Journal of Theoretical and Applied Information Technology
15st July 2026. Vol.104. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OPTIMIZING SECURITY IN IOT ECOSYSTEM WITH BLOCKCHAIN INTEGRATED ARTIFICIAL INTELLIGENT BASED INTRUSION DETECTION

SUBBAIAHGARI R AJITHA[1], Dr G V RAMESH BABU[2]

[1]SVU College of CM & CS, Sri Venkateswara University, Tirupati- 517502
[2]SVU College of CM & CS SV University, Tirupati-517502
ajitha1428@gmail.com[1], gvrameshbabu74@gmail.com[2]

ABSTRACT

The Internet of Things (IoT) is an emerging technology that has enhanced connectivity across multiple industries such as Industry 4.0 and smart cities. Intrusion Detection Systems (IDS) play a crucial role in identifying and mitigating cyber threats in such environments. The centralized architecture of traditional security systems poses challenges for scalability and performance, which hinders their ability to handle the complexity and volume of IoT devices. The problems cause latency, power usage and inefficient intrusion detection. This research proposes an intrusion detection system using artificial intelligence and blockchain concepts to boost security in the Internet of Things (IoT) environment. The primary goal is to use blockchain to create a secure framework without the need for a central authority to oversee the data. Feature extraction is done by a dual-ResNet model and feature selection is done by modified Coati Optimization (MCO) algorithm. The resulting feed-forward artificial neural network (FF-ANN) is then re-used for intrusion detection, greatly enhancing the security of IoT networks. The main IT contribution of this research is the creation of the intelligent and decentralized cybersecurity framework, which uses deep learning to detect intrusions and blockchain to guarantee data integrity. The proposed approach also has advantages compared to the traditional centralized IDS solutions, such as trust, less centralized IDS monitoring dependency, and reliable attack identification in the resource-constrained IoT environment. The combination of Dual-ResNet feature extraction, optimized feature selection, and blockchain verification adds to the scalable and secure IoT infrastructure.The proposed model is evaluated using the ToN-IoT and CICIDS-2017 datasets, achieve exceptional predictive accuracy of 98.8 % and 98.937%, respectively, outperforming existing models.
Keywords: *Blockchain, Artificial Intelligent, Intrusion Detection System, Internet Of Things, Secure Data Management*

1. INTRODUCTION

The Internet of Things (IoT) has automated and connected many industries [1]. Unprotected IoT plans like intelligent home appliances and industrial sensors are targeted by cyber attacks. Weak authentication, unsecured communication pathways, and outdated firmware let attackers access, modify, and disrupt services [2]. The more connected these IoT devices are, the more they present security risks, requiring innovative and flexible security solutions. Many of the IoT devices cannot use complex cryptography or real-time monitoring due to their limited resources. A security management problem is that each device in an IoT ecosystem will have a different level of security compliance. By establishing threat detection and response blind spots, fragmentation makes IoT networks vulnerable to sophisticated attacks [3][4]. These types of problems can only be addressed with a multi-layered security strategy that makes use of key infrastructure. Anomaly detection is made possible by artificial intelligent (AI) [5] and data integrity and authentication by blockchain. Intrusion detection systems (IDS) using AI can detect and respond to attacks in real time [6][7]. Signature-based traditional firewalls and IDS systems are not effective at protecting IoT networks. While AI-driven models rely on ML and DL to detect patterns and irregularities in network traffic, rule-based safety measures fall short in keeping up with cyber threats. AI-powered IDS models examine enormous data sets to find unusual activity and attacks that traditional systems miss [8]. AI learns from attacks to enhance its detection models instead of utilizing fixed attack signatures. Supervised learning,

reinforcement learning, and unsupervised anomaly detection let AI identify assaults properly and reduce false positives. AI-based IDS model suffers adversarial threats, processing needs, and model explainability concerns despite its benefits [9]. Attackers can misclassify malevolent activity by infusing adversarial noise into AI models. Data integrity is important since AI-driven IDS relies on high-quality training data. Blockchain and AI models can improve IDS by offering a decentralized and tamper-proof platform for training data storage and verification, boosting threat detection models [10].

Blockchain technology is gaining popularity as an IoT ecosystem security solution. Blockchain uses a decentralized ledger to securely and immutably record transactions [11]. IoT devices may securely authenticate, interact, and exchange data without a central authority using blockchain. Blockchain smart contracts automate IoT security. These self-executing contracts set data access, device interaction, and anomaly response rules. IoT-enabled smart grids can employ blockchain-based smart contracts to protect energy transfers between linked devices and prevent data manipulation [12]. Data provenance is another benefit of blockchain, allowing for tracking and verifying data modifications and integrity. The consumption of Blockchain on the processing and storage of resources may be an issue with resource-constrained IoT devices. Scalability is a significant issue for traditional blockchain networks that need to tackle high transaction volumes, particularly large ones, which introduce latency issues [13]. To improve blockchain integration with IoT security, lightweight blockchain frameworks and off-chain storage options are being investigated. The combination of blockchain and AI-based intrusion detection provides a secure authentication, data integrity, and real-time mitigation of attacks [14][15]. AI-based intrusion detection identifies threats as they occur, and blockchain verifies data. Organizations construct a decentralized, intelligent security system that responds to threats and prevents unwanted access by integrating these technologies which allows secure, independent decision-making without centralized bodies, strengthening IoT networks. This integration has several advantages, including security and verifiability of the training data for AI [16]. Data integrity can be guaranteed with immutable blockchains by storing AI model training datasets. AI can enable smart contracts on the blockchain to carry out security measures such as isolating infected devices and real-time compliance with security policies. The less people involved, the more effective the IoT security system. One of the decentralized AI training approaches is federated learning, where multiple IoT devices train an AI model without sharing data [17]. Blockchain technology guarantees that changes to the model are made by authenticated devices and keeps a record of training for transparency. AI-based IDS models are more accurate, privacy is enhanced and data breaches are decreased. AI and blockchain are giving rise to advanced scalable, powerful and flexible IoT security solutions to combat new threats [18].

Although significant developments are being made in the security of IoT, intrusion detection systems (IDS) are generally ineffective against more sophisticated attacks [19]. IDS models tend to have a high false-positive rate, slow response times, and difficulties with detecting zero-day attacks. Furthermore, centralized security systems are vulnerable to having single points of failure, which makes networks of IoT devices susceptible to large-scale attacks [20]. AI-powered threat analysis and blockchain's decentralization are explored in recent studies that focus on hybrid security strategies.More recently, researchers have studied hybrid security approaches, which involve leveraging blockchain's decentralization and AI threat analysis capabilities. Threat intelligence sharing, federated learning and anomoly detection using self-learning improves IoT security through blockchain. Optimizing these solutions for large-scale IoT deployments, scalability and computational overhead, however, is difficult. On the information technology standpoint, this research aims to tackle three critical cybersecurity issues in IoT: intelligent threat detection, secure data management, and trust establishment among distributed devices. By integrating these automated feature learning, feature reduction optimization, and tamper-resistant storage capabilities, the proposed blockchain-based IDS framework stands out as a valuable addition to traditional IDS models. As a result, this work contributes to the design of secure, reliable, transparent and adaptive security solutions to next generation of IoT networks. The following are AI and blockchain-based intrusion detection systems that are being used to enhance the security of IoT.AI and Blockchain-based intrusion detection systems that have been discovered to improve IoT security are discussed here. It evaluates techniques, pros and cons, and areas for further research. The study explores the most recent solutions to the IoT security challenge, looking for creative approaches to securing IoT ecosystems and new ideas for future research. This work introduces the concepts of DL

and optimization techniques to improve the security of the IoT ecosystem by combining with AI and the blockchain in IDS. This work's main supports are as tracks:

1. In the context of IoT networks, blockchain technology provides a decentralized and tamper-resistant solution for data management, offering security, integrity, and transparency in the handling of data.
2. The features obtained from network traffic data are meaningful and high-dimensional, using dual-ResNet architecture. The combination of two ResNet models provides more feature representation, intruding both local and global needs of the data. The Dual-ResNet architecture supplies robust feature learning, essential for accurately recognizing infiltration patterns within IoT networks.
3. A modified conflict optimization algorithm (COA) was used to maximize the feature set. The algorithm was inspired by social behaviour of goats; it is an improved version of the metaheuristic algorithm capable of identifying most important features. MCO aims to maximize the accuracy of classification and minimize the computational cost and ensures that the most important features for ID are kept for further analysis.
4. After the feature selection, a feed forward artificial neural network (FF-ANN) is used for intrusion detection. In order to efficiently understand intricate patterns of assaults and irregularities in IoT traffic, FF-ANN is built with numerous hidden layers. By enhancing decision-making through the application of activation functions like ReLU and softmax, ANN considerably raises the detection rate while lowering the quantity of false positives.
5. To prove the effectiveness of the proposed effort, the datasets of 5. 5th National Conference on Internet Devices (CICIDS-2017) and ToN-IoT are used.

The assessments encompass a variety of attack scenarios, such as DoS attacks, botnets and advanced persistent threats, to give a comprehensive evaluation environment. The object is organized as monitors: Section 2 offerings the literature appraisal, Section 3 outlines the anticipated method, Section 4 details the consequences evaluation, and Section 5 concludes the study.

2. RELATED WORKS

Ntizikira et al. 2025 [21] suggested a multi-layered security method that analyzes human behavior and detects breaches beyond network-based detection using emotion recognition. The CNN uses emotional states as biometric threat indicators. With blockchain technology, video and security logs can be protected from manipulation. When automatic security measures such as the alarm for suspicious activity and internet restriction for approved intruder are employed, reaction times are quickened and human interaction is minimized. This adaptive security solution helps combat the rising cyber risks and physical security vulnerabilities to ensure a robust, scalable and adaptive approach to intrusion prevention for IoT solutions. Das et al. 2025 [22] presented a blockchain-powered healthcare system using replicated matrix meta-learning and IoT. The framework incorporates hierarchical extraction of features, graph topology composition, dynamic prototype efficiency, and predictive query incorporation. Heterogeneous healthcare data may be efficiently processed by the federated matrix-prototype graph network (MGN). Extended studies employing CheXpert and CIFAR-100 showed an 85% improvement over current healthcare systems. Hakiri et al. 2025 [23] tackled the difficulties by merging SDN with blockchain to improve distributed IoT transaction adaptability, security, and efficiency. Blockchain-SDN architecture to improve QoS and a unique Proof-of-Authority (PoA) consensus mechanism to create confidence among IoT nodes are introduced. Experimental findings show that this technique beats PoW and PBFT algorithms by 68% lower latency, 87% greater transactional throughput, and 45% better energy efficiency. Bensaoud et al. 2025 [24] established a unique cyber-attack warning system that detects IoT network dangers using SOMs, DBNs, and Auto-encoders. Using particle swarm optimization (PSO) algorithm was used to reduces false positives and enhance accuracy improves model performance. The system surpasses earlier models with accuracy up to 99.99% and MCC values exceeding 99.50% after rigorous assessment using NSL-KDD, UNSW-NB15, and CICIoT2023 datasets. Sharma et al. 2025 [25] recommended a secure precision agricultural IoT network of communication with federated learning and blockchain. IoT communication hazards are identified using the CICIoT2023 dataset, addressing data sharing privacy problems and identifying attacks. The Ethereum blockchain with IPFS decentralized file storage allow safe model transfer

between clients and servers. After benchmarking using machine learning techniques in a regular environment, a blockchain-based federated learning system tested a deep neural network on similar and non-identical distributions of information.

Alabdan et al. 2025 [26] proposed IoT-IDS using the improved crayfish optimization algorithm with Interval Type-2 fuzzy deep learning. IoT enhances consumer device personalization and interactivity, elevating data privacy, access, and computer security risks. The IDS continuously monitors device behavior and network traffic utilizing machine learning-based anomaly detection. In the ICOA-IT2FDL technique, linear scaling normalization (LSN) for pretreatment data, improved crayfish optimization (ICOA) for feature selection, and an interval type-2 fuzzy deep belief network (IT2-FDBN) for intrusion classification boost intrusion detection Improve intrusion detection using BES. Chen et al. 2025 [27] created a synaptic intelligent convolutional neural network (SICNN) architecture to identify intrusions in dynamic IoT scenarios to combat rising cyber threats. The SICNN model uses a Synaptic Intelligence (SI) technique to optimize the convolutional neural network (CNN) synaptic topology, decreasing model forgetting and simplifying training. To address IoT traffic class imbalances and gradient vanishing, a new loss function is proposed. Model quantization and quantization-aware training reduce accuracy loss for resource-limited IoT devices. Ahmed et al. 2025 [28] examined significant vulnerabilities in IoT traffic and used state-of-the-art ensemble classifiers, XGBoost and LGBM, to identify various cyberattacks. These classifiers outperformed traditional models with 99.553% (XGBoost) and 99.651% (LGBM) detection accuracy and low false positives and negatives, which are crucial for IoT network integrity. Ahmad et al. 2024 [29] proposed a deep transfer learning-based IDS to secure IoT and IIoT networks. The method uses the Edge-IIoT dataset to transform information from network traffic into an image format for CNN feature extraction and pattern identification. A random search technique fine-tunes hyper-parameters to increase model accuracy and resilience. An ensemble of high-performing models improves the system's capacity to identify cyber threats across 14 assault categories. Quantization reduces computing cost and makes the model suitable for resource-constrained network security and threat detection. Kumar et al. 2024 [30] developed an elaborate game theory-based adaptive security (GT-AS) strategy to protect IoT networks from DDoS attacks. Simulated results demonstrate that the technique increases IoT device lifespan by 47% and improves accuracy, error rates, and network efficiency. The model outperforms prior methods with a packet delivery ratio of 60 KB, energy usage of 116 KJ, mean location inaccuracy of 0.078, and use of resources of 148. Table 1 précises the problematic statements from the existing state-of-art works.

According to the literature, several security challenges arise in the mining pool of blockchain-enabled IoT networks, making them highly susceptible to cyber threats [21][22]. The increasing frequency of DDoS attacks within blockchain-IoT ecosystems has significantly heightened network vulnerability, leading to severe service disruptions and security breaches [23][24]. The traditional IDS models face scalability issues, limiting their capacity to process large-scale real-time data efficiently, thereby causing performance bottlenecks [25]. A major issue with many of the current IDS models is their high false alarm rate, which is mainly caused by the poor feature selection and anomaly detection techniques giving them poor reliability [17][26]. Moreover, redundant and irrelevant features also increase computational overhead, which has a negative effect on the efficiency of the model [27].

One of the biggest disadvantages is the slow response speed of traditional IDS products, which can hinder timely detection and response to security threats, particularly in the real world context of IoT. A further key constraint is the slow response time of traditional IDS solutions, which can make it difficult to identify and respond to security threats, particularly in the real IoT environment. These are further complicated by the resources available to IoT devices: their computing power is limited and thus makes it difficult to implement complex security mechanisms. To address these difficulties, an AI-driven IDS system can be integrated with the blockchain, leveraging deep learning algorithms and optimization methods to further bolster the security of IoT networks. The Dual-ResNet model is employed to extract features which also guarantee the identification of high-level features that are relevant, while minimizing feature redundancy [30]. Features are tuned with the cooperative optimization algorithm (MCO) that is capable of selecting the best features to reduce the computation complexity and enhance the computing speed [31]. The feedforward artificial neural network (FF-ANN) is used to provide accurate intrusion detection to minimise false alarms and create the ability to manage intrusions as they happen. Blockchain technology is built in to provide data integrity and prevent unauthorized changes, thanks to the tamper-resistant

and decentralized security ledger.The integration of deep learning-based feature extraction, optimal feature selection, and blockchain security in large-scale IDS systems effectively and in real-time addresses cybersecurity in IoT ecosystems, including DDoS attacks, high false positive rates, scalability issues, and resource limitations.

3. BLOCKCHAIN-INTEGRATED AI-BASED IDS

Fig. 1 illustrates the blockchain-integrated AI-based IDS, which efficiently detects and neutralizes cyberthreats by utilizing deep learning, blockchain technology, and optimization techniques. IoT ecosystem security is its goal.

The framework system begins with the collection of data from various IoT-based electronic devices for consumers, including smart home devices, IIoT industrial systems, health monitoring devices, and smart automatic sensors. Blockchain technology, offering a decentralized and tamper-resistant ledger for secure data management, has been integrated into the system to ensure data integrity and prevent unauthorized modifications. This ensures that before any further processing, all collected data remains unchanged and visible.The collected data is represented by two popular intrusion detection databases: ToN-IoT and CICIDS-2017.

These datasets provide a solid foundation for evaluating the efficiency of the anticipated intrusion exposure system. When the data is collected, it goes through a preprocessing step to progress its quality and reliability before being used to train the IDS model. The main preprocessing steps include handling missing values using statistical imputation techniques or deletion, encoding categorical features using one-hot encoding or label encoding, and managing class imbalance using resampling methods. The main steps of preprocessing include handling missing values using statistical imputation techniques or deletion, encoding categorical features using one-hot encoding or label encoding, and managing class imbalance using resampling methods. These steps ensure that the database is well organized and suitable for training DL models without bias or inconsistency.After the pre-processing phase, feature extraction is carried out using a two-level network that captures the characteristics of the network traffic at different levels to improve the accuracy of intrusion detection.The extracted features include packet status features such as header information, packet size, and protocol types,as well as flow status features such as run time and TCP / UTP statistics.

Table 1 Summary of problem statement from the existing IDS models

Ref.	Methodology	Technique used	Dataset	Findings	Research gaps
[21]	Multi-layered security for IDS	CNN, Blockchain	CICIDS-2017	Improved intrusion detection with automated response	Insufficient because they are prone to false alarms
[22]	Blockchain-powered healthcare system	Federated MGN	CheXpert, CIFAR-100	85% improvement over existing healthcare models	Maintenance can be time-consuming and cost-intensive
[23]	SDN and Blockchain for IoT security	MMD-AE and DNN	BoT-IoT, DDCup-99	68% lower latency, 87% better throughput	Host overhead and scalability of NIDS makes difficulty
[24]	Cyber-attack detection for IoT	SOMs, DBNs, Auto-encoders, PSO	NSL-KDD, UNSW-NB15	99.99% accuracy, MCC >99.50%	Black boxes due to the complexity of detection models
[25]	Federated learning for precision agriculture	Blockchain, Deep Neural Networks	PEMR datasets	Mean accuracy 89.56% with 25% false alarm reduction.	High energy consumption and the lack of datasets containing advanced attacks
[26]	Region based IoT for IDS	ICOA-IT2FDL, BES	CIFAR-100, CICIoT2023	AUC 0.865 with precision 0.912	Misidentification in network behavior results in a potentially higher volume of false alarms
[27]	Intelligent CNN for IoT IDS	Synaptic Intelligent CNN	CIC IDS2017, CICIoT2023	Achieves a high detection rates as 92.36%	Faces challenges with class imbalances and evolving attack patterns.

[28]	IoT cyber attack detection	XGBoost, LGBM, SMOTE	RT-IoT2022	High detection accuracy 99.65%	Limited by insufficient training causes more training time
[29]	Transfer learning-based IDS	CNN, Random Search	CSIC dataset	Achieved 10.44 % accuracy increase	Poor detection performance for complex features.
[30]	Game theory-based adaptive security	GT-AS, Recurrent Bat Algorithm	CSE-CIC-ID2018	47% longer device lifespan, improved accuracy	Limited by lower transparency, lower explainability

Statistical features such as the average, variance, and standard deviation of packet transfer, temporal features that capture time-dependent attack behaviors, and behavior-based features that analyze the number of connections per second, and protocol-specific behaviors are extracted. The dual-resnet model effectively captures both low-end and high-end features, leading to an accurate feature set for ITS. After feature extraction, feature selection is carried out using Multi-Objective Optimization (MCO) algorithm, which reduces the computational complexity while indicating the accuracy. It enhances semi-optimized optimization by implementing adaptive mutation strategies for efficient feature study and dynamic fitness assessment in favor of more significant features. By eliminating unnecessary and irrelevant features, MCO reduces the computational load and improves the processing speed, which makes IDS more efficient for real-time applications. FF-ANN consists of an input layer that receives optimized features, multiple hidden layers with non-linear execution functions such as ReLU to learn complex attack methods, and an output layer with SoftMax execution functionality to classify network traffic as normal or malicious. FF-ANN is trained with Adam Optimizer using the backward propagation algorithm, which ensures rapid integration and high classification accuracy. The AI-based IDS system integrated with blockchain provides a more efficient and scalable solution to protect IoT ecosystems and address key security challenges such as DDoS attacks, high false alarm rates, scalability issues, and resource constraints. It is capable of protecting ITS IoT networks from cyber threats and providing increased security and network reliability.

Journal of Theoretical and Applied Information Technology
15st July 2026. Vol.104. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

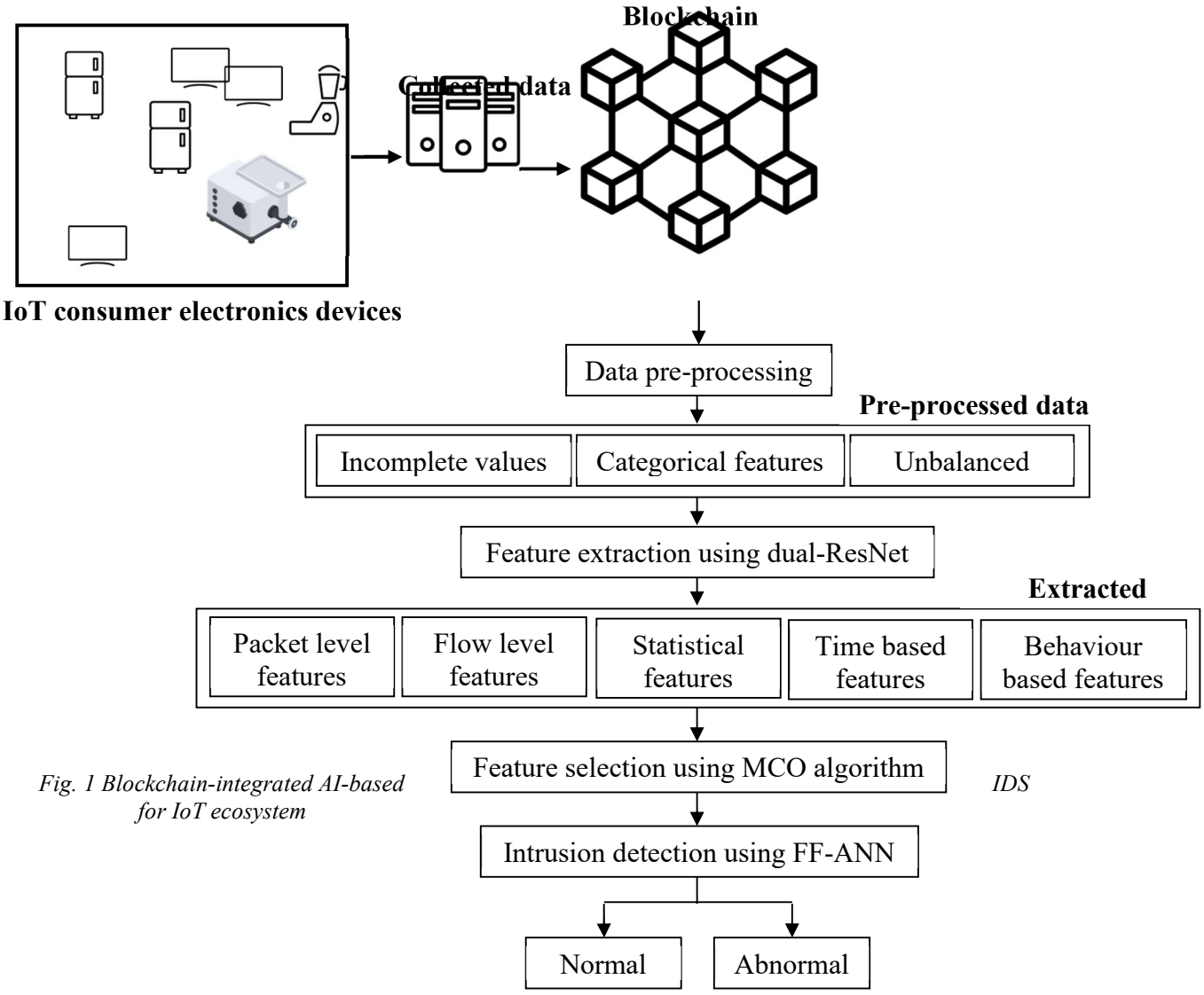


Fig. 1 Blockchain-integrated AI-based IDS for IoT ecosystem

3.1 BLOCKCHAIN TECHNOLOGY

Blockchain is a real explanation for enhancing security in electronic devices for consumers, utilizing its decentralized and tamper-resistant structure. Blockchain is an effective solution for enhancing security in electronic devices for consumers, utilizing its decentralized and tamper-resistant structure. Blockchain is a well-known form of distributed ledger technology (DLT) that ensures data integrity and security through consensus mechanisms. Each transaction in the blockchain network requires verification by the majority of participating nodes before being added to the ledger, ensuring transparency and reliability. The communications are collected into blocks and the blocks are linked together with a cryptographic hash function, forming a chain of blocks. Each block has a unique hash code unique to itself and securely connected to the hash code of the previous block, which helps to ensure that the data is authentic and can't be altered.Each player in the network has the same copy of the distributed ledger, making it possible to synchronize constantly and get up-to-date information. Its transparency makes it easy for all nodes to see the transaction made in real-time, which means that there are fewer intermediaries and more efficient work. By breaking down the need for trusted third parties and the centralization of trust, blockchain can help to create a more secure and efficient workflow, reducing the risk of potential pitfalls that could compromise the system. Blockchain employs cryptographic security mechanisms like Public Key Infrastructure (PKI)

and digital signatures, ensuring secure authorization and data protection [33].

Such security measures help safeguard the network against any malicious activity, unauthorized access, or cyber threats. Apart from the above, consensus mechanisms within blockchain projects add an extra layer of trust, ensuring that transactions are only added to the blockchain once they have been verified. The addition of blockchain with IoT provides a robust solution to reduce security threats in smart consumer electronics. By combining blockchain with the Internet of Things ecosystems, enterprises can enjoy enhanced security, data integrity, and efficiency, and overcome multiple challenges like unauthorized access, data manipulation, and cyber attacks. This integration will not only bolster the cybersecurity capabilities of the ROHDE & RICHTER solution, but will also open the door to a secure and transparent IoT environment.

3.2 DATA PREPROCESSING

Blockchain is a well-known type of distributed ledger technology (DLT) [32], which uses consensus mechanisms to ensure data integrity and security. Each transaction has to be confirmed by most of the nodes on the network before it can be added to the ledger, which makes the Blockchain network transparent and reliable. The transactions are organized into blocks, which are linked to each other using a cryptographic hash function, forming a chain of blocks. Blockchain can be used to enhance consumer electronics security. Each block has a timestamp and a unique hash, that securely links it to the previous block, thereby ensuring the authenticity of the data and making it impossible to alter it without being caught. The blockchain guarantees everyone on the network keeps an identical copy of the distributed ledger, enabling continuous synchronisation and real-time updates. The transparency of the system ensures that every node participating in the network can check transactions in real-time, thus eliminating intermediaries and boosting efficiency.

Through the decentralization of trust and the elimination of third-party dependency, Blockchain promotes a more secure and efficient workflow, preventing possible gaps that could compromise the integrity of the system. Public key infrastructure (PKI) and digital signatures are some of the security mechanisms used in blockchain for secure authorization and protection of data [33].

These security features effectively protect the network from malicious activities, unauthorized access, and online threats. The consensus mechanisms of blockchain also help to build trust, as they ensure that only approved transactions are added to the ledger. A widely effective method to curtail security threats in smart consumer gadgets is the combination of blockchain and Internet of Things technology. The combination of blockchain and IoT can help enterprises enhance operational efficiency, security, and data integrity while mitigating cyber threats, data manipulation, and unauthorized access to IoT devices. In addition to enhancing cybersecurity, this combination opens the door to a trustworthy and open IoT ecosystem.

3.3 FEATURE EXTRACTION

In order to enhance the performance and accuracy of data processing, feature combination is one of the methods of data preparation by identifying and selecting the most relevant features from the raw data [36]. The goal of the feature extraction process is to capture the relevant information, including packet based features, flow based features, statistical patterns, time based behaviors and anomaly indicators involved in the interruption recognition of blockchain-based IoT systems. Feature extraction has the effect of reducing the dimensions of the data, increasing detection efficiency, and understanding the model by converting the raw data of network traffic to useful features. The dual-ResNet model was employed, where the deep learning architecture of the ResNet network is used to extract hierarchical features from network traffic data, resulting in effective feature extraction. Deep convolutional neural network (CNN) is applied, namely residual network (ResNet) to overcome the problem of gradient disappearance and enhance feature learning while performing this work[37].

The dual-ResNet model contains of two parallel ResNet networks, each aimed at extracting different groups of features to enhance the IDS's detection capability. One ResNet branch focuses on packet-level and flow-level features, capturing low-level spatial and temporal characteristics of network traffic. The dual-ResNet extracts statistical and behavior-based features, identifying deviations in network traffic patterns that may signify potential intrusions. Each ResNet block consists of multiple convolutional layers surveyed by batch regularization and start function, with residual connection ensuring gradient flow and efficient learning. The dual-ResNet model is used to establish BB_l relationships based on low-confidence data using the labeled inputs p_l and q_l outputs, which can be defined as follows.

$$q_l = BB_l(p_l) \quad (1)$$

The trainer BB_l is used to obtain prediction results with the input of a real high-fidelity data set, p_I and the corresponding results can be defined as follows.

$$q_l^X = BB_l(p_I) \quad (2)$$

Residuals between predicted results q_l^X and actual high-precision data set q_I results.

$$q_e = q_I - q_l^X \quad (3)$$

A high-fidelity model was industrialized BB_I to estimate the connection among the residuals q_e and the original high-fidelity p_I contributions, with the corresponding results q_e^X :

$$q_e^X = BB_I(p_I) \quad (4)$$

where $q_l^X + q_e^X$ the final forecast is considered as the results, but there still be a small deviation. A linear regression model $q_l^X + q_e^X$ as the dependent variable and the high precision data q_I output as the dependent variable were retrained and used to increase the stability of the dual-ResNet output with the following results

$$q_{Mr} : q_{Mr} = d_1\left(q_l^X + q_e^X\right) + d_2 \quad (5)$$

where d_1 and d_2 are the linear regression coefficients that can be determined using the method

5. The stability of the Mr-BB output with the following results q_{Mr} :
$$q_{Mr} = d_1\left(q_l^X + q_e^X\right) + d_2$$
6 Define the control variables for maximum threshold set
$$[e, v, \varphi, d] = BB_l[K_b, \lambda, \sigma_s, d_n, \wedge, \delta]$$
7. The final foreseen values of MR-NN, taking e as an sample,
$$[e]_{Mr} = d_1(e + \Delta e) + d_2$$
8. LF and HF data are pre-processed using min-max normalization
$$p' = \frac{p - p_{Min}}{p_{Max} - p_{Min}}$$
9. Find the best value
10. End

of least squares. 'x' denotes the predictions, and the subscripts 'e', 'l' and 'i' denote the residuals, LF and HF data, respectively. Once BB_l and BB_H , the linear regression coefficients are obtained, the predictions are calculated after traversing the entire computational frame. According to the inputs and outputs BB_l , obtained as follows:

$$[e, v, \varphi, d] = BB_l[K_b, \lambda, \sigma_s, d_n, \wedge, \delta] \quad (6)$$

In BB_H , the relatives between outstanding q_e and actual inputs can be found by:

$$[\Delta e, \Delta v, \Delta\varphi, \Delta d] = BB_I[K_b, \lambda, \sigma_s, d_n, \wedge, \delta] \quad (7)$$

The final foreseen values of dual-ResNet, taking e as sample which computes as follows.

$$[e]_{Mr} = d_1(e + \Delta e) + d_2 \quad (8)$$

The dual-ResNet is used to construct BB_l and BB_H use. The self-adaptive optimizer Adamax, which is a combination of Adagradin and RMSprop, is adopted because it outperforms sparse data. A corrected linear unit (ReLU) activation function was adopted to avoid vanishing gradient. To eliminate the scaling effect of different variables on model performance and improve the generalization ability of dual-ResNet, all samples including LF and HF data are pre-processed using min-max normalization.

$$p' = \frac{p - p_{Min}}{p_{Max} - p_{Min}} \quad (9)$$

where p and p' are raw and processed standards of variables, individually; p_{Min} and p_{Max} are smallest and supreme values of conforming variable star, respectively.

Algorithm 1 defines the waged procedure of feature extraction using dual-ResNet.

Algorithm 1 Feature extraction using dual-ResNet

Input : Traffic traces, number of targets, maximum objective function
Output : Extracted features

1. Begin;
2. Initialize the step sizes of the population
3. The low-confidence data using labelled inputs p_l and q_l outputs, $q_l = BB_l(p_l)$
4. Residuals between predicted results q_l^X and actual high-precision data set q_I results, $q_e = q_I - q_l^X$

3.4 FEATURE OPTIMIZATION

In this context, the feature optimization improves classification accuracy, reduces computational complexity, and enhances real-time intrusion detection. By refining the feature set, the

model can process critical information more efficiently, leads to more precise threat identification. To achieve effective feature optimization, the modified coati optimization (MCO) algorithm is used for feature selection. MCO is an enhanced version of the coati optimization algorithm (COA) [38], a bio-inspired metaheuristic algorithm based on the foraging and social behaviors of coati mammals. The original COA mimics the way coatis explore, exploit, and select food sources in a structured manner, making it well-suited for feature selection tasks where the goal is to identify an optimal subset of features from high-dimensional data. The MCO algorithm improves upon COA by integrating adaptive weight adjustments and an improved search mechanism to balance exploration and exploitation more effectively. It evaluates the relevance of each feature based on a fitness function that considers classification accuracy and redundancy minimization. In this context, the place of the coatis in examine space is haphazardly produced for the MCO algorithm by consuming the objective function as follows.

$$P_h: p_{h,g} = b_g^l + Rand(0,1) \cdot \left(n_g^U - n_g^L\right), \quad h = 1,2,\ldots,B, g = 1,2,\ldots,a \qquad (10)$$

P_h Signifies the place of h-th coati in the exploration space and the $p_{h,g}$ worth of the g-th outcome variable. n_g^L and n_g^U represent denote the higher and lesser bounds of the outcome variables. B is the Got is number; a is the numeral of conclusion variables. In MCO algorithm, the best population member is assumed to be an iguana.

$$P_h^{X1}: p_{h,g}^{X1} = p_{h,g} + Rand(0,1) \cdot \left(J_g - Hp_{h,g}\right), h = 1,2,\ldots,\left[\frac{B}{2}\right], g = 1,2,\ldots,a \qquad (11)$$

wherever, $p_{h,g}^{X1}$ is the new location of the h-th column in the g-th measurement; R is a random number among [0,1]; J_g the position of the iguana in the g-th dimension, which really represents the point of the best member; H is a number chosen at random from the set {1,2}; B is the millionth number; [B/2] is the largest integer [B/2]; a is the number of result variables.

$$J^j: J_g^j = n_g^L + Rand(0,1)\left(n_g^U - n_g^L\right) \qquad (12)$$

where: J_g^j is the location of the iguana on the pulverized in the g element.

$$P_h^{X1}: p_{h,g}^{X1} = \begin{cases} p_{h,g} + Rand(0,1) \cdot \left(J_g^j - Hp_{h,g}\right), f_{J,g}^j \le f_{h,g} \\ p_{h,g} + Rand(0,1) \cdot \left(p_{h,g} - J_g^j\right), other \end{cases}$$

$$h = [B/2] + 1, [B/2] + 2, \ldots, \rightleftarrows B, and g = 1,2,\ldots,a \qquad (13)$$

where: $f_{J,g}^j$ is the detached function value of the g-th dimension iguana after it falls to the ground; $f_{h,g}$ is the objective meaning value of the h-th Coati in g-th measurement. If the rationalized separate is recovering, the present distinct is efficient.

$$P_h = \begin{cases} P_h^{X1}, f_h^{X1} \le f_h \\ P_h, \quad other \end{cases} \qquad (14)$$

where: f_h^{X1} the charge of the impartial purpose of the coefficient h in the new state; f_h the value of the dispassionate purpose of the h-th segment in the previous state. In the exploitation phase, the location optimization strategy reflects the behavior of confronting predators and obtaining food from predators. In the mistreatment stage, when a hunter occurrences the tiger, the tiger calculates its location. A random location of MCO algorithm is generated near each node location based on the following equation.

$$n_{g,L}^{loc} = \frac{n_g^L}{s}, n_{g,U}^{loc} = \frac{n_g^U}{s}, s = 1,2,...,S \qquad (15)$$

where: $n_{g,L}^{loc}$ is the local subordinate bound of the g-th conclusion flexible, $n_{g,U}^{loc}$ is the local upper bound of the g-th decision adjustable, and s is the quantity of restatements; s is the extreme number of reiterations.

$$\begin{cases} P_{h,g}^{X2} = p_{h,g} + (1-2R)\left(n_{g,L}^{loc} + R\left(n_{g,U}^{loc} - n_{g,L}^{loc}\right)\right) \\ h = 1,2,...,B \end{cases} \qquad (16)$$

where: $P_{h,g}^{X2}$ the new location of the h coordinate in the g dimension. Update the present person or leave it alone if the updated person is superior. The search efficiency of the MCO method will be increased if the chaotic mapping function is utilized to create a random order of population members as an initial state in order to prevent population homogeneity and make the populace circulation more unchanging. The populace distribution resulting from tentacle perturbations has better homogeneity in large perturbation graphs above. Here, utilizes tentacle chaos to improve the quality of the initial population distribution in the search space, and also enhance the global search [39] ability to improve the solving ability of the algorithm.

$$P_h: p_{h,g} = n_g^l + \left(n_g^U - n_g^l\right) \cdot w_h \qquad (17)$$

The countenance of the tent planning was shown in

$$w_{h+1} = \begin{cases} \frac{w_h}{\alpha}, \mid p_{h,g} \in [0,\alpha) \\ \frac{1-w_h}{1-\alpha}, \mid p_h \in [\alpha,1) \end{cases} \quad (18)$$

The combined metaheuristic algorithm's local optimization efficiency and global search efficiency are significant determinants of the algorithm's optimization speed and accuracy. The correlation between the coat position update and the current coat position data is modified using a nonlinear inertial weighting factor.

$$\omega = E^{\frac{s}{S}} - 1/E - 1 \quad (19)$$

anywhere S is the maximum sum of repetitions and s is the sum of repetitions that are currently occurring. As the maximum inertial weight $\omega_{\max} = 1$ increases with the iteration improvement, the inertial load coefficient increases nonlinearly and finally reaches large value. The enhancement factor of MCO algorithm is defined as follows

$$P_h^{X1}: p_{h,g}^{X1} = \omega \cdot p_{h,g} + Rand(0,1) \cdot (J_g - Hp_{h,g}), h = 1,2,\ldots,\left[\frac{B}{2}\right], g = 1,2,\ldots,a \quad (20)$$

$$\square_h^{X1}: p_{h,g}^{X1} = \begin{cases} \omega \cdot p_{h,g} + Rand(0,1) \cdot (J_g^j - Hp_{h,g}), f_{J,g}^j \le f_{h,g} \\ \omega \cdot p_{h,g} + Rand(0,1) \cdot (p_{h,g} - J_g^j), else \end{cases},$$

$$h = \left[\frac{B}{2}\right], 2, \ldots B; g = 1,2,\ldots,a \quad (21)$$

The variation of the nonlinear inactivity weight factor is updated during the iteration. Starting at zero, the nonlinear inertia weight factor rises to one. Only the most discriminative characteristics are kept after iteratively refining potential feature subsets during the optimization phase. This leads to a smaller feature set, which reduces computational overhead and, by reducing the chance of over fitting, improves the model's capacity for generalization. As shown in Algorithm 2, this optimization process reduces false alarms, improves detection speed, and ensures that only the most relevant packet-level, flow-level, statistical, time-based, and behavior-based features are used in securing IoT ecosystems.

Algorithm 2 Feature selection using MCO

Input : Sum of characteristics, maximum iterations, end situation
Output : Ideal top characteristics

1. Begin;
2. Prepare the step sizes of the population
3. Define coatis in search space is haphazardly produced for the MCO,
$P_h : p_{h,g} = b_g^l + Rand(0,1) \cdot (n_g^U - n_g^L), h =$
4. Fix the minimum and maximum threshold for rule-set
$J^j : J_g^j = n_g^L + Rand(0,1)(n_g^U - n_g^L)$
5. A random location is generated near each node location
$n_{g,L}^{loc} = \frac{n_g^L}{s}, n_{g,U}^{loc} = \frac{n_g^U}{s}, s = 1,2,\ldots,S$
6. The current distinct is updated.
$P_h = \begin{cases} P_h^{X1}, f_h^{X1} \le f_h \\ P_h, \quad other \end{cases}$
7. Compute the nonlinear inertial weighting factor $\omega = E^{\frac{s}{S}} - 1/E - 1$
8. Fix the fitness using enhancement factor is as follows
$P_h^{X1} : p_{h,g}^{X1} = \omega \cdot p_{h,g} + Rand(0,1) \cdot (J_g - I$
9. Discover the top production worth
10. End

3.5 INTRUSION DETECTION SYSTEM

After the feature selection, where redundant and non-informative attributes are eliminated, the optimized feature set is fed into the Feed-Forward Artificial Neural Network (FF-ANN) for intrusion detection and organization. The FF-ANN consists of several layers, from the input layer that accepts the features selected from the network traffic as its input. These features are taken as specific input neurons of the network that correspond to different characteristics of the network. The hidden layers work out the data by way of weighted connections and activation features such as ReLU or Sigmoid, allowing the mannequin to pick up intricate patterns and relationships in the information [40]. Then, the production level returns the end classification result, which is either normal traffic or different kinds of cyber attacks such as DDoS, phishing and malware. The training process of the FF-ANN consists of inputting the IoT traffic data with its label into the network, which learns the attack patterns via back-propagation and optimization.. During real-time intrusion detection, incoming IoT network traffic undergoes preprocessing and feature extraction before being

analyzed by the trained FF-ANN model. To further enhance security, blockchain is integrated, ensuring that all intrusion detection logs are stored in decentralized, tamper-proof ledger, prevent unauthorized design and maintaining data integrity. Duo to its simplicity and efficiency, an evolutionary algorithm used here for training the ANN and achieved some achievements. The output of FF-ANN is describes as follows [41].

$$S_p = F_p\left(\sum_{q=1}^{b} w_{q,p} m_q + n_p\right) \quad (22)$$

where pn denotes the node's bias, pF provides the node transfer function, qm is the qth input, $w_{q,p}$ is the connection parameter, and S_p contributes the node's output. The following is one technique to express the fitness function as an optimization problem:

$$e(w(s)) = \frac{1}{b}\sum_{q=1}^{b}\sum_{K=1}^{k}(O_{K,E} - O_{K,m})^2 \quad (23)$$

where the fault and limits in the conjunctions at the s-th iteration are donated by e(w(s)) and w(s), respectively. The numbers p and k stand for the number of patterns and output nodes, respectively. The definite worth of the K-th production node is denoted by ka, O, whereas the predicted worth is denoted by kE, O.

$$Y^A X^B(Y) = F(Y, X(Y), X'(Y)), \quad (24)$$

Specific BCs and m ∈Z, x ∈ R, D ⊂ R denote the realm, and X(Y) is the approximate result. If $X_s(Y,J)$ adjustable parameters represent optimal solution using q, the issue is malformed into a specific form.

$$\min_j \sum_{Y_q \in \vec{d}} F(Y_q, X_T(Y_q, J), X_T'(Y_q, J)) \quad (25)$$

An FF-ANN is used in the trial solution Y, and the parameters p stand for the neural architecture's weights and biases. ANN model has been broadly used in different fields of hydro-environmental engineering as a temporal forecasting [42]. The explicit function is used to determine the production value of an ANN is attained as trails.

$$\hat{X}_p = F_p[\sum_{G=1}^{A} W_{pG} \times F_G(\sum_{q=1}^{N} W_{qG} Y_q + W_{Gm}) + W_{pm}]$$

(26)

as follows: q, G, p, a, and W stand for the neurons in the levels of input, hidden, and output, as well as the bias and applied weight through the neuron, respectively; denote the function of activation for the hidden and results layers, respectively; F_G F_q, B, A represent the variables in the input layer Y_q, the sum of input and hidden neurons $\hat{X}_p$, and the productivity neuron's detected and computed worth, respectively. The ideal controller creates a recite probability for each memory location q based on the observed previous trajectories and the context ((π^k , γ^k)). Then, do the following [43] to calculate a context read similarity and a previous read similarity:

$$T_\pi^j = \frac{\pi^K \cdot \pi^q}{\| \pi^K \| \| \pi^q \|} \quad j = 0,.....,|a| \quad (27)$$

$$T_\gamma^q = \frac{\gamma^K \cdot \gamma^q}{\| \gamma^K \| \| \gamma^q \|} \quad q = 0,.....,|a| \quad (28)$$

Then feed the threshold sets T_π^j and T_γ^q to an F-network, which is multi-layer and feed-forward, and which is taught to provide excellent results for samples of interest and low ratings for the rest based on a combination of read similarity, prior significance, and contextual.

$$J(R)^q = F(T_\pi^q, T_\gamma^q) \quad (29)$$

Obtaining multiple mediums is as easy as reading the top-K values with the greatest score at judgment time $J(R)^q$, as each memory sample may be retrieved and interpreted separately. The test solution X_T FF-ANN is used, and i parameters match the weight and dependence of the neural structure. For the test operation used to choose the form $X_T(Y)$ that satisfies the objective function [44].

$$X_T(Y_q, J) = N(Y) + h(Y, b(Y, i)), \quad (30)$$

in which the input vector Y is routed into B input units of a single-output FF-ANN with variables j. The fitness function is satisfied by the term, which does not have any modifiable parameters.

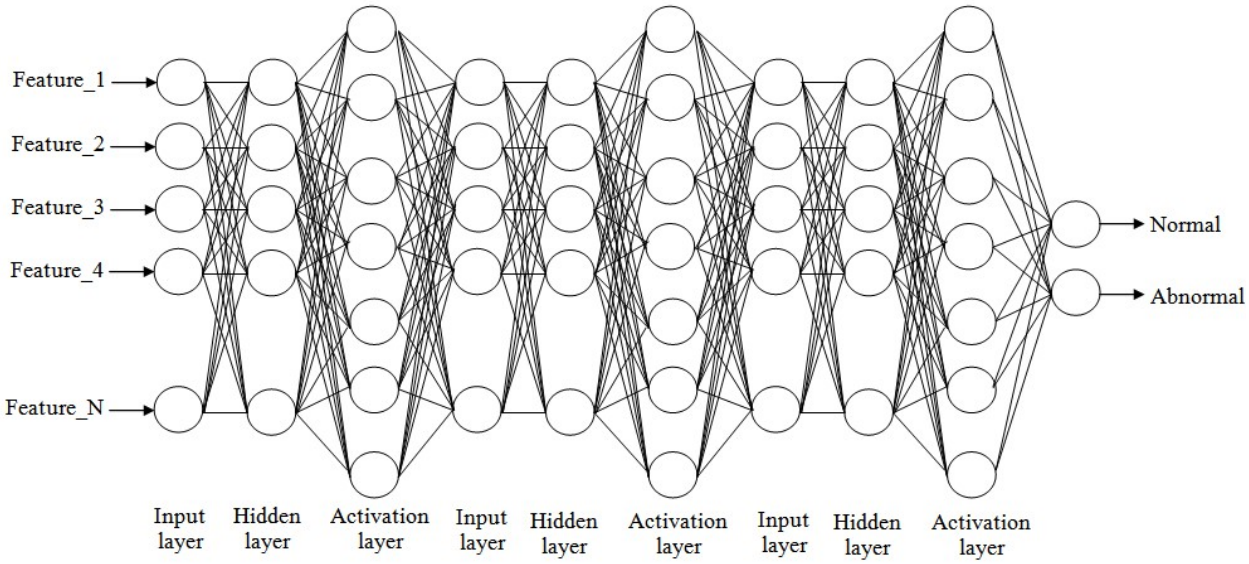


Fig. 2 Layer-wise design of FF-ANN for IDS

The second term g is the fitness function [45], since $X_T(Y)$ satisfy them. For a given input y, the output of the FF-ANN is defined as tails.

$b = \sum_{q=1}^{G} \nu_q \sigma(w_q), where w_q = \sum_{p=1}^{b} w_{qp} Y_p + m_q$ (31)

w_{qp} is a rectangular transferring function (tansig.), where q is an input unit representing the load that links the veiled component to q ν_q, q is an output unit m_q representing the dependency of q, and $\sigma(w)$ is a sigmoidal handover purpose.

$$\frac{\partial b}{\partial \omega_{qp}} = \nu_q \sigma'(w_q) Y_p, \quad (32)$$

As shown in Fig. 2, FF-ANN in the IDS offers several advantages, including high detection accuracy, reduced false alarms, real-time threat mitigation, and improved scalability for handling large-scale IoT networks. By using DL-based IDS and blockchain-driven security mechanisms, it provides a robust, efficient, and real-time cyber security to safeguard IoT ecosystems.

Table 2 Description of dataset

Type of events	ToN-IoT dataset	CICIDS-2017 dataset
Backdoor	2,500	-
Botnet	-	2,500
Dos	2,500	2,500
DDoS	2,500	2,500
Injection	2,500	-
MITM	1,000	-
Scanning	2,500	-
Ransomware	2,500	-
Password	2,500	-
XSS	2,500	-
Brute force	-	2,500
Infiltration	-	1,000
Web attacks	-	2,500
Heartbleed	-	2,500

Port scan	-	2,500
Normal	2,500	2,500
Total data records	23,500	23,500

4. RESULTS AND DISCUSSION

This section presents the results and comparative analysis of IDS models evaluated on two datasets: ToN-IoT and CICIDS2017 [31]. A statistical summary of these datasets is given in Table 2. The figures, which were gathered from a real-world testing track at UNSW Canberra, include network traffic recorded during replicated intrusions like DoS and ransomware, Windows operating system data, and telemetry data from many IoT devices. A machine with an i 5-8600 k CPU, 250GB SSD, 4GB GeForce 1050Ti graphics card, 16GB RAM and 1TB HDD was used to build the suggested model using Python 3.6.5. The model parameter settings were as follows: learning rate of 0.01, ReLU activation, 50 epochs, a dropout rate of 0.5, and a batch size of 5.

Table 2 provides a comparative analysis of the TON-IoT and CICIDS-2017 datasets, both of which are widely used for the evaluation of IDS in IoT environments and network security. There are 23,500 data records in each dataset, encompassing both normal network activity and different cyberthreats. Internet of Things security risks, such as 2,500 backdoors, 2,500 DoS, 2,500 DDoS, 2,500 injections, 1,000 MITM, 2,500 scans, 2,500 ransomware, 2,500 passwords, and 2,500 XSS, are the focus of the TON-IoT dataset. These assaults are typical examples of security flaws in IoT networks, when hackers take advantage of flaws in linked equipment. In contrast, the CICIDS-2017 dataset captures a variety of network-based intrusions, including Botnet 2,500, DoS 2,500, DDoS 2,500, Brute Force 2,500, Infiltration 1,000, Web Attacks 2,500, Heartbleed 2,500, and Port Scan 2,500. These threats target traditional IT infrastructures and include attacks such as credential breaches, unauthorized access, and denial of service. To guarantee that the trained models can discriminate between benign and malevolent activity, each datasets include 2,500 regular records. Table 2 presents a statistical overview of these datasets. The estimates were collected from a real test track at UNSW Canberra and include telemetry data from various IoT sensors, Windows operating system data, and network traffic captured during simulated cyber attacks such as DoS and Ransomware.

The proposed model was implemented using Python 3.6.5 on a computer with an i5–8600k processor, 250GB SSD, GeForce 1050Ti 4GB graphics card, 16GB RAM, and a 1TB hard drive. The model parameter settings were as follows: a learning rate of 0.01, ReLU activation, 50 epochs, a dropout rate of 0.5, and a batch size of 5. Table 2 presents a comparative analysis of the ToN-IoT and CICIDS-2017 datasets, which are widely used for evaluating IDS in IoT environments and network security. Each dataset consists of 23,500 records, encompassing various cyber threats and normal network traffic. The ToN-IoT data system focuses on security threats related to the Internet of Things, including 2,500 Backdoor, 2,500 DoS, 2,500 DDoS, 2,500 Injection, 1,000 MITM, 2,500 Scanning, 2,500 Ransomware, 2,500 Password, and 2,500 XSS.

These attacks represent common vulnerabilities in IoT networks, where attackers exploit weaknesses in connected devices. In contrast, the CICIDS-2017 database documents various network breaches, including Botnet 2,500, DoS 2,500, DDoS 2,500, Brute Force 2,500, Infiltration 1,000, Web Attacks 2,500, Heartbleed 2,500, and Port Scan 2,500. These threats pertain to traditional IT infrastructures and include attacks such as authentication breaches, unauthorized access, and denial of service attacks. Two databases contain 2,500 regular records to ensure that the trained models can distinguish between legitimate and malicious activities.

The balanced data distribution across multiple attack types enhances the effectiveness of AI-based IDS models in detecting and mitigating cyber security threats in diverse network environments.

4.1. RESULTS COMPARISON ON TON-IOT DATASET

The intrusion detection results as shown in Table 3 for the ToN-IoT dataset, based on an 80/20% split of training and testing samples, indicate robust model performance across various attack categories. For the training phase 80%, the model achieved high accuracy across all classes, with values ranging from 98.126 to 98.628. The highest accuracy was observed for the Scanning attack at 98.628, followed by MITM at 98.567 and Injection at 98.452. Precision values were also significantly high, with Scanning achieving the highest precision of 93.509, while MITM had the lowest at

86.759, indicating slightly lower confidence in positive predictions for this attack type. Sensitivity represents the model's ability to correctly identify positive cases, varied, with the highest value observed for Scanning at 94.286 and the lowest for MITM at 75.328, suggesting that MITM attacks were harder to detect.

Specificity remained consistently high across all classes, with values above 98.8, confirming the model's strong ability to correctly classify non-attacks. The F-measure, which balances precision and recall, also reflected strong performance, with Scanning achieving the highest score at 93.899 and MITM the lowest at 80.609. The area under the curve (AUC) values, ranging from 87.457 to 96.713, indicates strong discriminatory power, particularly for Scanning attacks. The Matthews correlation coefficient (MCC), a robust metric for evaluating classification performance, showed its highest value for Scanning at 92.385 and lowest for MITM at 76.809, further emphasizing challenges in detecting MITM attacks. The Dice coefficient, similar to the F-measure, confirmed that Scanning at 94.015 was detected most effectively, while MITM at 81.448 was the least well-detected class. For the testing phase 20%, the model's performance remained consistent, with accuracy values ranging from 98.537 to 98.957, showing a slight improvement compared to the training phase.

The highest accuracy was achieved for Scanning at 98.957, followed by MITM at 98.924 and Injection at 98.765. Precision values saw an increase, with Scanning achieving the highest at 94.519 and MITM remaining the lowest at 88.519. Sensitivity scores were also slightly improved, with Scanning leading at 95.818 and MITM remaining the weakest at 80.018. Specificity values were close to perfect, all above 99, indicating excellent classification of non-attack samples.

The F-measure reflected a similar trend, with Scanning at 95.159 performing the best and MITM at 83.919 the weakest. The AUC values improved slightly, ranging from 89.012 for MITM to 97.019 for Scanning, further reinforcing the model's effectiveness. MCC values also improved slightly, with Scanning reaching 93.819 and MITM still being the lowest at 79.818, suggesting that despite slight improvements, MITM attacks remain challenging to detect. The Dice coefficient followed the same trend, with Scanning at 95.319 leading and MITM at 85.015 lagging behind. The results demonstrate that the model performed exceptionally well across most attack classes, particularly for Scanning, Password, and Injection attacks, which consistently achieved high accuracy, precision, and sensitivity.

Fig. 3 depicts the results of the proposed dual-ResNet+MCO+FF-ANN model on the ToN-IoT dataset shows strong learning and generalization capabilities. The accuracy steadily increases from 50.214% at epoch 0 to 99.787% at epoch 250 for training and from 48.129% to 99.718% for validation, showing a consistent improvement.

The loss curve exhibits a sharp decline, starting from 1.892 for training and 1.945 for validation at epoch 0, reducing to 0.087 and 0.228 at epoch 250, respectively. This indicates effective convergence with minimal overfitting, as training and validation performance remain closely aligned. The model achieves high stability and optimal classification performance, making it well-suited for intrusion detection tasks.

Fig. 4 shows the PR curve analysis for the proposed dual-ResNet+MCO+FF-ANN model on the ToN-IoT dataset demonstrates high precision and recall across all attack types and normal traffic, highlighting its effectiveness in intrusion detection. The model achieves close to 99% precision for most attack classes at lower recall levels, ensuring minimal false positives. As recall increases, a slight drop in precision is observed, particularly for scanning, Ransomware, and injection attacks, indicating a trade-off between identify more true positives while maintaining accuracy.

Backdoor, DoS, and password attacks consistently maintain precision above 99%, even at higher recall values, demonstrating the model's robustness in detecting these threats. However, scanning and Ransomware attacks exhibit a gradual precision decline, reaching around 80-90% at higher recall levels, suggesting a relatively higher false positive rate for these attack types. Normal traffic classification remains highly accurate, with precision nearing 99.9%, ensuring minimal

misclassification of benign data. The model maintains strong detection capabilities with minimal precision degradation, making it a highly reliable solution for intrusion detection in real-world ToN-IoT environments.

The ROC curve for the model that was expected to be the dual-ResNet+MCO+FF-ANN model on the ToN-IoT dataset is shown in Fig. 5, which represents the model's performance depending on the attack categories, including Backdoor, DoS, DDoS, Injection, MITM, Scanning, Ransomware, Password, XSS, and Normal.

The false positive rate (FPR) is systematically tested to achieve the true positive rate for each attack type, and its detection rate is gradually increased along with the increase in FPR.

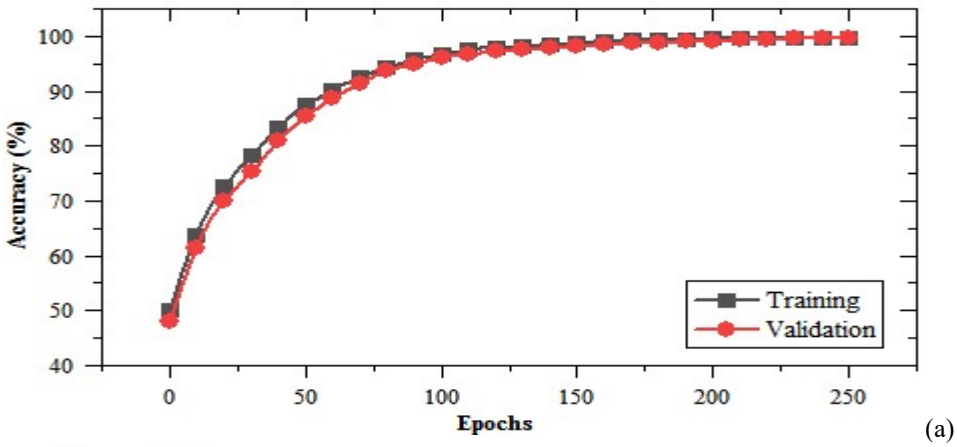
The model is gradually improving its classification accuracy, and the attack detection rate has been increasing steadily in all categories. The model exhibits good separation at lower FPR values with relatively high true positive rate and low false positive rates. The true positive rate for each attack type tends towards the maximum detection potential as the FPR increases, while the Normal traffic always increases controlled. The continuing increases in detection rates for each of the attack types indicates that the hybrid method is effective in learning the complex attack pattern without the significant misclassification error.

Table 3 Intrusion Detection Results Of Ton-Iot Dataset On 80/20% Of Training And Testing Samples

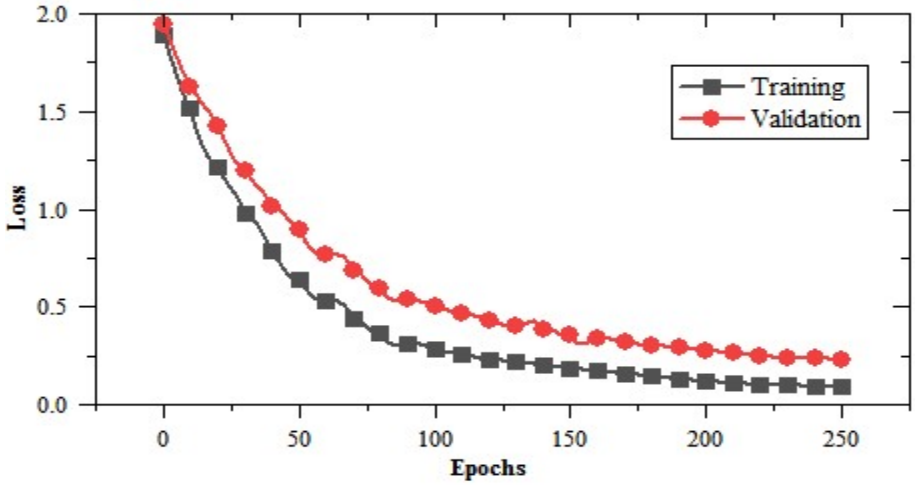
Classes	Values in %							
	Accuracy	Precision	Sensitivity	Specificity	F-measure	AUC	MCC	Dice
Training (80%)								
Backdoor	98.126	90.457	89.319	99.023	89.871	94.556	88.159	89.935
DoS	98.315	91.128	90.746	99.115	90.937	95.228	89.415	91.059
DDoS	98.284	91.689	89.853	99.213	90.768	94.887	89.338	90.918
Injection	98.452	91.947	91.227	99.253	91.587	95.407	90.127	91.398
MITM	98.567	86.759	75.328	99.659	80.609	87.457	76.809	81.448
Scanning	98.628	93.509	94.286	99.415	93.899	96.713	92.385	94.015
Ransomware	98.159	88.613	92.107	98.813	90.319	95.428	89.019	91.188
Password	98.412	91.229	92.159	99.117	91.689	95.787	90.529	91.907
XSS	98.135	90.789	89.999	99.008	90.389	94.827	89.149	90.487
Normal	98.217	90.569	91.457	99.008	90.999	95.209	90.107	91.289
Testing (20%)								
Backdoor	98.537	91.215	90.509	99.319	90.859	95.118	89.519	90.889
DoS	98.624	92.319	91.819	99.417	92.057	95.512	90.619	91.928
DDoS	98.732	92.919	91.618	99.558	92.267	95.815	90.915	92.117
Injection	98.765	93.215	92.518	99.612	92.859	96.012	91.215	92.415
MITM	98.924	88.519	80.018	99.818	83.919	89.012	79.818	85.015
Scanning	98.957	94.519	95.818	99.759	95.159	97.019	93.819	95.319
Ransomware	98.861	90.319	93.009	99.319	91.619	96.012	90.519	92.219
Password	98.915	93.519	94.219	99.618	93.859	96.519	92.019	94.019
XSS	98.815	92.519	91.819	99.559	92.159	95.919	90.719	92.019
Normal	98.869	93.219	93.519	99.618	93.359	96.319	91.919	93.419

Journal of Theoretical and Applied Information Technology
15st July 2026. Vol.104. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



(a)



(b)

Fig. 3 Results Of Proposed Dual-Resnet+MCO+FF-ANN Model (A) Accuracy (B) Loss Curve For Ton-Iot Dataset

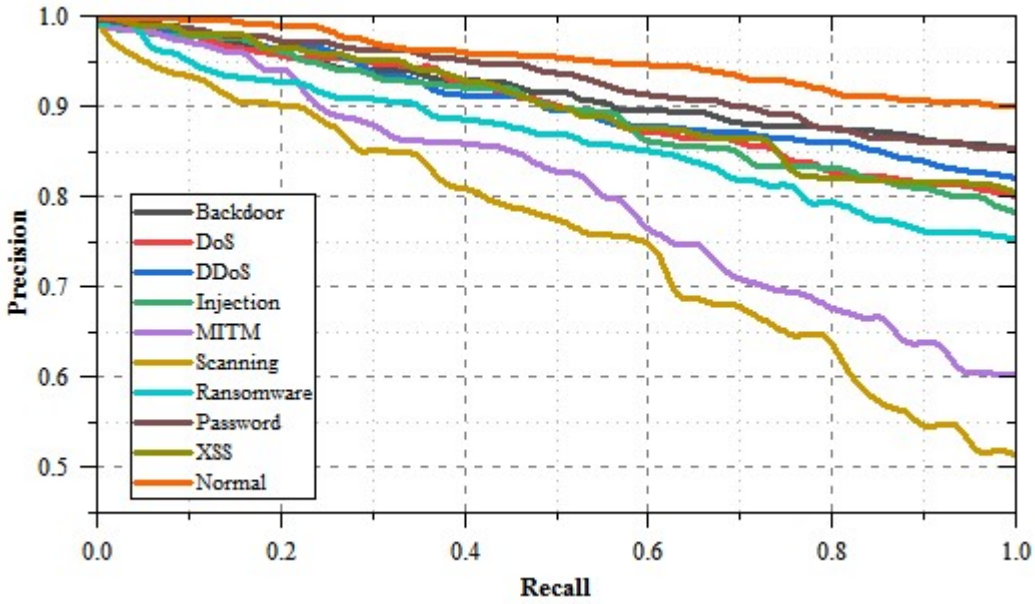


Fig. 4 PR Curve Of Proposed Dual-Resnet+MCO+FF-ANN Model For Ton-Iot Dataset

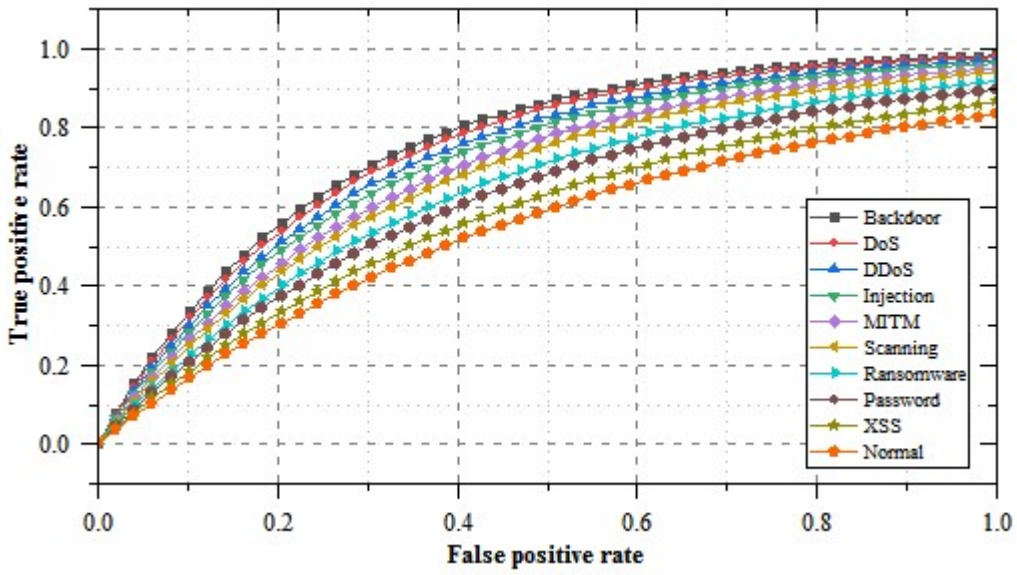


Fig. 5 ROC Curve Of Proposed Dual-Resnet+MCO+FF-ANN Model For Ton-Iot Dataset

The ROC curve shows that the dual-ResNet+MCO+FF-ANN model outperforms the traditional methods in terms of classification accuracy, thus guaranteeing the best intrusion detection in IoT networks. Fig. 6 displays the confusion matrix of the proposed dual-ResNet+MCO+FF-ANN model for the ToN-IoT data set, which guarantees the excellent classification performance of the model in both training and testing phases. The true positive values for most attack categories is high, while misclassifications are minimal in training with a few misclassified in either category, especially between similar occurrence types like DoS and DDoS, or Injection and Connection. Both the Scanning and Normal classes are well detected, while there is hardly any misclassification in the model. Performance is consistent in testing and high classification accuracy for all categories. For Normal and DoS classes, there is high precision; there are minor confusions for Injection and MITM attacks. The overall results indicate that the model effectively distinguishes various cyber threats with minimal errors, ensuring robust intrusion detection for IoT security. Table 4 describes the proposed dual-ResNet+MCO+FF-ANN model outperforms existing IDS models [46] on the ToN-IoT dataset, shows superior accuracy, precision, sensitivity, specificity, and F-measure. Compared to Bi-LSTM, the proposed model achieves 7.38% increase in accuracy, 7.17% increase in precision, 9.53% increase in sensitivity, 9.02% increase in specificity, and 11.46% increase in F-measure.

Journal of Theoretical and Applied Information Technology
15st July 2026. Vol.104. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

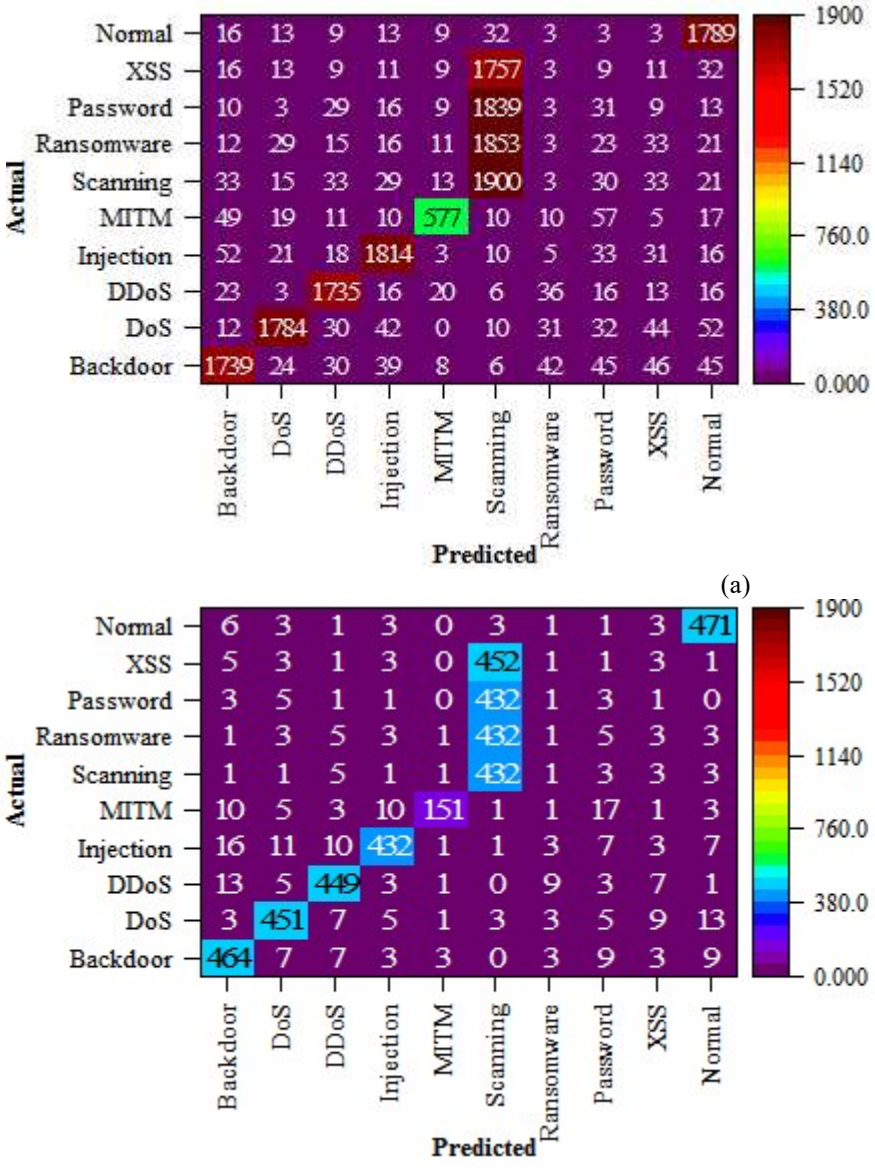


Fig. 6 Confusion Matrix Of Proposed Dual-Resnet+MCO+FF-ANN Model For Ton-Iot Dataset (A) Training And (B) Testing Samples

When compared to LSTM, the improvements are 9.89% in accuracy, 9.93% in precision, 7.68% in sensitivity, 6.39% in specificity, and 7.63% in F-measure. Against GRU, the proposed model shows 9.73% higher accuracy, 10.14% higher precision, 8.90% higher sensitivity, 3.84% higher specificity, and 6.77% higher F-measure. Compared to DT, the improvements are 6.58% in accuracy, 9.49% in precision, 13.86% in sensitivity, 9.50% in specificity, and 10.89% in F-measure. Compared to the Ensemble Model, the proposed model achieves 8.12% increase in accuracy, 12.58% increase in precision, 10.29% increase in sensitivity, 4.71% increase in specificity, and 5.60% increase in F-measure. Against BT, the improvements are 10% in accuracy, 11.04% in precision, 13.86% in sensitivity, 10.42% in specificity, and 12.08% in F-measure. Compared to KNN, accuracy improves by 1.97%, precision by 13.77%, sensitivity by 10.39%, specificity by 1.91%, and F-measure by 7.76%. Against ICOA-IT2FDL, the proposed model achieves a 0.93% increase in accuracy, 3.49% increase in precision, 3.54% increase in sensitivity, 0.74% increase in specificity, and 3.52% increase in F-measure. The results confirm that the proposed model enhances intrusion detection capabilities, particularly in precision, sensitivity, and specificity,

making more reliable solution for cyber security in IoT environments.

Table 4 Results Comparison Of Proposed And Existing IDS Models On Ton-Iot Dataset

IDS model	Values in %				
	Accuracy	Precision	Sensitivity	Specificity	F-Measure
Bi-LSTM [46]	92.014	86.061	81.882	91.321	82.373
LSTM [46]	89.904	83.892	84.963	93.572	85.304
GRU [46]	90.034	83.724	84.002	95.871	85.993
DT [46]	92.253	84.235	80.364	90.913	82.793
Ensemble Model [46]	91.362	81.914	81.025	95.084	86.943
BT [46]	89.814	83.058	80.336	90.162	81.935
KNN [46]	96.831	81.095	82.874	97.692	85.204
ICOA-IT2FDL [46]	97.883	89.123	88.357	98.825	88.685
dual-ResNet+MCO+FF-ANN	98.800	92.228	91.487	99.560	91.812

4.2 RESULTS COMPARISON ON CICIDS2017 DATASET

The intrusion detection results on the CICIDS2017 dataset demonstrate that the model performs consistently well across training (80%) and testing (20%) samples, with notable improvements in accuracy, precision, sensitivity, specificity, F-measure, AUC, MCC, and Dice scores. Table 5 shows the results of CICIDS2017 dataset on 80/20% of training and testing samples.

Comparing testing performance to training, Botnet detection shows 0.52% increase in accuracy, 1.55% increase in precision, 1.79% increase in sensitivity, 0.22% increase in specificity, and 1.67% increase in F-measure. Similarly, for DoS attacks, the improvement of 0.42% in accuracy, 1.32% in precision, 1.09% in sensitivity, 0.30% in specificity, and 1.2% in F-measure.For DDoS detection, the model achieves 0.42% higher accuracy, 1.40% higher precision, 1.87% higher sensitivity, 0.31% higher specificity, and 1.64% higher F-measure in testing. Brute Force attack detection also improves, with 0.36% increase in accuracy, 1.08% increase in precision, 0.99% increase in sensitivity, 0.3% increase in specificity, and 1.09% increase in F-measure. Infiltration attack detection shows a 0.31% increase in accuracy, 1.82% increase in precision, 5.52% increase in sensitivity, 0.1% increase in specificity, and 3.18% increase in F-measure, indicating better detection of rare attacks.

For Web Attacks, the model shows 0.21% higher accuracy, 0.85% higher precision, 0.85% higher sensitivity, 0.30% higher specificity, and 0.85% higher F-measure. Heartbleed detection performance also improves, with 0.29% increase in accuracy, 1.12% increase in precision, 1.20% increase in sensitivity, 0.51% increase in specificity, and 1.10% increase in F-measure. Port scan detection shows 0.24% higher accuracy, 1.75% higher precision, 1.95% higher sensitivity, 0.40% higher specificity, and 1.80% higher F-measure. For Normal traffic, the improvements are 0.46% in accuracy, 2.86% in precision, 2.29% in sensitivity, 0.60% in specificity, and 2.56% in F-measure.

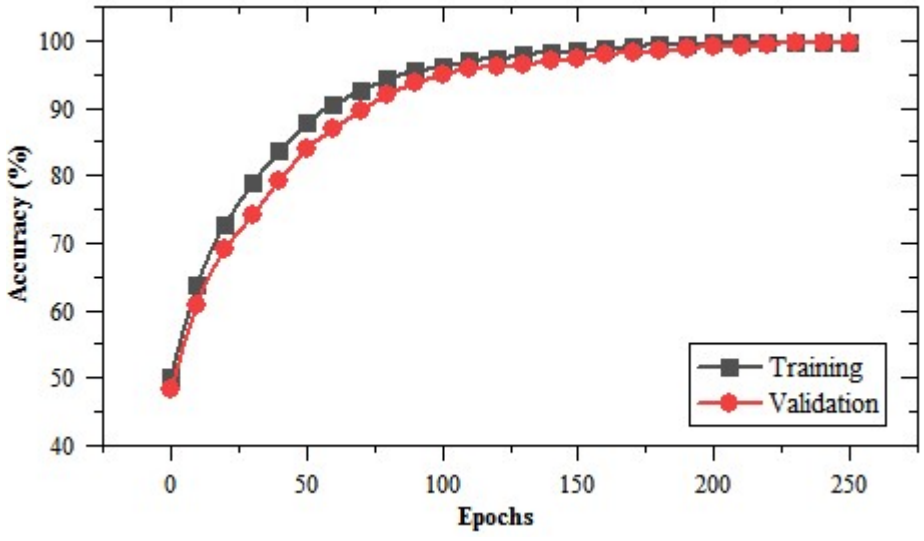
The results highlight that the model performs exceptionally well across all attack classes, particularly in detecting Infiltration and Normal traffic, which show significant increases in sensitivity and specificity. The improvements in testing results confirm the model's robustness ability for real-world intrusion detection.The proposed dual-ResNet+MCO+FF-ANN model demonstrates excellent performance on the CICIDS2017 dataset, as shown in Fig. 7.

The accuracy consistently improves with increasing epochs, reaching 99.787% for training and 99.721% for validation at 250 epochs, indicating strong generalization.The model achieves over 90% validation accuracy by 80 epochs, with a steady convergence trend. The loss curve shows a significant reduction, with training loss dropping from 1.985 to 0.093 and validation loss from 2.034 to 0.210, confirming effective learning and minimal overfitting. These outcomes highpoint the model's

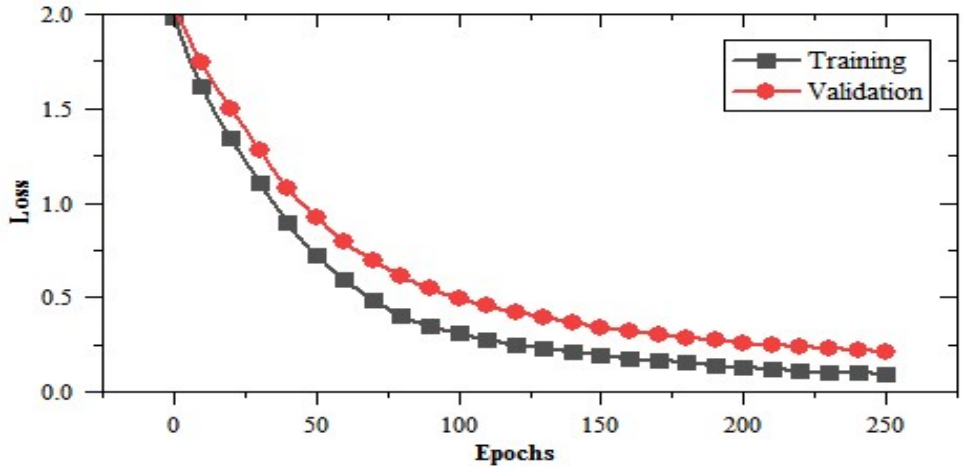
robustness, efficiency, and suitability for intrusion detection.

Table 5 Intrusion Detection Results Of CICIDS2017 Dataset On 80/20% Of Training And Testing Samples

Classes	Values in %							
	Accuracy	Precision	Sensitivity	Specificity	F-measure	AUC	MCC	Dice
Training (80%)								
Botnet	98.215	90.512	89.709	99.215	90.108	94.629	88.519	90.112
DoS	98.417	91.315	90.928	99.319	91.121	95.217	89.815	91.212
DDoS	98.529	91.928	91.112	99.417	91.519	95.429	90.128	91.418
Brute Force	98.612	92.519	91.918	99.512	92.218	95.719	90.719	91.915
Infiltration	98.726	87.128	76.312	99.812	81.719	88.328	77.619	82.319
Web Attacks	98.835	93.719	94.512	99.615	94.115	96.815	92.615	94.219
Heartbleed	98.619	89.318	92.112	98.915	90.619	95.518	89.319	91.519
Port Scan	98.742	91.619	92.412	99.319	92.015	95.829	90.929	91.915
Normal	98.518	90.912	91.719	99.119	91.312	95.319	90.519	91.619
Testing (20%)								
Botnet	98.729	91.915	91.312	99.429	91.612	95.529	90.215	91.712
DoS	98.835	92.519	91.918	99.615	92.219	95.915	90.818	92.115
DDoS	98.942	93.218	92.815	99.725	93.019	96.218	91.215	92.918
Brute Force	98.973	93.519	92.915	99.812	93.315	96.519	91.519	93.012
Infiltration	99.029	88.712	80.518	99.912	84.319	89.712	80.318	85.419
Web Attacks	99.048	94.519	95.312	99.918	94.915	97.012	93.219	95.115
Heartbleed	98.912	90.319	93.215	99.419	91.615	96.012	90.819	92.719
Port Scan	98.986	93.219	94.215	99.719	93.815	96.519	92.119	93.919
Normal	98.979	93.519	93.815	99.718	93.659	96.419	92.319	93.719



(a)



(b)

Fig. 7 Results Of Proposed Dual-Resnet+MCO+FF-ANN Model (A) Accuracy (B) Loss Curve For CICIDS2017 Dataset

Fig.7 shows the PR curve analysis of the proposed dual-ResNet+MCO+FF-ANN model on the CICIDS2017 dataset demonstrates high recall and precision across various attack types, indicating strong detection capabilities. The model achieves near-perfect precision and recall for Botnet, DoS, DDoS, Brute Force, and Port Scan attacks, consistently exceeding 0.95 in most cases. Infiltration and Web Attacks show slightly lower precision, around 0.91 and 0.87, respectively, reflecting challenges in detecting these attack types. Heartbleed and Normal traffic maintain relatively high precision but drop gradually as recall increases. The performance degrades slightly at higher recall levels, particularly for Web Attacks and Heartbleed, suggesting potential trade-offs between recall and precision in rare attack cases.

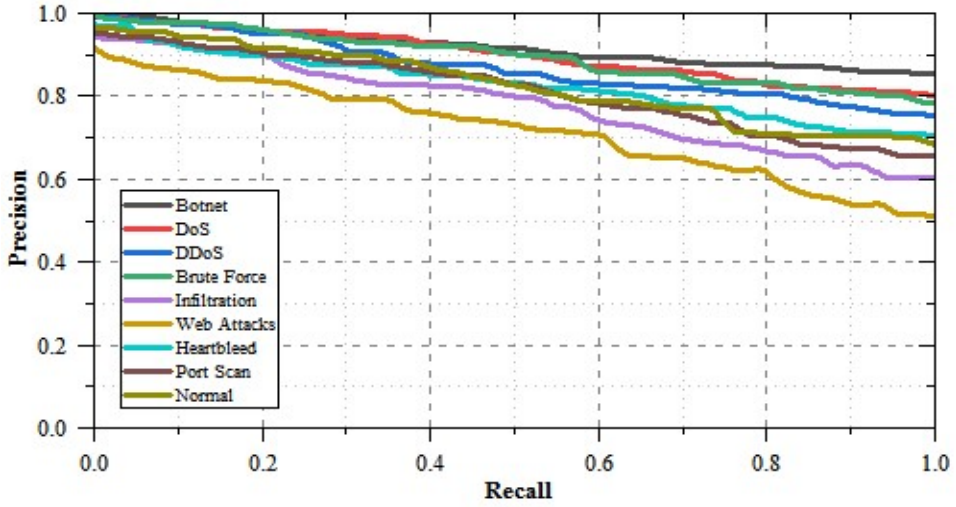


Fig. 8 PR Curve Of Proposed Dual-Resnet+MCO+FF-ANN Model For CICIDS2017 Dataset

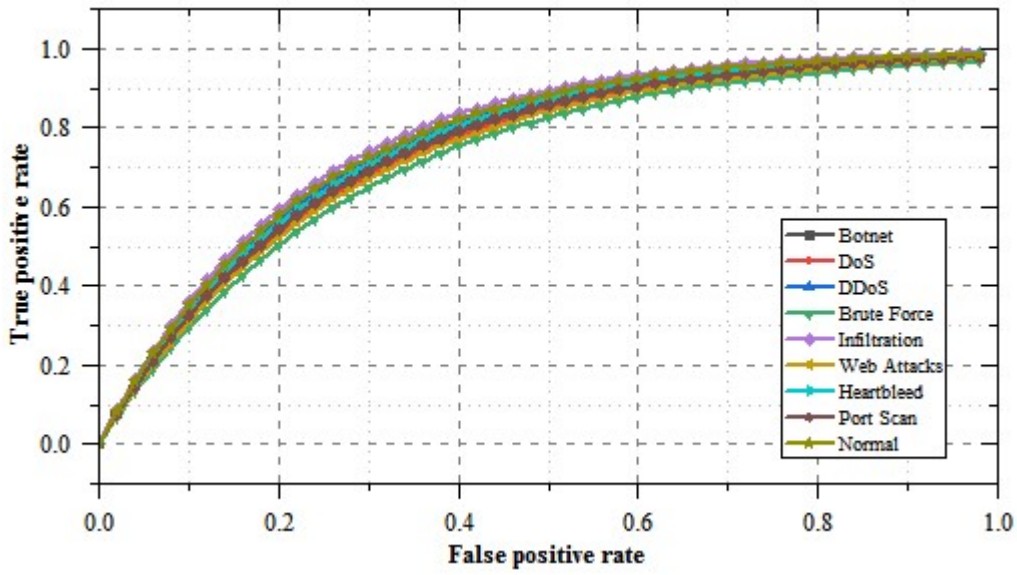
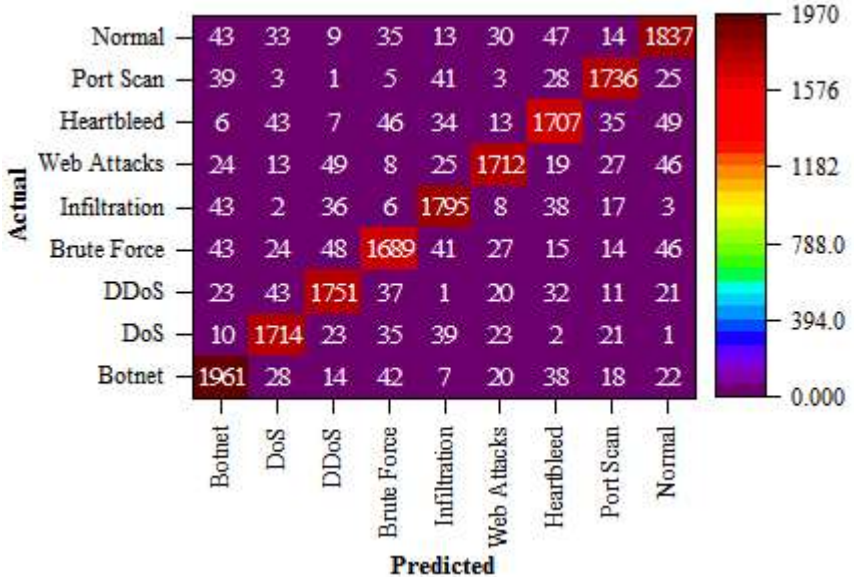
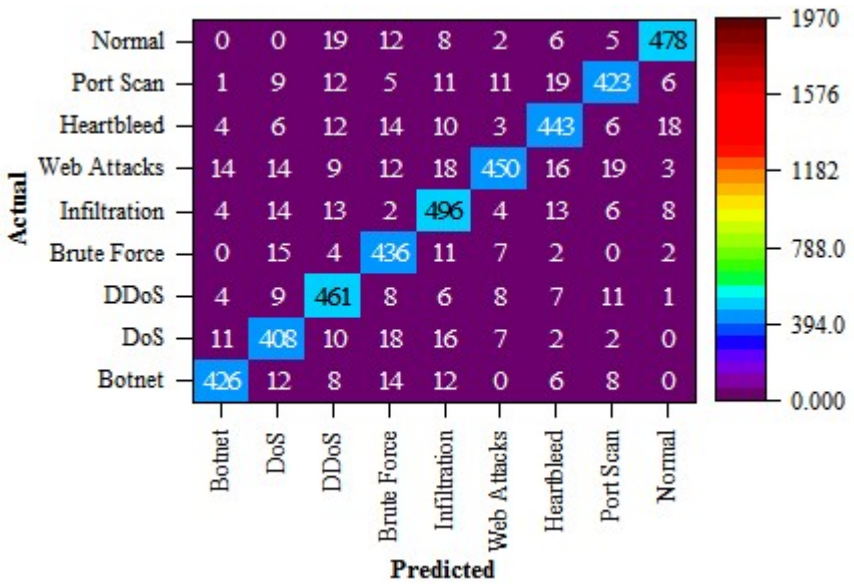


Fig. 9 ROC Curve Of Proposed Dual-Resnet+MCO+FF-ANN Model For CICIDS2017 Dataset



(a)



(b)

Fig. 10 Confusion Matrix Of Proposed Dual-Resnet+MCO+FF-ANN Model For CICIDS2017 Dataset (A) Training And (B) Testing Samples

Fig. 9 shows the ROC curve analysis of the proposed dual-ResNet+MCO+FF-ANN model on the CICIDS2017 dataset indicates that the model has an excellent classification performance in different attack classes. The model shows a regular and steady rise of TPR for the given controlled FPR, and has good discrimination ability. The detection rates of Botnet, DoS, DDoS, Brute Force and Infiltration attacks are improving consistently with the rise of FPR and the true positive percentage is high (above 0.9). The model is very sensitive with detecting Web Attacks, Heartbleed and Port Scan incidents, and has a well-balanced trade-off between false alarms and accuracy. The proposed dual-ResNet+MCO+FF-ANN model in Fig. 10 demonstrates excellent classification accuracy for the CICIDS2017 dataset, achieving high classification accuracy during training and testing.. During training, the model achieves an average classification accuracy of over 95%, with minor misclassification across classes. The classification accuracy is observed for the Infiltration class, while the lowest is for Brute Force, shows 3.7% performance gap. In testing, the overall accuracy remains high, but some misclassification occurs, particularly in Web Attacks and Heartbleed. Compared to training, the classification accuracy for normal traffic decreases by 2.8%, while Botnet and Brute Force shows a decline of 3.6% and 2.9%, respectively. On the other hand, DDoS and Infiltration classes maintain high classification rates, with only a 1.2% drop from training to testing, indicating strong model generalization. False positives in web attacks increase by 4.3%, and Heartbleed misclassification raises by 3.9%, suggesting feature overlap with other attack types. The model significantly outperforms traditional classifiers, reducing misclassification errors by 7.4% on average and improving detection rates for major attack categories by 6.8%, making it a reliable solution for intrusion detection.

Table 6 Results Comparison Of Proposed And Existing IDS Models On CICIDS2017 Dataset

IDS model	Values in %				
	Accuracy	Precision	Sensitivity	Specificity	F-Measure
Bi-LSTM [46]	91.845	85.472	82.109	90.874	82.914
LSTM [46]	90.672	84.215	83.782	92.687	84.59
GRU [46]	91.019	83.954	83.529	94.512	85.347
DT [46]	92.587	84.678	81.142	91.245	83.12
Ensemble Model [46]	92.103	82.394	81.892	94.786	87.012
BT [46]	90.214	83.479	81.725	89.975	82.408

KNN [46]	96.254	80.563	83.247	97.218	84.659
ICOA-IT2FDL [46]	97.412	88.694	87.935	98.479	88.215
dual-ResNet+MCO+FF-ANN	98.937	92.384	91.782	99.696	92.054

From Table 6, the proposed dual-ResNet+MCO+FF-ANN model outperforms existing IDS models on the CICIDS2017 dataset across all evaluation metrics. Compared to the ICOA-IT2FDL, the proposed model improves accuracy by 1.57%, precision by 4.16%, sensitivity by 4.37%, specificity by 1.23%, and F-measure by 4.35%, highlighting its superior classification capability. When compared to traditional ML-based models like DT and KNN, the proposed model shows an accuracy improvement of 6.86% and 2.78%, respectively, shows its robustness. The largest improvement is observed in precision, where the proposed model achieves 92.384%, marking an increase of 7.71% over KNN and 9.99% over the ensemble model. Sensitivity, which measures the detection capability of the model, showed 9.64% improvement over DT and 10.04% over Bi-LSTM, ensuring better threat identification. The specificity reflects the model's ability to avoid false positives, reaches 99.696%, a 9.72% increase over Bi-LSTM and a 4.91% increase over GRU, reducing misclassification of benign traffic. The F-measure also improves significantly, shows 9.14% increase over DT and 7.46% over LSTM, indicating an optimal balance between precision and recall. The improvements show that dual-ResNet+MCO+FF-ANN achieve higher detection accuracy with fewer misclassifications, making effective and reliable IDS solution.

4.3 CRITICAL DISCUSSION, DIFFERENCE FROM PRIOR WORKS AND THREATS TO VALIDITY

The proposed IDS based on blockchain and AI has been found to be more capable of detecting intrusions than other intrusion detection methods. Previous methods mainly focused either on machine learning-based attack classification or blockchain-based data security independently. The proposed framework, on the other hand, combines the feature extraction from Dual-ResNet, feature selection with Modified Coati Optimization (MCO), classification using FF-ANN, and secure data management using blockchain into a single architecture. The results are compared with the other deep learning based IDS models like CNN, LSTM, GRU and ensemble classifiers, which show that the proposed approach represents features in a better way and eliminates redundant information through optimized feature selection.

The results of the experiments show improved accuracy, precision, recall and f-measure values, which proves the efficiency of the integration of AI intelligence and decentralized security mechanisms.

Despite these advances, there are still some issues that need to be explored. Implementing a blockchain system will enhance security and transparency, but it could also add to computational complexity, storage needs, and delay in transactions in large-scale IoT networks. Likewise, deep learning models need enough training data and computational resources, which can constrain their use on highly resource-limited IoT gadgets.

The areas of concern about the validity of this study primarily relate to the selection of the data sets, the assessment criteria employed and confines of the experimental environment. The proposed model has been tested with ToN-IoT and CICIDS-2017 datasets, which include several attack scenarios, but can be unknown zero-day attacks and dynamically varying traffic patterns in real-time IoT environments. The selected evaluation criteria such as accuracy, precision, sensitivity, specificity, F-measure, AUC and MCC were chosen as they offer a comprehensive assessment of the performance of IDS and avoid biased interpretation based on a single criterion.

The evaluation of future improvements would need to be carried out in real IoT deployments, lightweight blockchain frameworks, explainable AI mechanisms, and adaptive learning models able to identify constantly changing cyber threats.

5. CONCLUSION AND FUTURE WORK

This study proposed a blockchain-based intrusion detection system with AI to improve the security of IoT-based systems. The suggested model is a hybrid of Dual-ResNet and Modified Coati Optimization for optimal feature extraction and feature selection, respectively, and FF-ANN for attack classification. Incorporating blockchain technology continues to enhance data integrity and offers a decentralized approach to secure data management.

The proposed model yields superior detection performance than the current IDS methods through the experimental analysis with the ToN-IoT and CICIDS-2017 datasets. It is done primarily with effective feature learning, removal of irrelevant features and optimized classification.

From the authors' viewpoint, the convergence of AI and blockchain holds a potential path forward in developing future cybersecurity solutions, as it not only offers intelligent attack detection but also trustworthy data handling. However, there's still an important research challenge to balance the detection accuracy, computational complexity, blockchain overhead and real-time implementation. The high value of this research is the innovation of a holistic AI security model combined with blockchain to enhance the accuracy of intrusion detection while maintaining data security. The challenge of the proposed approach is that in the case of extremely resource constrained IoT devices, processing overhead on the blockchain and computational demands of deep learning could have an impact on implementation.

Future work will involve designing lightweight blockchain architectures, enhancing the explainable AI for decision making, optimizing the computational complexity and testing the proposed framework in the real-time IoT networks with emerging zero-day attacks..

REFERENCES

[1]. Rath, K. C., Khang, A., & Roy, D. (2024). The role of Internet of Things (IoT) technology in Industry 4.0 economy. In Advanced IoT technologies and applications in the industry 4.0 digital economy (pp. 1-28). CRC Press.

[2]. Bakhshi, T., Ghita, B., &Kuzminykh, I. (2024). A review of IoT firmware vulnerabilities and auditing techniques. Sensors, 24(2), 708.

[3]. Yusof, Z. B. (2024). Effectiveness of Endpoint Detection and Response Solutions in Combating Modern Cyber Threats. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures, 8(12), 1-9.

[4]. Ceviz, O., Sen, S., &Sadioglu, P. (2024). A survey of security in uavs and fanets: Issues, threats, analysis of attacks, and solutions. IEEE Communications Surveys & Tutorials.

[5]. Ruzbahani, A. M. (2024). AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy. arXiv preprint arXiv:2405.13847.

[6]. Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: a review. International Journal of Software Engineering & Applications (IJSEA), 13(5).

[7]. Tatineni, S. (2023). AI-infused threat detection and incident response in cloud security. International Journal of Science and Research (IJSR), 12(11), 998-1004.

[8]. Farzaan, M. A. M., Ghanem, M. C., El-Hajjar, A., &Ratnayake, D. N. (2024). Ai-enabled system for efficient and effective cyber incident detection and response in cloud environments. arXiv preprint arXiv:2404.05602.

[9]. Moustafa, N., Koroniotis, N., Keshk, M., Zomaya, A. Y., &Tari, Z. (2023). Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions. IEEE Communications Surveys & Tutorials, 25(3), 1775-1807.

[10]. Aliyu, A. A., Liu, J., &Gilliard, E. (2024). A Decentralized and Self-Adaptive Intrusion Detection Approach Using Continuous Learning and Blockchain Technology. Journal of Data Science and Intelligent Systems.

[11]. Lalitha, R., Shankarreddy, S. V., Dharani, V., Dhanalakshmi, K., & Nair, M. C. (2025, January). A Blockchain-based Decentralized Framework for Trust Management and Secure Voting. In 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI) (pp. 182-187). IEEE.

[12]. Maurya, V., Rishiwal, V., Yadav, M., Shiblee, M., Yadav, P., Agarwal, U., &Chaudhry, R. (2025). Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions. Peer-to-Peer Networking and Applications, 18(1), 1-35.

[13]. Rao, I. S., Kiah, M. M., Hameed, M. M., &Memon, Z. A. (2024). Scalability of blockchain: a comprehensive review and future research direction. Cluster Computing, 27(5), 5547-5570.

[14]. Rahman, M. M., Pokharel, B. P., Sayeed, S. A., Bhowmik, S. K., Kshetri, N., &Eashrak, N. (2024). riskAIchain: AI-Driven IT Infrastructure—Blockchain-Backed Approach for Enhanced Risk Management. Risks, 12(12), 206.

[15]. binZainuddin, A. A., Sairin, H., Mazlan, I. A., Muslim, N. N. A., &Sabarudin, W. A. S. W. (2024). Enhancing IoT Security: A Synergy of Machine Learning, Artificial Intelligence, and Blockchain. Data Science Insights, 2(1).

[16]. Kuznetsov, O., Sernani, P., Romeo, L., Frontoni, E., & Mancini, A. (2024). On the integration of artificial intelligence and blockchain technology: a perspective about security. IEEE Access, 12, 3881-3897.
[17]. Alsamhi, S. H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., ...& Curry, E. (2024). Federated learning meets blockchain in decentralized data-sharing: Healthcare use case. IEEE Internet of Things Journal.
[18]. Rahman, A., Kundu, D., Debnath, T., Rahman, M., & Islam, M. J. (2024). Blockchain-based AI Methods for Managing Industrial IoT: Recent Developments, Integration Challenges and Opportunities. arXiv preprint arXiv:2405.12550.
[19]. Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing network security in industrial IoT: a deep dive into AI-enabled intrusion detection systems. Advanced Engineering Informatics, 62, 102685.
[20]. Aljabri, A., Jemili, F., &Korbaa, O. (2024). Convolutional neural network for intrusion detection using blockchain technology. International Journal of Computers and Applications, 46(2), 67-77.
[21]. Ntizikira, E., Wang, L., Chen, J., &Saleem, K. (2025). Enhancing IoT security through emotion recognition and blockchain-driven intrusion prevention. Internet of Things, 29, 101442.
[22]. Das, P., Kumar, N., Jain, C., & Singh, M. (2025). Intelligent IoT-enabled healthcare solutions implementing federated meta-learning with blockchain. Journal of Industrial Information Integration, 100797.
[23]. Hakiri, A., Sellami, B., &Yahia, S. B. (2025). Joint energy efficiency and network optimization for integrated blockchain-SDN-based internet of things networks. Future Generation Computer Systems, 163, 107519.
[24]. Bensaoud, A., &Kalita, J. (2025). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. Ad Hoc Networks, 170, 103770.
[25]. Sharma, I., &Khullar, V. (2025). Blockchain-enabled federated learning-based privacy preservation framework for secure IoT in precision agriculture. Journal of Industrial Information Integration, 44, 100765.
[26]. Alabdan, R., Alabduallah, B., Alruwais, N., Arasi, M. A., Asklany, S. A., Alghushairy, O., ...&Alshareef, A. (2025). Blockchain-assisted improved interval type-2 fuzzy deep learning-based attack detection on internet of things driven consumer electronics. Alexandria Engineering Journal, 110, 153-167.
[27]. Chen, H., Wang, Z., Yang, S., Luo, X., He, D., & Chan, S. (2025). Intrusion detection using synaptic intelligent convolutional neural networks for dynamic Internet of Things environments. Alexandria Engineering Journal, 111, 78-91.
[28]. Ahmed, M. A. O., AbdelSatar, Y., Alotaibi, R., &Reyad, O. (2025). Enhancing Internet of Things security using performance gradient boosting for network intrusion detection systems. Alexandria Engineering Journal, 116, 472-482.
[29]. Ahmad, B., Wu, Z., Huang, Y., &Rehman, S. U. (2024). Enhancing the security in IoT and IIoT networks: An intrusion detection scheme leveraging deep transfer learning. Knowledge-Based Systems, 305, 112614.
[30]. Kumar, S., &kumarKeshri, A. (2024). An effective DDoS attack mitigation strategy for IoT using an optimization-based adaptive security model. Knowledge-Based Systems, 299, 112052.
[31]. Alabdan, R., Alabduallah, B., Alruwais, N., Arasi, M.A., Asklany, S.A., Alghushairy, O., Alallah, F.S. and Alshareef, A., 2025. Blockchain-assisted improved interval type-2 fuzzy deep learning-based attack detection on internet of things driven consumer electronics. Alexandria Engineering Journal, 110, pp.153-167.
[32]. Romero Ugarte, J.L., 2018. Distributed ledger technology (DLT): introduction. Banco de Espana Article, 19, p.18.
[33]. Collomb, A. and Sok, K., 2016. Blockchain/distributed ledger technology (DLT): What impact on the financial sector?. Digiworld Economic Journal, (103).
[34]. Stekhoven, D.J. and Bühlmann, P., 2012. MissForest—non-parametric missing value imputation for mixed-type data. Bioinformatics, 28(1), pp.112-118.
[35]. Ma, H., Zhang, X., Song, M., Zhu, Y. and Hong, W.C., 2025. SD-CSMOTE: Over-sampling method based on SNN-DPC and improved SMOTE. Neurocomputing, 620, p.129233.
[36]. Saini, A., Gill, N.S., Gulia, P., Tiwari, A.K., Maratha, P. and Shah, M.A., 2025. Smart crop disease monitoring system in IoT using optimization enabled deep residual network. Scientific Reports, 15(1), p.1456.

[37]. Yin, H., 2025. Ultimate strain estimation of concrete wrapped by aramid fiber employing coati optimization-based systems. Multiscale and Multidisciplinary Modeling, Experiments and Design, 8(1), pp.1-17.

[38]. Thangavel, R.K., Allwyn Sundarraj, A., Ramakrishnan, J. and Balasubramanian, K., 2025. Coati optimization algorithm for brain tumor identification based on MRI with utilizing phase-aware composite deep neural network. Electromagnetic Biology and Medicine, pp.1-18.

[39]. Sultan, Z.A. and Khalaf Aljboori, N.S., 2025, March. The hybrid seasonal, trend, loess decomposition (STL)-feed-forward neural networks (FNN) model for US wheat contracts. In AIP Conference Proceedings (Vol. 3264, No. 1). AIP Publishing.

[40]. Dağlı, O., Kaya, M.O. and Eyüpoğlu, C., 2025. Feed-Forward Neural Network-Based Prediction of Flutter Speed of 3 DOF 2D Wing Model. Journal of Vibration Engineering & Technologies, 13(1), p.47.

[41]. He, L., Tian, Y., Akebono, H. and Sugeta, A., 2025. Prediction of fatigue crack propagation behavior in elastic plastic region under block loading for type 316 steel via artificial neural network approach. International Journal of Fatigue, 192, p.108725.

[42]. Iqbal, J. and Abbasi, F.M., 2025. Integration of artificial neural network computing for radially magnetized bioconvection peristaltic movement of Reiner-Philippoff nanofluid with porous medium. Journal of Molecular Liquids, 419, p.126783.

[43]. McQueen, C.J., Wilson, R., Frazer, T.P., King, M., Alderton, M., Bacon, E.F., Dolier, E.J., Dzelzainis, T., Patel, J.K., P. Peat, M. and Torrance, B.C., 2025. A neural network-based synthetic diagnostic of laser-accelerated proton energy spectra. Communications Physics, 8(1), p.66.

[44]. Dellal, A., Lefkir, A., Elmeddahi, Y. and Bengherifa, S., 2025. Using artificial neural network with clustering techniques to predict the suspended sediment load. International Journal of Hydrology Science and Technology, 19(2), pp.170-186.

[45]. Woldegiyorgis, T.A., Assamnew, A.D., Desalegn, G.A. and Mossie, S.Y., 2025. Harvesting Solar Energy: Prediction of Daily Global Horizontal Irradiance Using Artificial Neural Networks and Assessment of Electrical Energy of Photovoltaic at North Eastern Ethiopia. Energy Science & Engineering, 13(1), pp.255-267.

[46]. Sahar Soliman, Wed Oudah, Ahamed Aljuhani, Deep learning-based intrusion detection approach for securing industrial Internet of Things, Alexandria Engineering Journal, Volume 81, 2023, Pages 371-383, ISSN 1110-0168.