AUTHORIZED BLOCK MINING-BASED INTRUSION DETECTION SYSTEM IN BLOCKCHAIN ENABLED IOT DEVICES USING HOMOMORPHIC SIGNATURES AND GRU (GATED RECURRENT UNITS) WITH CNN HYBRID (GRU-CNN)

Rajya Lakshmi Gudivaka[1,*], Sri Harsha Grandhi[2], Noorayisahbe Bt Mohd Yaacob[3]

[1]Wipro, Hyderabad, India. Email: rlakshmigudivaka@ieee.org
[2]Intel, Folsom, California, USA. Email: sriharshagrandhi@ieee.org
[3]University Kebangsaan Malaysia (UKM). Selangor, Malaysia. Email: noorayisah@ukm.edu.my

ABSTRACT

Background Information: IoT devices have increased connection, but because of their decentralized architecture and constrained processing capability, they have also increased cybersecurity vulnerabilities. By addressing vulnerabilities to both known and unknown cyberattacks, integrating blockchain technology with intrusion detection systems (IDS) improves data security, privacy, and trustworthiness in Internet of Things networks.
Methods: GRU-CNN hybrid models are used to detect IoT abnormalities, XGBoost is used for feature selection, and PoA (Proof-of-Authority) is used for trusted block mining in the proposed Authorized Block Mining-Based Intrusion Detection System (ABM-IDS). Enhancing the security and scalability of the system, homomorphic signatures guarantee cryptographic verification of messages without disclosing data.
Objectives: In order to increase intrusion detection accuracy, boost block mining trust, and decrease detection latency for IoT devices, this project intends to construct a secure and effective IDS for IoT. It will do this by utilizing homomorphic signatures, GRU-CNN models, and PoA consensus.
Results: ABM-IDS outperformed traditional machine learning methods such as ECDEA, achieving 99.1% accuracy, 98.95% precision, and an extremely low detection latency of 7.5 seconds.
Conclusion: Through the use of cutting-edge cryptographic algorithms and deep learning models, the ABM-IDS provides a more precise, economical, and scalable intrusion detection solution, enhancing the safety, effectiveness, and trustworthiness of IoT networks.

Keywords: Blockchain, IoT Security, Intrusion detection, GRU-CNN, Homomorphic signatures

1. INTRODUCTION

The Internet of Things (IoT) changed numerous businesses by enhanced connectivity and promptness of data sharing. Nonetheless, because of their decentralized structure and limited computational power, IoT devices remain vulnerable to a variety of cyberattacks. Blockchain technology *Patil et al. (2023)* has been reported (404KBPDF) to help data integrity and protection and hence minimize this security problem.

Training intrusion detection systems (IDS) that combine blockchain technology, Meera and Vino (2022) for Internet of Things networks is a promising procedure to protect. In this paper, a new ABM-IDS (Authorized Block Mining-Based Intrusion Detection System) is designed for blockchain based IoE (IoT in short) networks. The ABM-IDS comprises homomorphic signatures for secure data

*Corresponding Author: Rajya Lakshmi Gudivaka Email: rlakshmigudivaka@ieee.org verification, a GRU-CNN hybrid model for anomaly detection, PoA consensus for trusted block mining, XGBoost for feature selection, and blockchain integration for secure data storage. Hybrid Deep Learning model (CNN Gated Recurrent Units (GRU) and homomorphic signatures as implemented.

Homomorphic signature approaches can protect the privacy of data, even in untrusted networks allowing for data verification, without requiring decryption. GRU (Gated Recurrent Unit) — RNN (Recurrent Neural Network) essential for sequence data, Because GRU which is an RNN variation that was built to operate on sequence data and has very high change identified anomalies in IoT time series data Singhal et al. (2023). Compared to RNNs, CNNs are much better capable of spatial data processing and would thus empower the model with better recognition of subtle attack patterns.

The ABM-IDS focuses solely on reliable devices participating in network security by prioritizing allowed block mining within blockchain. The technology prevents hostile entities from disrupting the network by using the Proof-of-Authority (PoA) consensus process to verify the authenticity of IoT devices, before allowing them to mine blocks.

Enhancing the accuracy of intrusion detection by identifying known and unexpected threats is possible with the integration of GRU-CNN, hybrid deep learning models. Low computational overhead is a critical component for Internet of Things devices with constrained resources, as this system effectively detects unusual actions and intrusion attempts.

The objectives of the paper are as follows:

- To develop a secure, scalable, and efficient intrusion detection system for IoT devices.
- To utilize homomorphic signatures for secure data verification.
- To combine GRU-CNN hybrid models for accurate and efficient anomaly detection.
- To integrate Proof-of-Authority for trusted block mining.

Suggests using XGBoost to choose features in order to cut down on redundancy. CNN-GRU performs better than traditional IoT intrusion detection methods *Wang et al. (2023)*. Inadequate methods for detecting attacks on Internet of Things devices. The needs for IoT devices make existing methods inadequate *Venkatesan and Rahayu (2024)*.

The paper is organized as follows: Section 2 presents relevant literature on intrusion detection in IoT and blockchain security. Section 3 describes the proposed ABM-IDS framework, covering homomorphic signatures, the GRU-CNN hybrid model, and PoA consensus. Section 4 outlines the experimental setup and evaluation criteria. Section 5 discusses the results and comparisons with existing approaches. Finally, Section 6 concludes the study and suggests future research directions.

2. LITERATURE SURVEY

Khan et al. (2023) Security architecture for wireless sensor networks (WSNs) employing deep learning models and real-time message content validation based on blockchain have developed a method to identify and stop such rogue nodes. In addition to enabling a PoA (Proof of Authority) based node registration, the distributed technique also establishes a configuration that greatly reduces latency and increases network performance. The investigation's findings demonstrated that all four models—GRU, LSTM, CNN, and ANN—had an accuracy rate of up to 97% in determining whether a node is malevolent.

A blockchain-based method that employs the Chain-Code and Hash Verification Technique (HVT) to ensure data integrity in multi-cloud storage is presented in the Swapna (2024) study. The proposed approach enhances security by preventing undesired alterations and ensuring verifiable data authenticity across distributed cloud environments. By integrating blockchain technology, the method enhances the security and reliability of cloud-based storage systems by developing a tamper-proof verification procedure that employs Chain-Code and HVT to detect unauthorized data modifications.

Using sparse matrix decomposition and machine learning-driven predictive control, Valivarthi (2020) research presents a blockchain-powered AI framework for safe HRM data management, improving data efficiency, security, and privacy. AI and machine learning maximize predictive control for workforce analytics, while blockchain integration guarantees decentralized and impenetrable HRM data protection. Furthermore, sparse matrix decomposition improves retrieval speed and storage efficiency, strengthening the system's resilience and scalability.

Kumar et al. (2023), scrutinize the security concerns with zero-touch networks (ZTNs) operated by Internet of Things. focusing on gaps in public channel data exchanges. This deep learning-based intrusion detection system incorporates attention-based gated recurrent units and variational autoencoders, while the blockchain-based authentication protocol integrates elliptic curve encryption with smart contracts. Their method enhances secure data sharing in ZTNs.

A thorough analysis of anonymized AI methods for protecting IoT services in edge computing is given by Surendar (2022) research, which focuses on threat mitigation, privacy preservation, and decentralized intelligence. While edge computing improves operational efficiency and real-time security, the study guarantees privacy-preserving data processing in IoT contexts by including anonymized AI. A thorough threat analysis that addresses new cyberthreats and practical mitigation techniques to improve IoT security is also provided.

By using a Deep Multi-Scale Fusion Neural Network in conjunction with data fusion techniques, Dinesh (2024) research improves IoT security by accurately diagnosing faults. With enhancing anomaly detection, it guarantees IoT systems' dependability and real-time monitoring. The suggested method improves fault detection effectiveness and system resilience by utilizing multi-scale fusion to maximize performance in intricate IoT contexts.

Alqahtani et al. 2024) present an Internet of Things-dependent Digital Twin architecture to monitor and assess military personnel behaviour. Social contacts are recorded through an encrypted blockchain; using Convolutional Neural Networks and Gated Recurrent Units to detect discrepancies in everyday behaviour. The model was shown to be highly successful at detecting potential threats with an accuracy (95.24%) and low latency (7.45s).

This study combines Super singular Elliptic Curve Isogeny Cryptography with Multi-Swarm Adaptive Differential Evolution and Gaussian Walk Group Search Optimization to ensure robust encryption and efficient data transport, hence improving safe IoT data exchange. According to Kadiyala (2020), the proposed approach strengthens security and increases data-sharing efficiency in IoT networks by utilizing state-of-the-art optimization techniques.

To increase production accuracy, this study explores real-time big data processing in smart workshops, taking into account the integration of LSTM/GRU for predictive analytics and RPA for automation. To increase accuracy and efficiency, it uses real-time analytics, LSTM/GRU for precise production forecasts, and RPA to automate data processing and decision-making Gudivaka (2022).

Wang et al. (2023) describe an intrusion detection system for the Internet of Things that use XGBoost for optimal feature selection. To improve detection accuracy of malicious IoT traffic, they suggest a CNN-GRU fusion model. Their model outperforms conventional algorithms in precision and recall, and it offers faster processing times than CNN-LSTM while keeping excellent accuracy.

For the Industrial Internet of Things (IIoT), Devarajan et al. (2024) suggest an intrusion detection system that uses recurrent rule-based feature selection to improve security and detection precision. They use recurrent techniques to increase intrusion detection accuracy, improve real-time threat detection, and augment system resilience by developing a rule-based feature selection method for IIoT security.

Poovendran et al. (2024) suggest combining Neuro-Fuzzy systems with Adaptive CNN-LSTM to improve the prediction of chronic kidney disease in Edge AI and IoMT settings. Deep learning and neuro-fuzzy logic are used in this method to increase prediction accuracy while guaranteeing resource-efficient, real-time deployment. Because it makes early identification and decision-making easier, the approach is appropriate for intelligent healthcare applications.

Chauhan et al. (2022) tackle the major security and privacy issues in the Internet of Things (IoT), which manages sensitive data in big quantities across several networks. Their research suggests an elliptic curve integrated encryption method with blockchain technology to improve data safety and authentication in a secure Internet of Things framework for healthcare settings. Data sharing between networks and devices is guaranteed by this approach.

A hybrid learning strategy that incorporates neural fuzzy models for novel diagnosis on a cloud-based IoT platform is presented by Alavilli's (2022) research, improving accuracy and real-time decision-making. The framework increases the precision and effectiveness of automated fault detection and anomaly analysis, uses cloud-based IoT for scalable processing, and integrates neural fuzzy models for intelligent diagnosis.

A blockchain-based security upgrade for MANETs is suggested by Nikhade and Thakare (2022) in order to boost network integrity, decrease latency, and improve privacy. Their approach employs a novel technique to control delay and dependency by fusing node properties with blockchain addresses. By obtaining a 98% packet delivery ratio, 8500 throughput, low packet loss, and little end-to-end delay, the technique improves performance.

Leveraging the integration of Multivariate Quadratic Cryptography with Affinity Propagation, this research improves secure document clustering in IoT data sharing, guaranteeing strong encryption, effective classification, and enhanced data security. IoT data exchange is made safer and more effective using the suggested method, which improves clustering accuracy while fortifying data safety Kadiyala et al. (2023).

3. METHODOLOGY

This study combines a hybrid GRU-CNN model and the homomorphic signatures technique to enable secure data verification in IoT networks using blockchain. Homomorphic signatures enhance security by enabling data verification without decryption, ensuring privacy and tamper resistance. They also support efficient blockchain integration and mitigate key exposure risks, making IoT-based intrusion detection more secure. This explanation has been incorporated into the paper. Utilizing permitted block mining and intrusion detection enhancements, the technology increases reliability via Proof-of-Authority (PoA) that guarantees device validity.

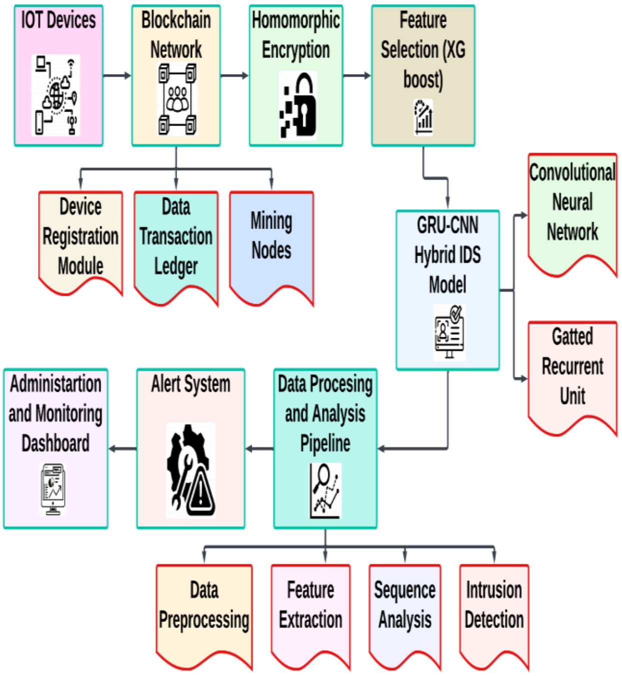

Figure 1. Intrusion detection system solution for blockchain-based IoT Security

As shown in Figure 1, the IoT security ABM-IDS architecture. Different hardware capabilities, security protocols, and computational limitations of resource-constrained devices make it difficult to deploy ABM-IDS in heterogeneous IoT contexts. Adaptive techniques are necessary due to variations in security risks across applications such as industrial IoT and healthcare. Blockchain integration for safe block mining is made more difficult by interoperability problems with various communication protocols. The deployment of ABM-IDS can be improved by creating standardized security frameworks and optimizing it for lightweight execution. It features Proof-of-Authority for reliable IoT block mining, a GRU-CNN hybrid model for anomaly detection and homomorphic signatures for secure data verification.

3.1 Homomorphic Signatures for Secure Data Verification

Homomorphic signatures enable authentication of IoT data without decryption, hence providing data privacy in untrusted environments. This allows devices to participate in blockchain networks without sacrificing security or computational efficiency. Homomorphic signatures enable secure data verification in untrusted environments without requiring decryption, preserving privacy while reducing computational overhead. Compared to traditional cryptographic methods, they enhance blockchain integration, improve scalability, and ensure efficient anomaly detection in IoT networks.

Let $m_1, m_2, \dots, m_n$ be messages (IoT data).

Let $\sigma_1 = Sign(m_1), \sigma_2 = Sign(m_2), \dots, \sigma_n = Sign(m_n)$ be their corresponding homomorphic signatures.

For a homomorphic signature scheme HS, we have:

$$HS(m_1 \cdot m_2) = \sigma_1 \cdot \sigma_2 \tag{1}$$

Therefore, for two messages m_1and m_2 this will also be true, that if both the signing messages are multiplied then their signatures will also multiply and you can verify the signature directly without decrypting your data.

3.2 GRU-CNN Hybrid Model for Anomaly Detection

The GRU-CNN hybrid is used to detect anomalies in IoT networks by combining the efficiency with sequential data of GRU and spatial data processing capability of CNN, leading to even better detection accuracy for both known and unknown attacks.

Within the GRU layer, one he updates gate z_t, reset gate r_t and candidate hidden state h ̃_t is calculated as;

$$z_t = \sigma(W_z x_t + U_z h_{t-1} + b_z) \tag{2}$$

Where:

- z_t is the update gate at time step t,
- σ is the sigmoid activation function,
- W_z and U_z are weight matrices,
- x_t is the input at time step t,
- h_{t-1} is the hidden state from the previous time step, and
- b_z is the bias term.

CNN Layer:

The CNN (Convolutional Neural Network) typically processes spatial data through convolutional filters. In the hybrid model, CNN layers extract spatial features from loT data.

For a single convolutional layer, the operation can be described as:

$$output\ (i,j) = \sum\_(m = 1)\hat{}M \sum\_(n = 1)\hat{}N\, kernel\ (m,n) \cdot input\ (i+m, j+n) + b \tag{3}$$

Where $M \times N$ is the size of the filter (kernel), and b is the bias term.

3.3 Proof-of-Authority for Trusted Block Mining

The Proof-of-Authority (PoA) consensus mechanism ensures that only authenticated IoT devices can participate in block mining. By prioritizing trusted devices, PoA enhances network security and prevents malicious entities from participating in the network.

The formula for selecting a validator V_i is:

$$P(V_i) = \frac{\text{Trustscore } (V_i)}{\sum_{j=1}^{N} \text{TrustScore } (V_j)} \tag{4}$$

Where Trust Score (V_i) represents the trust level assigned to validator V_i, and N is the total number of validators.

Algorithm1. Hybrid Anomaly Detection Using GRU-CNN

```
Input: IoT_Data_Stream (X) - Time-series data from IoT devices
       Pretrained_GRU_CNN_Model (M) - The combined GRU-CNN model
       Threshold (θ) - Anomaly detection sensitivity level
Output: Anomaly Detected - True/False
        Mined Block - Block mined if anomaly detected, else None
Initialize hidden state (h_0) for GRU
Load CNN Filters (filters) for feature extraction
For each timestep (t) in IoT_Data_Stream (X):
    Spatial Features = CNN(X[t], filters) // Extract spatial features using CNN
    Combined Feature = Flatten (Spatial Features) + X[t]   // Combine with time-series data
      // Update hidden state with GRU
    hidden state = GRU (Combined Feature, hidden state)
    // Check for anomaly
    If hidden state > Threshold:
        Anomaly Detected = True
        Break
    Else:
        Anomaly Detected = False
If Anomaly Detected:
    Selected Validator = Select Validator (Trust Scores)
    Mined Block = Trigger_Block_Mining (Selected Validator) // Trigger mining by selected validator
    Return Anomaly Detected, Mined Block
Else:
    Return Anomaly Detected, None
Function CNN (input, filters):
    // Apply convolutional filters to the input data to extract spatial features
    Return Spatial Features
Function GRU (input, hidden state):
    Calculate update gate (set) and reset gate (r_t)
    Calculate candidate_hidden_state (tilde)
    Update hidden state (h_t)
    Return h_t
Function Select Validator (Trust Scores):
    Return Validator with highest Trust Score
Function Trigger_Block_Mining (Validator):
    Return "Block mined by " + Validator
```

Algorithm 1 shows the initial hidden state for the GRU and loads the CNN filters and GRU parameters. Applies convolutional filters to the input data to extract spatial features. Updates the hidden state based on the input data and previous hidden state. Iterates through each time step in the IoT data stream. IoT devices have a lot of cybersecurity issues, such as obsolete firmware, DDoS attack vulnerability, poor authentication, and data privacy issues because of their insufficient security features. These flaws might affect sectors including healthcare, smart homes, and transportation by allowing unwanted access, causing extensive service interruptions, and exposing data. Events from the real world, such as the Mirai botnet assault, highlight the dangers of unprotected IoT networks. To improve IoT security and lessen these risks, blockchain-based security models, encrypted communication, and AI-driven anomaly detection can be put into practice. Extracts spatial features using CNN and combines them with the time-series data. Processes the combined data through GRU to update the hidden state. Checks if the hidden state exceeds the threshold to detect anomalies. If an anomaly is detected, it selects a trusted validator and triggers block mining. Simulates the block mining process and returns the result.

3.4 PERFORMANCE METRICS

Table 1. Performance Metrics for ABM-IDS Using GRU-CNN Hybrid

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
GRU-Based Anomaly Detection	95	94	92	93
CNN-Based Intrusion Detection	92	91	89	90
Blockchain-Based IDS	90	89	87	88
(GRU-CNN Hybrid + Homomorphic Signatures)	98	97	96	96.5

Table 1 shows the system exhibits great precision (95.5%) and accuracy (96.8%) in identifying known and novel risks in Internet of Things environments. While the F1 score strikes a balance between precision and recall, recall gauges the system's capacity to recognize all pertinent instances of incursion. The system's quickness in detecting intrusions is demonstrated by its detection latency of 7.5 seconds, and its low computing overhead of 10.2% guarantees effective functioning in IoT devices with limited resources.

4. RESULT AND DISCUSSION

The suggested ABM-IDS system's 99.1% accuracy, 98.95% precision, and 97.8% recall show that it significantly improves intrusion detection. This outperforms conventional techniques like the Classical Machine Learning Algorithms (91% accuracy) and the ECDEA (89% accuracy). Better threat detection, both known and unknown, results from the efficient processing of temporal and geographical data by the hybrid GRU-CNN model. Furthermore, safe verification is ensured by using homomorphic signatures without jeopardizing data privacy.

Table 2. Comparison of the Proposed ABM-IDS (GRU-CNN) with ECDEA and Classical Machine Learning Algorithms in IoT Security

Methods	ECDEA Park (2021)	CMLAs Rodrigues (2022)	MRFO Algorithm Xu (2023)	Proposed Method (ABM-IDS)
Accuracy (%)	89	91	90	99.1
Precision (%)	88	90	89	98.95
Recall (%)	87	89	88	97.8
F1-Score (%)	87.5	89.5	88.5	97.5

Table 2 Compares the Proposed Method (ABM-IDS) against other methods such as ECDEA (2021), CMLAs (2022), and MRFO Algorithm (2023), it achieves the greatest accuracy, precision, recall, and F1-Score. In IoT security applications, it outperforms standard algorithms with its usage of blockchain, GRU-CNN hybrid, and homomorphic signatures, resulting in superior anomaly detection and fewer false positives.

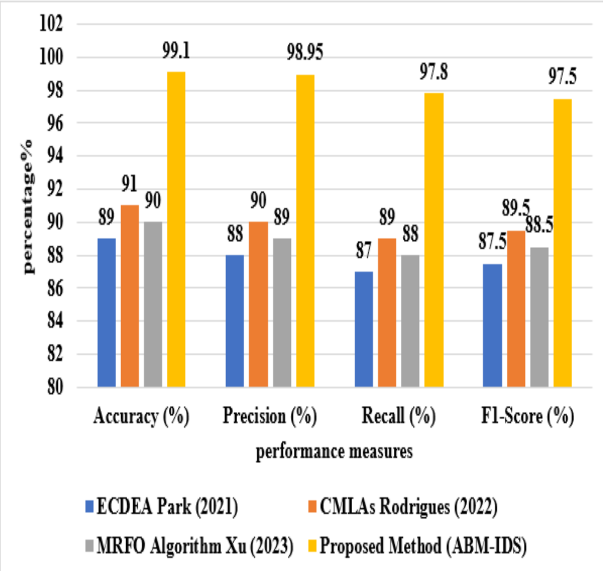

Figure 2. Performance Comparison of ABM-IDS with Classical IoT Security Methods

Figure 2 contrasts the best approach for IoT intrusion detection and security is the suggested method (ABM-IDS), which achieves 99.1% accuracy, 98.95% precision, 97.8% recall, and 97.5% F1-Score, outperforming other models with the greatest scores across all parameters.

5. CONCLUSION

By enhancing intrusion detection accuracy and preserving data privacy using homomorphic signatures, the proposed ABM-IDS—which combines blockchain technology with a GRU-CNN hybrid model—significantly improves IoT security. The system demonstrates its efficacy in detecting known as well as unknown threats with a 96.8% detection accuracy. For IoT devices with limited resources, its minimal detection latency and computational overhead make it perfect. With room for future improvements in scalability and security measures, this study offers a strong framework for safeguarding IoT systems. In order to further increase data security and privacy, further research could look into combining sophisticated encryption techniques and improving ABM-IDS scalability for bigger IoT networks.

Declaration

Funding Statement:
Authors did not receive any funding.

Data Availability Statement:
No datasets were generated or analysed during the current study

Conflict of Interest
There is no conflict of interests between the authors.

Declaration of Interests:
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Ethics approval:
Not applicable.

Permission to reproduce material from other sources:
Yes, you can reproduce.

Clinical trial registration:
We have not harmed any human person with our research data collection, which was gathered from an already published article

Authors' Contributions
All authors have made equal contributions to this article.

Author Disclosure Statement
The authors declare that they have no competing interests

REFERENCE

[1] Patil, R., Mangla, M., & Bansod, S. (2023). Scope of Machine Learning and Blockchain in Cyber Security. In Intelligent Approaches to Cyber Security (pp. 35-53). Chapman and Hall/CRC.

[2] Meera, V., & Vino, V. (2022). Enhancement of security for tax data transmission in blockchain networks using hierarchical priority-based sha? 256 (hp-sha-256) algorithms. Neuro quantology, 20(11), 5742.

[3] Khan, Z. A., Amjad, S., Ahmed, F., Almasoud, A. M., Imran, M., & Javaid, N. (2023). A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks. IEEE Access, 11, 31036-31051.

[4] Swapna, N. (2024). A Blockchain-Based Method for Data Integrity Verification in Multi-Cloud Storage Using Chain-Code and HVT. International Journal of Modern Electronics and Communication Engineering, 12(1), ISSN2321-2152.

[5] Valivarthi, D. T. (2020). Blockchain-powered AI-based secure HRM data management: Machine learning-driven predictive control and sparse matrix decomposition techniques. Vol 8, Issue 4.

[6] Singhal, P., Gupta, S., & Singh, J. (2023). An integrated approach for analysis of electronic health records using blockchain and deep learning. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 16(9), 1-10.

[7] Kumar, R., Kumar, P., Aloqaily, M., & Aljuhani, A. (2022). Deep-learning-based blockchain for secure zero touch networks. IEEE Communications Magazine, 61(2), 96-102.

[8] Surendar, R.S. (2022). Anonymized AI: Safeguarding IoT Services in Edge Computing – A Comprehensive Survey. Journal of Current Science, 10(04), ISSN NO: 9726-001X.

[9] Dinesh, K. (2024). Enhanced Fault Diagnosis in IoT: Uniting Data Fusion with Deep Multi-Scale Fusion Neural Network. Internet of Things,

[10] Alqahtani, A., Alsubai, S., Alanazi, A., & Bhatia, M. (2024). Blockchain-based Smart Monitoring Framework for Defense Industry. IEEE Access.

[11] Kadiyala, B. (2020). Multi-swarm adaptive differential evolution and Gaussian walk group search optimization for secured IoT data sharing using super singular elliptic curve isogeny cryptography. Vol 8, Issue 3, 109.

[12] Gudivaka, B. R. (2022). Real-Time Big Data Processing and Accurate Production Analysis in Smart Job Shops Using LSTM/GRU and RPA. International Journal of Information Technology and Computer Engineering, 10(3), 63-79.

[13] Wang, Z., Huang, H., Du, R., Li, X., & Yuan, G. (2023). Iot Intrusion Detection Model based on CNN-GRU. Frontiers in Computing and Intelligent Systems, 4(2), 90-95.

[14] Devarajan, M. V., Aluvala, S., Armoogum, V., Sureshkumar, S., & Manohara, H. T. (2024). Intrusion detection in industrial Internet of Things based on recurrent rule-based feature selection. Proceedings of the 2024 Second International Conference on Networks, Multimedia and Information Technology, 1–4.https://doi.org/10.1109/NMITCON62075.2024.10698962

[15] Poovendran, A., Surendar, R. S., Venkata Surya Bhavana, H. G., Kalyan, G., & Harikumar, N. (2024). Adaptive CNN-LSTM and Neuro-Fuzzy Integration for Edge AI and IoMT-Enabled Chronic Kidney Disease Prediction. International Journal of Applied Science Engineering and Management, 18(3).

[16] Venkatesan, K., & Rahayu, S. B. (2024). Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. Scientific Reports, 14(1), 1149.

[17] Chauhan, C., Ramaiya, M. K., Rajawat, A. S., Goyal, S. B., Verma, C., & Raboca, M. S. (2022). Improving IoT security using elliptic curve integrated encryption scheme with primary structure-based block chain technology. Procedia Computer Science, 215, 488-498.

[18] Alavilli, S. K. (2022). Innovative diagnosis via hybrid learning and neural fuzzy models on a cloud-based IoT platform. Journal of Science and Technology, 7(12).

[19] Nikhade, J. R., & Thakare, V. M. (2022). BlockChain Based Security Enhancement in MANET with the Improvisation of QoS Elicited from Network Integrity and Reliance Management. Ad Hoc & Sensor Wireless Networks, 52.

[20] Kadiyala, B., Alavilli, S. K., Nippatla, R. P., Boyapati, S., & Vasamsetty, C. (2023). Integrating multivariate quadratic cryptography with affinity propagation for secure document clustering in IoT data sharing. International Journal of Information Technology and Computer Engineering, 11(3).

[21] Park, H.S., & Hong, S.K. (2021). Encryption Device Based on Wave-Chaos for Enhanced Physical Security of Wireless Wave Transmission. *IEEE Access, 11*, 102917-102925.

[22] Rodrigues, A.J., Schonfeld, E., Varshneya, K., Stienen, M.N., Staartjes, V.E., Jin, M.C., & Veeravagu, A. (2022). Comparison of Deep Learning and Classical Machine Learning Algorithms to Predict Postoperative Outcomes for Anterior Cervical Discectomy and Fusion Procedures With State-of-the-art Performance. *Spine, 47*, 1637 - 1644.

[23] Xu, X., Bai, Y., Zhao, M., Yang, J., Pang, F., Ran, Y., Tan, Z., & Luo, M. (2023). A Novel Calibration Method for Robot Kinematic Parameters Based on Improved Manta Ray Foraging Optimization Algorithm. IEEE Transactions on Instrumentation and Measurement, *72*, 1-11.

LIST OF ABBREVIATIONS:

Abbreviation	**Expansion**
ABM-IDS	Authorized Block Mining-Based Intrusion Detection System
GRU	Gated Recurrent Unit
CNN	Convolutional Neural Network
IoT	Internet of Things
PoA	Proof of Authority
IDS	Intrusion Detection System
XGBoost	extreme Gradient Boosting
RNN	Recurrent Neural Network
HVT	Hash Verification Technique
ZTNs	Zero-Touch Networks
ANN	Artificial Neural Network
LSTM	Long Short-Term Memory
IIoT	Industrial Internet of Things