversarial Network. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-022-09776-x

TANEJA, A., & KUMAR, G. 2024. Attention-CNN-LSTM based intrusion detection system (ACL-IDS) for in-vehicle networks. *Soft Computing*. https://doi.org/10.1007/s00500-024-10313-0

THAKKAR, A., & LOHIYA, R. 2021. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-021-10037-9

YAN, F., ZHANG, G., ZHANG, D., SUN, X., HOU, B., & YU, N. 2023. TL-CNN-IDS: transfer learning-based intrusion detection system using convolutional neural network. *The Journal of Supercomputing*, *79*(15), 17562–17584. https://doi.org/10.1007/s11227-023-05347-4

YASSINE AKHIAT, KAOUTHAR TOUCHANTI, ZINEDINE, A., & CHAHHOU, M. 2023. IDS-EFS: Ensemble feature selection-based method for intrusion detection system. *Multimedia Tools and Applications*, *83*(5), 12917–12937. https://doi.org/10.1007/s11042-023-15977-8