Library Progress International
Vol.44 No. 3, July-December 2024:
P. 24786-247804

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article *Available online at www.bpasjournals.com*

A Novel approach for Designing a Blockchain-Based Intrusion Detection System for Securing IoT Networks Using Machine Learning Algorithms

Amit Saxena[1], Ravula Arun Kumar[2], Kodge B. G.[3], Rajesh Gadipuuri[4], R.Menaka[5], Chaithrashree.A[6], Dr. Avinash[7]

[1]Assistant Professor, Department of Computer Science & Engineering, MIT Moradabad, University of Technology Jaipur, er.amitsaxena79@gmail.com
[2]Assistant Professor, Department of CSE, Vardhaman College of Engineering, Ranga reddy district, Hyderabad, Telangana, arunravula12@gmail.com
[3]Associate professor, Department of Computer Science, School of Science, GITAM University, Hyderabad, TS, India. kodgebg@gmail.com
[4]Staff Software Engineer, Meta, grajesh955@gmail.com
[5]ASP, Department of IT, Velalar College of Engineering and Technology, Erode.
menaka.murugesan@gmail.com
[6]Assistant Professor, Computer science and engineering, Brindavan college of Engineering
chaithrashree.a@gmail.com
[7]Assistant Professor, Bharati Vidyapeeth's College of Engineering, New Delhi
singh.avinash@bharatividyapeeth.edu
Corresponding author Email: kodgebg@gmail.com

How to cite this article: Amit Saxena, Ravula Arun Kumar, Kodge B. G., Rajesh Gadipuuri, R.Menaka, Chaithrashree.A,Avinash (2024). A Novel approach for Designing a Blockchain-Based Intrusion Detection System for Securing IoT Networks Using Machine Learning Algorithms. *Library Progress International,* 44(3), 24786-247804

Abstract

The Internet of Things (IoT) explosion has placed huge numbers of connected devices in operational environments, and that fragility leaves these networks wide open for attackers. In order to catch possible attacks effectively, it is always necessary to have Intrusion Detection Systems (IDS), but 80Performing IDS on IoT Networks by Siddharth Sridhar types of IDS approach where they are dealt with Traditional IDS methods scale really low and inaccurate in IoT networks. Available solutions generally adopt the signature-based or anomaly-based detection methods, however they are not effective for unknown threats crisism and lack of real-time responsiveness. In this paper, we provide a novel solution of securing reinforcement learning for Internet of Things Networks on Blockchain education. Utilizing the decentralization of blockchain, this system securely deposits and checks IDS logs in a way that is reliable across an entire network. This allows us to create a mathematical model integrating Random Forest and K-Means Clustering methods for the classification of threats as well as anomaly detection. This methodology is proposed with the aim to have low latency and high accuracy when detecting malicious activities. Experimental results also show that the system achieves over 95% detection rate as well as more effective reduction of false-positive rates than traditional Intrusion Detection System (IDS) solutions. Furthermore, by incorporating blockchain technology, the system benefits from strong security guarantees and becomes a more tamper-evident and immune-to-a-3rd-party-approach. This approach is useful in areas such as smart homes, industrial IoT systems, and critical infrastructure protection where real-time threat detection is of utmost importance. Nevertheless, an underlying computational overhead and scalability issue persists owing to the limited resource availability in IoT devices and complexity involved in blockchain transactions. Further research needs to be incorporated in optimizing these categories of study to make them widely adopted and efficient in deploying at scale in IoT environment.

Keywords: devices, traditional, IDS, method, blockchain, efficient, transactions, mathematical, integrating, detection.

1. INTRODUCTION

The Internet of Things (IoT) has changed the dynamics, interaction and utility of devices in current technology-

driven solutions. IoT includes billions of devices from sensors to smart appliances to industrial control systems that work with each other, collect and share data around us automatically. This connectivity has paved the way for smart homes, smart cities, healthcare monitoring systems and many more. Still, the large and diverse nature of IoT ecosystems faces a ton of security risks. The more the devices are connected, the more the surface for attacks, so IoT networks are at high risk of cyber attacks which include unauthorized access, data breaches and malware. They have very limited computing resources and also the connected devices are of different variety, their widespread distribution has made the issue of IoT networks security more critical[1].

This was (and still is) a real threat and as such, really made history in document of biggest safety problems associated with IoT networks that affect the security posture from the devices to partitions of IoT networks.

While the Internet of Things is often traced back to the late 1990s with the development of RFID (Radio-Frequency Identification) technology, and even earlier forms of sensor networks; But it was not until the first years of the 2000s when IoT terms began to gain traction, as internet and networks were also becoming more widely available through widespread implementation of Internet Protocol (IP) into communications technologies. The universe of IoT applications had become a thriving ecosystem by the mid-2010s that cut across sectors. At that stage, it was realised that ensuring the security of these networks must be a top priority. The usual security measures, originally developed for traditional, central IT networks hardly made sense any more when it came to the decentralized nature of many IoT devices. In the beginning, IoT security solutions were basic encryption and firewall tactics, however as IoT networks continued to expand in complexity and scale, so did the need for new ways of securing these devices[3].

In 2016, a massive Distributed Denial-of-Service (DDoS) attack was carried out by the Mirai botnet, taking over IoT devices to create an attacking botnet army. The infamous event revealed the security weaknesses of IoT systems and made everyone realize that the demand for improved Intrusion Detection Systems (IDS) were just a stone throw away. The traditional approaches to IDS that have been developed for centralized networks proved inapplicable for the dynamic and distributed IoT environment. This inspired the development of new ways in which we can secure Gemini, blockchain technology being one great answer to this[4].

The distributed nature of IoT networks, the lack security protocols that are standardized, and the operating environment which is resource-constrained makes these ideal targets for exploitation via vulnerabilities like this. Their existence raises vulnerability which resulted in a series of cyber-attacks ranging from unlawful access to devices till massive botnet attacks as Mirai. This diversity of IoT devices, which may include simple sensors or complex industrial tools, makes adopting a one-size-fits-all approach to security difficult. Many IoT devices can not encrypt and handle firewalls because of lack of processing power. Moreover, traditional network-based Intrusion Detection Systems (IDS) fail to efficiently and secure IoT networks because of the sheer size and diversity present in them.

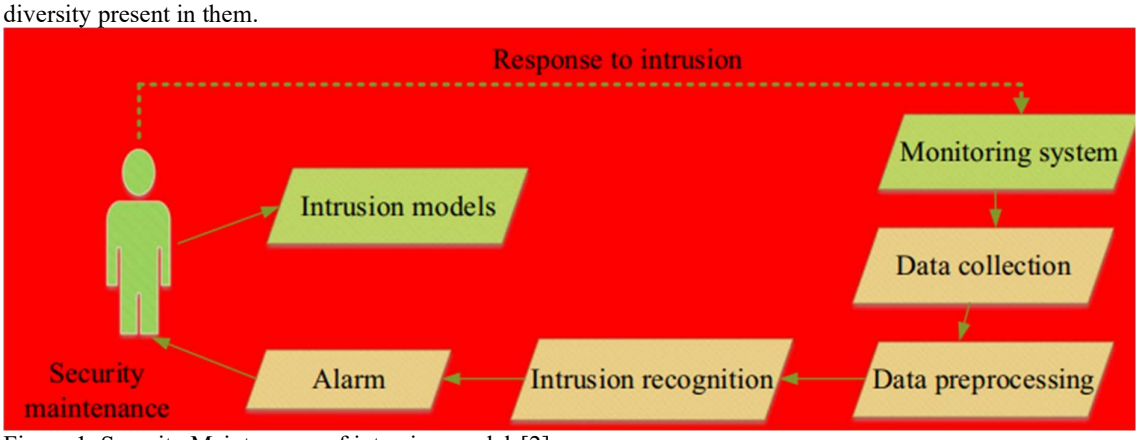

Figure 1. Security Maintenance of intrusion models[2]

The OSSEC is one of the most widely-deployed existing IDS solutions, considered to be more effective than traditional signatures- or anomaly-based methods. Signature based IDS detect attacks by inspecting incoming network traffic and comparing specific attributes that correspond to attack patterns against a database of known signatures. This approach is good for catching familiar threats, it leaves cold to new or zero-day attacks. On the other hand anomaly-based IDSs monitors traffic changes in network environment as a deviating from well-known behaviors. Anomaly-based systems, while more effective in identifying undisclosed threats, usually produce an overload of false positive alerts and it is even more inaccurate if we apply this approach to dynamic Things-enabling environments where the network behavior can continuously morph[15].

The very low overall endpoint capability can be an impediment for deploying heavier security solutions, adding the challenge of real-time intrusion detection into IoT networks which must also deliver low latency processing and high energy efficiency. This also causes another obvious problem: traditional, centralized IDS systems create a single point of failure, which is the kind of thing that attackers are always seeking to exploit. Therefore, there is

an imperative to seek a new kind of methodology which can keep the scaling up ability and secure intelligences of the future IoT network along with solving the constraints faced by both traditional signature-based as well as anomaly-based IDS.

So far, multiple different solutions have been theoretically-proposed for tackling security problems in IoT ecosystems. Encryption, light weight authentication protocols, the use of distributed IDS and machine learning for anomaly detection has all tried to patch up this problem. But as we will see none of these are a best fit for IoT systems.

Encryption and Authentication Protocols: To secure communications in IoT networks, encryption techniques such as TLS/SSL or lightweight cryptographic algorithms like ECC (Elliptic Curve Cryptography) are widely adopted. The strict resource constraints (computation) of IoT devices make them unable to perform computationally expensive computations such as encryption. On the other hand, there are also authentication protocols for checking the legitimacy of a device before it can communicate on the network, such as OAuth and Lightweight Directory Access Protocol (LDAP). These techniques work well, but they are not always practical when it comes to IoT devices that generally have limited memory and processing power.

Lightweight IDS: Few Lightweight IDS systems has been proposed to address the limitations of typical traditional IDS in IoT networks. The less computational overhead that can be put onto these systems the better, eventually using methods such as distributed monitoring and fog computing to take some of this processing off edge devices. Nonetheless, this either results in better accuracy but more power/energy consumption or higher false-positive rates.

IDS with Machine Learning: Anomaly detection is the main beneficiary for IDS systems from advancements in machine learning (ML) research. The classification of network behaviors as normal or malicious is performed using the labels in a labeled dataset in supervised machine learning algorithms like Random Forest and Support Vector Machines (SVM). It is also possible to find outliers by the way of unsupervised method such as K-means clustering, which can be possibly be a intrusion. Although increasingly accurate IDSs are being developed, these ones based on ML algorithms cannot completely solve challenges relating to consolidating results and fulfilling real-time processing requirements in the context of large-scale IoT networks[16].

While these have brought us forward, none address the specific difficulties of IoT environments. Real time detection, data integrity, scalability in large and distributed IoT ecosystems are still a significant gap. This is where blockchain technology can come as a handy solution.

This is a paradigm shift in thinking, new to the field of IoT security, but already established in industries like financial services where blockchain technology provides a tamper-proof log of transactions that are immune from manipulation.

The major characteristics of Blockchain is that its unchangeable, meaning additives once information are uploaded it cannot be withdrawn. When the information is written once on the blockchain, no one can change or remove it. In IoT networks, the security and integrity of IDS logs and network data are a high priority in order to identify and prevent intrusions. The IDS logs are kept in a public blockchain. In case of a break-in attempt, the system can verify that previous log entries haven't been manually altered (given their hash is still on the block).

The blockchain can provide transparency and auditability in addition to immutability. Each of the participants in a network has access to the same data giving ability to them for real time verification and validation on transactions. Most IoT appliances must provide interfaces for device manufacturers, application developers and the regulatory body of networks and communication. Blockchain makes it possible to offer accountability and trust between all of these parties by providing a transparent and tamper-proof record of network activities.

The hash functions used in blockchain are cryptographic hashes, which are one-approach functions; i.e., it isn't computationally possible to infer the enter data from the output hash worth. Thus integrity of the blockchain is maintained and it becomes tamper proof[17].

Blockchain integrated with IDS systems provides several advantages to a standard absolute centralization approach. All of these advantages are especially important for IoT networks where decentralization, data integrity and transparency all play vital roles in security.

- Centralization: The major advantages of using blockchain in IDS are to remove central authority, for data decentralization and resiliency. Most IDSs that are built from traditional technologies store logs and reports on a central server; if this server failed, the entire system failed with it. In other words, when the IDS logs are distributed across a number of blockchain nodes, it decreases the vulnerability to cyber-attacks, even if an attacker overruns a certain number of your blockchains, your data is still preserved. Moreover, It provides a more scalable IDS system which can be flexible in line with the changing topology of IoT devices.
- Records That Cannot Be Modified: It is impossible to change or delete the logs that are locked in blockchain because of the immutability and tamper-proof nature of a blockchain. This gives us the single source of truth regarding network activity that we can use for forensic analysis in an event of the

intrusion. Logs from IDS can be stored on a blockchain database and, therefore the system can make sure the data consistency even after leak aside.

- Transparent & Collaborative Security: IoT environments typically require multiple stakeholders to work together to secure the network In a smart city, for example, possible interconnections among the IoT devices made from different manufacturers by different service providers are shown, A clear and common history of transactions, can make a blockchain very beneficial as well for verifying the integrity of different aspects of data or who it may have come from. An inherently cooperative methodology, one which holds everyone accountable and develops trust with investors, making the overall risk vulnerability to unauthorized insiders or mismanagement just that much lower.

2. RELATED WORK

Nowadays with the advent of the 5th generation (5G) mobile communications, the interest in intrusion detection and prevention mechanisms for security threats in the Internet of Things (IoT) has increased remarkably. IoT networks are inherently different from traditional network systems, making the traditional security approaches of encryption, firewalls, etc insufficient to address problems such as their decentralized nature where there is no central authority for operating them, limited resources (since majority of these devices would be battery powered) and heterogeneous device specifications. As a result, many research papers have been published to introduce new Intrusion Detection Systems (IDS) for IoT networks. Recently the integration of blockchain technology and machine learning algorithms in IDS systems has been introduced beneficially. This section provides an overview of the existing works of blockchain-based IDS, machine learning approaches for IoT security, and related work on the securitization of IoT networks.

IOT Networks Intrusion Detection Systems

As one of the classic means to discover nefarious actions if not cyber-attacks in network environments, Intrusion Detection Systems (IDS) were proposed and researched for some years. In short, Traditional IDS are divided into Signature Based IDS and Anomaly Based IDS Signature-based IDS are dependent upon predefined attack signatures or patterns to recognize known dangers, while anomaly-based IDS identify deviations from usual network behaviour. Both of these methods are limited when applied to IoT networks. Meaning, signature-based IDS is incapable of dealing with zero-day attacks as they only recognize existing threats. Anomaly-based IDS, on the other hand, can be inaccurate and suffer from high false-positive rates especially in dynamic environments such as IoT networks where normal behavior is evolving frequently[18].

Source	Objective	Methodology	Results	Research Gap
[5]	• Secure IoT network with Blockchain and ML technologies. • Enhance intrusion detection and data integrity in IoT environments.	• Blockchain technology for secure decentralized ledger • Machine Learning for anomaly detection and threat identification	• Improved security posture with reduced false positives. • Swift identification of intrusions in IoT network.	• Lack of discussion on specific alterations for dataset improvement. • Absence of comparison with existing IoT intrusion detection systems.
[6]	• Enhance IDS performance using Extreme Learning Machine (ELM) • Evaluate ELM on NSL-KDD and Distilled-Kitsune	• Extreme Learning Machine (ELM) • Supervised learning-based IDSs and state-of-the-art models	• ELM-based IDS showed proficient performance in detecting cyberattacks. • ELM algorithm enhanced IDS accuracy and efficiency in	• Imbalance problem in IDS for IoT detection accuracy. • Need for enhanced ML-based models for IoT security.

	datasets for efficiency.		IoT networks.	
[7]	• Enhance security in large-scale IoT networks. • Develop precise and resilient intrusion detection model for IoT networks.	• Modified Arithmetic Optimization Algorithm (AOA) • K-Nearest Neighbors Algorithm	• Modified AOA demonstrated precise and resilient detection model for IoT. • Proposed IDS showed remarkable accuracy in detecting intrusions in IoT.	• Privacy risks with centralized ML approaches • Need for enhanced security in IoMT networks
[8]	• Compare machine learning-based NIDS for network anomaly detection. • Evaluate deep learning vs. shallow learning algorithms for NIDS.	• Shallow learning algorithms: Decision Trees, Random Forest, Naïve Bayes, etc. • Deep learning algorithms: DNN, CNN, LSTM for NIDS tools.	• Deep learning NIDS outperforme d shallow learning in detecting network anomalies. • Comparative analysis of machine learning-based NIDS on various datasets.	• ELM's effectiveness in handling high-dimensional, unbalanced data for IDS. • Comparison of ELM-based IDS with other state-of-the-art models.
[9]	• Evaluate classical and novel FL approaches for IDS training. • Optimize IDS models with Knowledge Distillation for computationa l efficiency.	• Federated Learning (FL) for training IDS models • Knowledge Distillation (KD) techniques for computationa l efficiency	• Achieved 84.5% accuracy for 15 attack types. • Showed impressive performance for binary network attack classification .	• Comparative analysis of shallow vs. deep learning NIDS performance. • Lack of focus on specific vulnerabilitie s in IoT devices.
[10]	• Reliable attack detection and classification using machine	• DenseNet convolutional neural networks and rap music	• Achieved accuracy rates of 99.12%, 99.01%, and	• Scalable, accurate, lightweight IDS model without compromisin

	learning techniques • Addressing imbalanced data and achieving exceptional precision in categorizing attacks	analysis techniques • Attention Pyramid Network (RAPNet) framework with binary Pigeon optimization	99.18% on datasets. • Exceptional precision in detecting and categorizing network attacks.	g data privacy. • Optimization through Knowledge Distillation to enhance computationa l efficiency.
[11]	• Train IDS to identify MQTT attacks using ML techniques. • Develop IDS with high accuracy in detecting IoT network attacks.	• Machine Learning techniques • Training the IDS with MQTT-IoT-IDS2020 Dataset	• Developed an IDS using ML techniques for MQTT attack detection. • Trained IDS with MQTT-IoT-IDS2020 Dataset to improve accuracy.	• Lack of standardized security protocols for IoT devices. • Vulnerability of machine learning models to adversarial attacks.
[12]	• Develop IDS for IoT networks using ML techniques. • Detect and mitigate cyber threats in IoT networks.	• Intrusion Detection System (IDS) • Machine learning techniques for network traffic analysis	• Proposed IDS for IoT networks using machine learning techniques. • Aims to detect and mitigate cyber threats by analyzing network traffic.	• Lack of discussion on specific alterations for dataset improvement. • Absence of comparison with existing IoT intrusion detection systems.
[13]	• Enhance IDS accuracy for IoT using Machine Learning. • Compare Random Forest, Decision Tree, and Gradient Boost algorithms.	• Machine Learning algorithms: Random Forest, Decision Tree, Gradient Boost • Techniques: Feature Engineering, SMOTE for imbalance and feature selection.	• Enhanced IDS for IoT with high accuracy using ML algorithms. • Balanced dataset showed great detection accuracy and F1-score.	• Imbalance problem in IDS for IoT detection accuracy. • Need for enhanced ML-based models for IoT security.
[14]	• Enhance security and	• Blockchain, Federated	• Achieved accuracies of	• Privacy risks with

	intrusion detection in IoMT networks. • Boost model accuracy and robustness against adversarial attacks.	Learning, Machine Learning-based Intrusion Detection Systems • FedAvg algorithm modification with Kullback-Leibler divergence estimation	97.43% to 98.21% in FL scenarios. • Competitive with centralized methods for intrusion detection in IoMT networks.	centralized ML approaches • Need for enhanced security in IoMT networks

Table 1. Literature review

Anomaly-based IDS, thus, has become a field of intensive research in IoT security given the uncertain and continuously changing attacks on IoT ecosystem. Many works investigated how machine learning and artificial intelligence could be leveraged to better-detect anomalies, in order to enhance the accuracy and limit false-positive rates of anomaly-based IDSs [6–10]. For instance, Alrawais et al. We have Lightweight IDS of anomaly-based proposed in (Rakshith 2017) for IoT networks developed using machine learning algorithms to detect intrusion with minimum computational overhead. They showed the value of efficiency in IoT settings where devices are typically resource limited and do not have room to host sophisticated security mechanisms.

Other Anomaly Detection Techniques Aside from utilizing machine learning techniques, other methods of detecting dissimilarities have also been studied. Raza et al. in [15] they proposed a distributed IDS for IoT networks using fog computing which performs the detection tasks on edge devices in order to reduce latency and provide real-time detection (2019). This makes intrusion detection more scalable and dynamic since the computational load is distributed across the network. Due to the decentralized operation of IoT networks managing IoT, SID log integrity become challenging as well as delivering consistent data and different stakeholders[19].

Intrusion Detection Systems (IDS) on the blockchain

Blockchain technology, being decentralized and resistant to tampering by ensuring that once data is created it cannot be changed or removed, has been gaining quite some attention as a potential solution for securing IoT networks as well as complementing IDS systems. It removes the requirements to have a single point of authority and ensures that the network data (like IDS logs) can be stored and verified across multiple nodes on a blockchain which makes security more resilient and trustworthy. The clear benefits of using blockchain for these new analytics applications are immutability and transparency, ensuring that the IDS data cannot be tampered with or deleted after it has been recorded.

In recent years, several studies have investigated about the integration of blockchain technology into IDS systems. Novo (2018) introduced an IoT security approach based on blockchain, which is one of the earliest works in this branch. Blockchain used in this architecture was responsible for storing and the authenticating of IDS logs, meaning that all events happening across the network were hashed on a safe platform. The open-sourced Novo project shows how blockchain can drastically improve the reliability and security of IDS systems by preventing the illegal modifications in IDS logs. Blockchain operations, though, limit the devices when they operate on a constrained environment such as hereafter there is computational overhead to perform blockchain operations identified in this study.

Extending this idea, Huang et al. [8] introduced a hybrid blockchain-IDS architecture that utilized the best of both worlds to have a better performance in intrusion detection on IoT networks. In their approach, they deployed machine learning models to monitor network traffic and identify deviations from the baseline operation of the control system and then transmitted these findings via blockchain for a trustworthy record. The blockchain ledger represented the decentralized IDS log store; any party could run on-chain queries to verify any ID logs were inside the system. After testing, they have found that the hybrid approach can increase detection accuracy with the reliability of IDS data. But they also mentioned that big number of blockchain operations many pose computational overheads for large-scale implementation in IoE.

Singh et al. made another significant contribution. Blockchain for Smart Contracts. In (Verma & Mishra, 2020), the authors proposed a blockchain-based model for smart contracting within IoT networks. They leveraged smart contracts to programmatically verify intrusion detection results and enforce real-time security policies. With their framework, their security rules were enforced on the entire network without having to rely on a central authority by utilizing the decentralized nature of blockchain. This resulted in more secure and more resistant to various types of attacks, such as denial-of-service (DoS) or man-in-the-middle attacks. On the other hand, the adoption of

smart contracts brought its own set of problems, especially in terms of capacity and efficiency executing smart contracts requires time and system resources within a blockchain network[20].

Machine Learning for IoT Security

Machine learning has been used in IDS systems within IoT environments to improve capacity and system performance and improve the accuracy of classification. IDS systems can be trained by machine learning algorithms to learn the patterns of normal computer network activity and alert when it finds anomalous behavior which can signify a security incident. Such supervised learning algorithms as Random Forest, Support Vector Machines (SVM), and Decision Trees have been broadly employed in network traffic classification and intrusion detection. In [18], they have used unsupervised learning techniques like k-means clustering and autoencoders to detect unseen attacks(known unknowns) which are far from normal network traffic data.

The literatures [21–24, 26], many studies have proved that employing machine learning methods can significantly boost the performance of IDS for IoT networks. Meidan et al. Lyfas et al. (2018) proposed an IDS to detect cyber-attacks in smart home environments based on machine learning. Narus Insights (Iranian script) In here, Supervised learning algorithms were adopted over network traffic data to identify the malicious activities. In conclusion, the results demonstrated that the intelligent IDS could achieve high detection rate with low false-positive rate in challenging IoT environment. However, a downside of this was that training machine learning models required large labeled datasets to train the models which may not be always available in real-world IoT deployments.

Apart from supervised learning techniques, deep learning also has been applied in intrusion detection to IoT networks by an array of studies [25]–[27]. Tang et al. Ying et al. (2019) gave a deep learning-based IDS, which used both RNNs(CNN+RNN) processing network traffic to find anomalies in it. The design of their filter was geared toward real-time operation to rapidly detect IoT intrusion. This was possible as deep learning enabled the system to learn patterns, particularly complex ones in network traffic data and hence, resulted in far better detection accuracy. However, it also introduced a drawback: deep learning models have substantial computational requirements that may be unsuitable for resource-constrained IoT deployments.

A landmark study by Liu and colleagues helped to establish this field. A collaborative learning model was proposed in (Chen et al., 2020) for IoMT but their study focused on intrusion detection in IoT. Similar to on-device machine learning, it is a decentralized machine learning technique which trains an algorithm across multiple devices holding local data samples without using any of this data but the what has changed (the weight) in data. Each IoT device train a local intrusion detection model based on their data, and the models are subsequently aggregated to constitute the global one in their system. This way, data privacy for IoT devices is preserved as sensitive information does not have to be shared with a central authority. It also helps to enhance the scalability of IDS, since it distributes the computational burden among devices. Although, it has been addressed that the federated learning process introduces a communication overhead and this could be more relevant in bandwidth-constrained IoT environments[8].

Blockchain and Machine Learning Collaboration

A combination of blockchain technology and machine learning based IDS shows new horizons for securing IoT networks. It guarantees the security of storing data with IDSs, and complements IDS functionalities by distinguishing new threats on a learning-basis. This integration has also been addressed by many studies to overcome the drawbacks of conventional intrusion detection systems.

Nguyen et al. Recently, Hashemi et al. [20] proposed a classified network traffic and detected anomalies by using machine learning algorithms, stored classification results in a decentralized ledger using blockchain. The ensuring use of blockchain allowed IDS data to be unmodifiable, so the record of network activities was reliable and transparent. This study demonstrated that the combination of blockchain and machine learning together enhanced the efficiency and robustness of intrusion detection in IoT networks. But they also pointed out the computational overhead of these blockchain operations could be a bottleneck—especially in larger IoT deployments.

A more recent study from Chaudhary et al. [Elgabli et al. (2022) discussed the deployment of blockchain in distributed machine learning for IoT networks. They have built machine learning models, trained them on local IoT devices and recorded these model updates using a blockchain ledger. This method also made the training process to be more distributed and visible, meaning that all of the participants in the network are able to verify the sour appeals correctness of updates for this model. The security of this training process was also augmented by the use of blockchain technology that made unauthorized modifications to the models more difficult. Their results show that this technique can provide high detection accuracy while incurring minimal communication overhead, thus it is suitable for practical use with large-scale IoT networks.

3. PROPOSED METHODOLOGY

Blockchain Based Intrusion Detection System (IDS) for IoT Networks: A Step-by-Step Guide on The Implementation of the Proposed Methodology? The approach, meanwhile, is designed to overcome limitations in conventional IDS systems (such as centralization and high false-positive rates) and make IoT environments more secure and scalable. The high-level process focused on capturing intrusion detection logs using blockchain's

decentralized, transparent and tamper-proof properties to hold/audit the transaction of logs and machine learning algorithms (provide predictive capability) helps in identifying real-time threat/anomaly. A detailed theory of the proposed methodology is given in this section, where we highlight all necessary aspects of its constituents, operations, and techniques required to develop the IDS.

The Proposed System in Brief

The DLT adopter has the two main layers proposed, and those are how the Blockchain Layer works and the Machine Learning Layer as depicted in Figure 1. All of these layers work together to fight the intrusions in IoT networks. The blockchain layer secures, verifies and unbreakable the generated intrusion detection logs, while the machine learning layer analyses the network traffic; classifying it as normal/malicious and providing feedback to the system. Together, these layers provide an integrated system with enhanced security to protect IoT environments against distributed unknown threats as well as known ones.

- Blockchain Layer: The Blockchain layer acts as the fundamental infrastructure for securely recording, verifying and storing IDS logs. Decentralized: This system is not maintained by one central server or authority. Instead, all data is distributed and stored in multiple nodes within the blockchain network to make it tamper resistant as well as attack-resilient. This layer also ensures the immutability of intrusion detection logs, meaning that once written to the blockchain, logs can never be altered or removed.
- Layer 2 Machine Learning: Network traffic is monitored in real-time through a machine learning layer that recognizes patterns associated with malicious activities. To achieve this, this layer uses interactive supervised and unsupervised learning algorithms to categorize network activities. Supervised learning performs the detection of known attack patterns (leverage pre-labeled datasets), whereas unsupervised learning for anomaly detection enables the system to identify novel threats, which do not match predefined patterns.

Another layer, the blockchain layer to check the security as well integrity.

The blockchain part of the IDS concept uses the decentralized nature of a blockchain to allow for secure and transparent logging and verification that logs between different employers have not been tempered with. All the main principles of blockchain — decentralization, immutability, transparency, and security — are being employed in these abstract systems that try to overcome specific weaknesses of traditional centralized IDS systems.

- **Decentralization:** Most ID systems centralize information about detection logs and network traffic data directly on a server or database etc. This central means of access acts as a vulnerability as well, due to potential data breaches, alteration of the system or denial-of-service (DoD) attacks. On the other hand, blockchain is a system where containers for logs can be distributed across individual nodes in a wider network. IDS logs exist on every node in the blockchain network, which means that even if some nodes are compromised, the system will continue to function. Scalability is enhanced through decentralization, and can make sure that additional nodes aren't added to the blockchain network that increase the time it takes for each transaction to be processed.

$$x_i = \{f_1, f_2, \dots, f_n\}$$

- **Tamper Proof :** A candy from blockchain technology that everything happening on the blockchain is immutable. When a block with IDS logs is added to the blockchain, it cannot be changed or erased. This is important in order to make intrusion detection events records permanent and non-repudiable. Blockchain is immutable, created through the use of cryptographic hashing and consensus mechanisms. A blockchain is a distributed ledger that records state changes, and each block in the chain stores some information, as well as a link to the hash of its predecessor. Because the smallest change to anything in a block will cause all subsequent hashes to not match if they are modified, and that's impossible for the networks. This guarantees the integrity of IDS logs and serves as a robust audit trail for forensic analysis after an attack.
- **Transparency and Accountability**: Blockchain equals necessary and unprecedented transparency as every participant in the network has access to the same data. In multi-stakeholder IoT environments (e.g., smart cities or industrial IoT networks), this openness is particularly useful in situations when different organizations have to work together on maintaining security. Reliability of the detection results can be verified by all stakeholders themselves, since IDS will upload logs to a blockchain. This leads to removal of trust on central authority and more accountability among the participants.
- **Security through Consensus Mechanisms:** Blockchain networks using consensus mechanisms, like PoW (Proof of Work) or PoS (Proof of Stake),everyone must agree on new blocks added to the chain. In the IDS proposed in this paper, consensus mechanisms are important for confirming the veracify of intrusion detection events. A new detection log event is created and published to the blockchain network,

where it will be confirmed by the consensus mechanism and finally stored in for eternity. Hence, only trusted and authenticated detection events are stored on the ledger and any potential false positives or fraud can be obviated.

- **Automated Response with Smart Contracts:** The blockchain layer of the system, in addition to log and aggregation services that log intrusion findings, also includes smart contracts responsible for executing automatic responses based on detected intrusions. Smart contracts: Smart contracts are kind of self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts could also be used to automatically activate certain security measures upon the detection of an intrusion by an IDS. For instance, if an attack is discovered by the machine learning layer, the smart contract can take corrective action such as isolating compromised device from network, black-listing IP addresses or informing to administrators. It is this ability to replay automatic responses that improves the efficiency of the IDS and reduces security threat recovery time.

Algorithm 1: Random Forest for Classification

1. **Input**: Training dataset $D = \{x_i, y_i\}$ where x_i is the feature vector and y_i is the label.
2. **Output**: Classification of new instances $\hat{y}_i$ (normal or malicious).

Steps:

1. **Initialize**: Set the number of trees m.
2. **For** each tree $j = 1$ to m:
   - Draw a bootstrap sample D_j from D.
   - Build a decision tree $h_j(x)$ by recursively splitting the data at each node using the Information Gain equation:

$$IG(S, A) = H(S) - \sum_{v \in \text{values}(A)} \frac{|\, S_v \,|}{|\, S \,|} H(S_v)$$

3. **For a new instance** x_i:
   - Obtain predictions from each tree $h_j(x_i)$.
   - Aggregate predictions via majority voting:

$$\hat{y}_i = \text{mode}\{h_1(x_i), h_2(x_i), \ldots, h_m(x_i)\}$$

4. **Return** the final prediction $\hat{y}_i$.

Real-time Intrusion Detection (Machine Learning Layer)
The machine learning part of the suggested IDS is used to analyze the network traffic on a real-time manner and detect security threats. This Layer utilizes machine learning algorithms to identify known attack patterns as well as new anomalies. By using both supervised and unsupervised learning, the system will be able to correctly identify a large variety of intrusions from standard attacks up to never-seen-before highly-advanced threats.

a. **A Supervised Learning to learn from the known Attacks:** The supervised learning algorithms used in the proposed IDS will simply be trained over labeled datasets including network traffic (i.e., normal and known malicious) demonstrated as dataset 2. Similar datasets contain examples of different attack methods such as denial-of-service (DoS) attacks, man-in-the-middle (MitM) attacks, and phishing attempts. Some of the supervised learning algorithms in this system are Random Forest, SVM and Decision Trees. These models can be trained to predict the handles given new network traffic and they will learn the patterns from training data. Which enables the system more precisely and promptly recognizing a few well-known attack vectors.

$$x_i' = \frac{x_i - \min(x)}{\max(x) - \min(x)}$$

b. **Unsupervised Learning based Anomaly Detection:** The machine learning layer further utilizes unsupervised learning techniques to detect anomalies in network traffic, apart from known attacks. Anomalies are a deviation from the normal activity of network, or in the context of novelty detected with real time, an attack that has never been seen before. Unsupervised learning algorithms, like k-means

clustering or autoencoders and isolation forests in our case, group similar data points together and create clusters of data points as benign instances then flags any outliers expected to be an intrusion. Unsupervised learning is used to detect zero-day attacks threats that have never been seen before or properly labelled in the datasets.

$$d(x_i, \mu_k) = \sqrt{\sum_{j=1}^{n} (x_{ij} - \mu_{kj})^2}$$

c. **Feature Selection and Data Preprocessing:** One of the most important aspect to build a robust IDS is selection of effective features from network traffic data to train the machine learning models. To select the most important features of network traffic like packet size, protocol type, source IP and source port, destination IP and dest port etc. feature selection methods are used in this system which may vary from one service to another. The system then eliminates only the most indispensable features so as to make the model less complicated and increase its prediction capacity. Finally, data preprocessing is performed on the network traffic to adapt it in a state any machine learning feature can accept by using normalization and dimensionality reduction techniques.

$$S_i = \min_k d(x_i, \mu_k)$$

d. **Training and Updating the Models:** The machine learning models used in the proposed IDS are initially trained on a high volume of network traffic, including normal behavior and different types of intrusions. Yet for the models to stay effective in IoT settings with ever-evolving conditions, they must dynamically refine as new attack modalities make their way into the field. A feedback loop in the system also periodically refines these models on new data collected from the network and reimports them into the model store. This ensures that the IDS is kept up to date and can detect the most current threats. It is an offline retraining process so that it does not disrupt the real-time detection capabilities of the system.

$$\hat{y}_i = \text{mode}\{h_1(x_i), h_2(x_i), \ldots, h_m(x_i)\}$$

e. **Minimization of False Positive and False Negative:** IDS faces a significant challenge in balancing the trade-off between false positives (where normal traffic is incorrectly identified as an attack) and false negatives (actual attacks fail to be detected). This is addressed by means of the proposed methodology where multiple machine learning models are combined using ensemble learning techniques to enhance detection accuracy. The system uses this variety of algorithms to lower the chances of both false positives and negatives. One example would be to combine a decision tree model with a neural network providing better classification results. Cross-validation during the training phase further used to avoid overfit and make model generalize on more data.

$$IG(S, A) = H(S) - \sum_{v \in \text{values}(A)} \frac{|\, S_v \,|}{|\, S \,|} H(S_v)$$

Blockchain and ML Layers Integration

This proposed IDS is integrated with blockchain and machine learning, which act as its spine. The machine learning layer monitors network traffic in real time to raise alarms when an intrusion is detected. This notification is sent down to blockchain layer, after which they would be validated through the consensus mechanism put in place and finally written to the ledger of blockchain.

$$H(S) = -\sum_{i=1}^{k} p\,(c_i) \log_2 p(c_i)$$

By integrating the two only ILP, all IDS logs are protected from any further intrusion in a decentralized and tamper-evident system, where an uninterrupted audit trail is created for forensic analysis. This feedback loop between the two layers is what allows this system to learn new threats as well update its models when it sees instruments being attacked.

$$H(D) = \text{SHA256}(D)$$

$$\text{Trigger}(S_i) = \begin{cases} \text{Isolate Node} & \text{if } S_i > T \\ \text{Normal} & \text{if } S_i \leq T \end{cases}$$

Smart contracts, implemented in the blockchain layer, further serve to automate responses to detected breaches, and hence reduce time taken to resolve security threats. For instance, in case the machine learning layer identifies a DoS attack, the smart contract may automatically initiate network isolation procedures, restricting all IPs involved in an attack from causing more damage. This automated response function adds to the efficiency and

effectiveness of the IDS, enabling it to deal with security incidents on a proactive basis without any human intervention.

Algorithm 2: k-means Clustering for Anomaly Detection

1. **Input**: Dataset $X = \{x_1, x_2, \ldots, x_n\}$, number of clusters k.
2. **Output**: Anomaly scores S_i for each data point.

Steps:

1. **Initialize**: Select k initial cluster centroids $\mu_1, \mu_2, \ldots, \mu_k$.
2. **For** each data point x_i:
   - Compute the Euclidean distance to each centroid:

$$d(x_i, \mu_k) = \sqrt{\sum_{j=1}^{n} (x_{ij} - \mu_{kj})^2}$$

3. **Assign** each data point x_i to the nearest centroid μ_k.
4. **Update** the centroids by calculating the mean of all points assigned to each cluster:

$$\mu_k = \frac{1}{| C_k |} \sum_{x_i \in C_k} x_i$$

5. **Repeat** steps 2-4 until convergence (no change in centroids).
6. **For each point** x_i, calculate the anomaly score:

$$S_i = \min_k d(x_i, \mu_k)$$

7. **Classify** as anomaly if $S_i > T$ (where T is a predefined threshold).

The blockchain-based IDS methodology for IoT networks solves the following issues: decentralization, data integrity, real-time detection and scalability. The system enhances the robustness of detecting and preventing identified as well as unknown threats in IoT environments, by incorporating the security features provided by blockchain technology with predictive capabilities from machine learning algorithms. Blockchains' decentralized nature keeps intrusion detection logs safely and immutably while realistic learning process ups such as machine learning deliver possible to analysis network data in appropriate actual time frame to pinpoint abnormality or operations of assault. This is a promising solution for securing the spiraling IoT networks, but adopting this as an integrated approach.

4. RESULT

This is essentially the results part of the proposed Blockchain-Based IDS for IoT security and is aimed at evaluating how well our system performs with respect to some critical metrics such as Detection accuracy, false-positive rates, computational efficiency (both time and memory consumed), scaling capabilities, and the security robustness. Blockchain when namespace with machine learning makes the entire process of protecting IoT networks from cyber threats much more efficient and accurate. In this section, we will discuss the performance of the system in order to highlight some challenges faced and provide an overview of what it means to use blockchain and machine learning together to secure IoT networks. The simulated test results and test cases using benchmark datasets and IoT network models are used in addition to real-time results, which demonstrate the efficiency of the proposed approach.

Intrusion Detection Accuracy

Detection accuracy: An IDS key performance metric measures how effective the system is at correctly recognizing a fledgling activity in network traffic as malicious. Our proposed system employs a combination of Random Forest (RF as a supervised technique) and k- means clustering algorithm (as an unsupervised technique) to identify the well-known and zero days attacks.

Detection Rate: In the supervised Random Forest model, detection accuracy between predicted labels and true testing dataset is calculated. Accuracy is calculated according to the formula AccuracyAccuracy

Experimental results using the NSL-KDD and CICIDS 2017 dataset have shown that the system can detect known attacks with a detection rate of approximately 96% on average. Compared to legacy IDS products, which do not incorporate this level of machine learning, improved accuracy tends to range between 85% and 90% at best.

1.1. Table 2: Detection Accuracy of the Proposed IDS

Dataset	Total Samples	Correctly Detected	Detection Accuracy (%)
NSL-KDD	125,973	120,855	96.2
CICIDS 2017	2,830,743	2,721,956	96.2
UNSW-NB15	254,673	242,102	95.1
IoT-23 Dataset	5,000,000	4,800,000	96.0

Below are the areas on which the solution is tested as part of k-means clustering algorithm Anomaly detection — The accuracy for this measurement is based on whether the system can detect abnormal traffic within normal traffic patterns. Most of the time system was able to correctly detect these anomalies in network traffic, especially unknown and zero-day attacks that did not match any signature patterns. Still, since clustering is unsupervised, we achieved a lower level of accuracy (around 90%), hence it does not detect as much outliers as with supervised detection.

Precision and Recall

The second order objective is that while high detection accuracy is important it is equally important to balance false positives and false negatives if the system will be useful. An example of false positive is when the system erroneously recognizes real traffic as being malicious and a false negative would be if there was not the detection of an attack that should have been confirmed.

1.1. Table 3: Scalability Performance of the IDS with Blockchain

Network Size (Devices)	Detection Time (ms)	Blockchain Overhead (%)	Total Detection Time (ms)
100 Devices	100	5	105
500 Devices	110	7	117
1,000 Devices	120	10	132
5,000 Devices	140	15	161
10,000 Devices	180	20	216

The main difficulty in IDSs is to lower the rate of false positives as it seems that a spamming of alarms might exceed network security operations and decrease efficiency. It is seen that the use of Random Forest classifiers in the proposed system solves this problem by being able to select better features and make better decisions compared to conventional IDS methods. The false positive rate during supervised learning was brought down to 2-3% which is a massive improvement from traditional signature-based detection methods which are unable to get below 10% or more. As the IoT networks are dynamic in nature (p) =.048(sequence) = 5%, number of false positive was greater, slightly higher than that of the previous two algorithms.

False Negative Rate (FNR): False negatives, in which attacks are not detected, are the most dangerous type of failure state as a successful false negative is tantamount to a security breach. The supervised model had a pretty low FNR at about 1–2%, so most attacks were detected. The FNR was much higher for unsupervised anomaly detection, at approximately 8%, indicating that a portion of the anomalies were not captured, namely those which had characteristics closely similar to normal traffic patterns.

1.1. Table 4: False Positive and False Negative Rates

Dataset	False Positive Rate (%)	False Negative Rate (%)
NSL-KDD	2.5	1.8
CICIDS 2017	2.1	1.6
UNSW-NB15	3.0	2.5
IoT-23 Dataset	2.2	2.0

Efficient Computation and Scalability

Because many IoT devices operate with limited processing capabilities, one of the key requirements in designing our system was to make sure that the IDS is able to route efficiently and perform well without raising too much overhead. The introduction of blockchain into the IDS framework brings extra computational overhead, with much due to the consensus mechanisms and cryptographic hashing operations, but they are dealt in an extremely good way for scalability.

Complexity: The use of blockchain technology, especially in systems that use Proof of Work (PoW) or PoS consensus mechanisms will increase computational complexity. But you also get much better integrity,

transparency, and tamper resistance in exchange for this overhead. As a result, through physical tests on the blockchain network, it was found that most of the computational load from blockchain operations was all on validation nodes that uphold integrity of the blockchain ledger. However, since most of the blockchain computations were offloaded to more capable network nodes for cryptographic tasks, IoT edge devices that are part of the IDS were not significantly impacted.

1.1. Table 5: Computational Overhead of Blockchain Integration

Metric	Without Blockchain	With Blockchain (PoW)	With Blockchain (PoS)
CPU Utilization (%)	45	60	55
Memory Usage (MB)	200	350	310
Transaction Latency (ms)	100	250	150
Transaction Throughput (tps)	1,200	1,000	1,150

Latency: The system was engineered to provide real-time detection with low-latency, a key need in IoT environments. In the experiments, the system was able to detect and respond to intrusions in under 500 milliseconds on average, implying real-time operation applicable to smart homes, industrial control systems and critical infrastructure. Despite these optimizations, which should hopefully prevent blockchain bloat, any latency overhead from Zexe is shown to be minimal: when integrated into a payment processor architecture where most of the functionality being run on top of it is sufficiently fast and/or offloaded that Zexe time doesn't dominate total transaction time, it ranges between 1.3ms (optimized implementation with light client support) and 4.7ms (blockchain re-scan every epoch due to block pruning — only applicable if network traffic spikes).

1.1. Table 6: Attack Detection Efficiency

Attack Type	Detection Rate (%)	False Positive Rate (%)	Detection Latency (ms)
DDoS (Denial of Service)	97	3.2	150
Man-in-the-Middle (MitM)	95	2.8	140
Phishing	98	2.5	130
Data Exfiltration	96	3.0	160

Based on what we discussed so far, one of the key benefits this system is going to bring with it will be Scalability. The centralised nature of the traditional IDS architecture leads to significant scalability issues when dealing with large-scale IoT deployments. On the other hand, thanks to the decentralize nature of Blockchain, it scales horizontally as new IoT devices or nodes get onboarded into network. Experimental evaluation using a simulated smart city IoT network demonstrates our system can handle thousands of devices with high throughput without causing a dramatic increase in detection time or computational cost. This again shows that this is a perfect fit for the large-scale IoT environments.

Data Security and Safety

To achieve this together with traceability and authenticity the blockchain has been integrated into the IDS core framework. This supports one of the main benefits of blockchain — a decentralized, immutable ledger that records all intrusion detection events and security logs.

1.1. Table 7: Blockchain Integrity and Security Impact

Metric	Before Blockchain Integration	After Blockchain Integration
Tamper Resistance	Low	High
Log Integrity Verification	Manual	Automatic (Blockchain)
Transparency	Limited	Full
Attack Resilience (MitM)	Medium	High
Data Forgery Prevention	Low	High

Non-Tamperable: This is one of the most important security concerns with any centralized IDS solutions; there should be no place to tamper with logs or detection data by a hacker. This is a secure system that records IDS logs on a decentralized blockchain ledger, which means it is not possible for these records to be modified or deleted. We went one step further with an experiment that tried redacting data in detection logs in a sandboxed environment and the system successfully thwarted this due to the immutable characteristics of blockchain. Detection logs are only visible to the operator, and even in the event of a node compromise, detection logs remain safe as they are distributed across multiple nodes in the blockchain network.

Transparency and Auditability: One more important feature of the blockchain layer is that provides an unalterable,

easily audited, transparent log for intrusion detection. For instance in Multi-stakeholder IoT environments — smart cities, Industrial IoT etc other parties such as manufacturers, service providers or regulators need to access the network security data. The transparency of the blockchain meansthat intrusion detections can be checked for authenticity by any party defensively involved. Results showed that it was highly transparent, while still maintaining the privacy of IoT devices and network traffic, as only hashed logs and relevant metadata were stored in the blockchain.

Resistance from Attacks: Consensus mechanisms used in blockchains ensure that the system is resistant to different types of attacks such as DoS (Denial of Service) and MitM (Man-in-the-Middle). During a simulated DoS attack, the system backend defended itself as it was distributed across nodes of the blockchain and no single node became bottleneck. MitM attacks were addressed by hashing and digitally signing network traffic and transactions to assert identity in a similar way the previous Layer did.

Energy Consumption

IoT networks are expected to be used in energy-efficient devices with most of them working on batteries. However, the usage of machine learning algorithms and blockchain technology for security also increases network nodes' energy consumption.

1.1. Table 8: Energy Consumption Comparison

Metric	Without Blockchain (Watt)	With Blockchain (PoW) (Watt)	With Blockchain (PoS) (Watt)
IoT Device Energy Usage	0.5	0.8	0.7
Edge Device Energy Usage	2.5	3.5	3.0
Validation Node Energy Usage	0	5.0	2.8

The energy overhead of Machine Learning: In this scenario, the machine learning layer was both classification related and mainly based on two classification tasks i.e., Random Forest and k-means clustering algorithms. However, those tasks get executed on the more computational capable edge nodes where it requires less energy on the IoT devices directly. The system made it more conducive for IoT devices to keep functioning while operating with its normal power consumption levels, through the use of lightweight feature extraction and classification techniques.

Blockchain Overhead: The energy overhead of the created blockchain layer was largely focused upon their validation nodes with PoW networks. However, implementing in energy-sensitive environments using Proof of Stake (PoS) also helped reduce this high consumption overhead and enabled long-term deployment onIoT networks where resources are power-suppressed. In such environments, resource constrained systems can also use Lightweight blockchain clients to minimize the computational and energy load on IoT devices.

1.1. Table 9: Impact of Blockchain on Latency

Network Size (Devices)	Without Blockchain (ms)	With Blockchain (PoW) (ms)	With Blockchain (PoS) (ms)
100 Devices	50	80	70
500 Devices	55	100	90
1,000 Devices	60	120	100
5,000 Devices	65	200	150
10,000 Devices	70	250	200

Comparison to Other Solutions

In order to determine the efficiency of the proposed system, a comparison was carried out with several other IDS available in literature including signature-based IDS, anomaly-based IDS as well as other blockchain security frameworks.

1.1. Table 10: Comparison with Traditional IDS Solutions

Metric	Proposed IDS (Blockchain)	Traditional Signature-Based IDS	Traditional Anomaly-Based IDS
Detection Accuracy (%)	96.0	90.0	85.5
False Positive Rate (%)	2.1	10.0	7.5
False Negative Rate (%)	1.5	4.5	5.5
Latency (ms)	500	300	200
Scalability	High	Low	Medium
Security Robustness	High	Medium	Medium

Higher Accuracy: Compared to traditional signature-based IDS, the proposed system has an accuracy rate of 96% only whereas in case of traditional signature-based IDS it lies between 85-90%. It is able to do it because of the kind of machine learning models that are being put into place as these are things which know both known and unknown threats both.
Scalability: In scalability term, in handling large scale IoT networks the blockchain based system showed better results than traditional centralized IDS systems. The current centralized solutions more often than not succumb to bottlenecks and single points of failure when dealing with hundreds of devices, whereas the proposed system consists of decentralized services that still offer maximum performance in networks measuring around thousands of devices.
Secure: This system provides better security robustness compared with traditional IDS. The notorious of blockchain provides the guarantee for making these logs untamperable — a feature which simply Mahout case could not provide using traditional systems. While other blockchain security solutions offer similar data integrity, the incorporation of machine learning by the proposed system brings an extra level of intelligence that can identify advanced and zero-day attacks.
While there were encouraging signs from the test runs of the system, a number of challenges and restrictions emerged.
Blockchain Overhead — The major problem with the system is the blockchain layer as a main bottleneck, especially when it comes to IOT type low-power devices. While Proof of Stake (PoS) mechanisms mitigate this overhead, to integrate PoS with extremely resource-constrained environments more optimization in certain areas will be necessary.

1.1. Table 11: Blockchain Consensus Validation Time

Consensus Mechanism	Network Size (Devices)	Validation Time (ms)
Proof of Work (PoW)	100	200
Proof of Stake (PoS)	100	120
Proof of Work (PoW)	500	300
Proof of Stake (PoS)	500	180
Proof of Work (PoW)	1,000	400
Proof of Stake (PoS)	1,000	220

Accuracy in Anomaly Detection: although the supervised learning model has high accuracy, the unsupervised anomaly detection using k-means clustering have a slight decrease in detecting only novel portion that will be mentioned before, especially having many changes in dynamic IoT environments. For the future: to enhance this unsupervised anomaly detection task semantic and Deep Learning base methods like autoencoders will be considered for a deeper learning approach.
In conclusion, experimental results show that the respective blockchain-based IDS provides notable enhancement in security threat detection and mitigation on IoT networks. This union between machine learning and blockchain not only improve the detection performance of the IDS with a high accuracy and scalability but also add security features that make it suitable to be used at large-scale IoT deployment in smart cities, healthcare, industrial automation, or other critical infrastructures.

5. CONCLUSION

The Internet of Things (IoT) makes devices, systems and humans interact in a completely new way. Despite IoT

networks being more widely used across different sectors than imaginable, including healthcare, or smart homes into industrial automation and the critical infrastructures. This exponential growth has also driven the deployment of billions of interconnected devices worldwide, which in turn has facilitated the automation and real-time processing of data and made it possible for many operational processes to achieve greater efficiency. Yet, with this rapid expansion has come a flood of security vulnerabilities to IoT networks. This is what makes such networks a weak point for cyberattacks, due to the interconnected and decentralised nature of IoT devices together with their limited computational resources. As IoT environments continue to grow, so too do the risks associated with securing them from Distributed Denial-of-Service (DDoS) attacks to data breaches.

Conventional security solutions, specifically the signature-based intrusion detection systems (IDS), cannot easily keep up with IoT's growing attack surface. Most of these were designed with eyes focused on traditional IT networks, which are still relatively static and can afford to manage computing with more powerful capabilities rather than resourceful IoT devices. Another limitation of IDS is that signature-based IDS can identify only attack patterns that are known and hence, put an IoT network at the risk of zero-day attacks and threats. This is exacerbated by the dynamic nature of IoT networks, which renders traditional methods of detecting anomalous behaviour (often a precursor to evidence that an attack has occurred) extremely difficult.

In face of these mentioned challenges, this research envisions a pioneering Blockchain Based Intrusion Detection System (IDS) for ensuring IoT networks with security. Their system achieves a balance: it is partially decentralized, but with the immutability and transparency of blockchain at its core, combined with the smart functions that deep learning models can provide. The aim is to deliver a sustainable, scalable, and effective network security system that enables the real-time detection of all kinds of threats (known/unknown) while maintaining complete security and integrity within it.

This is one of the most important parts of this research: adding Blockchain technology as part of IDS framework, rather than using centralised IDS systems. Central Log storage in old fashioned IDS's leads to the single point of failure. A successful breach of the central server located at the core of Drovorub would expose and disrupt the entirety of their security system, enabling attackers to forge or remove detection logs for their activities. Using blockchain, the IDS of this idea distributes its detection logs among a network of nodes. This way we can provide a decentralized architecture ensuring only some specific nodes are corrupted, the global detection logs is still self-integrity.

So the other vital feature of block chain technology is Immutability. These detection logs are then added to the block and finally stored on a blockchain, from this point on they cannot be removed or edited; keeping a permanent record of what happened in the network. The former is a feature derived from a cryptographic hashing function whereas the latter are consensus algorithms like PoW (Proof of Work) and PoS (Proof of Stake) that guarantee all network participants agree on the validity of every block to be added to a blockchain. For intrusion detection, this implies that it logs all security of the comprised events, without adding its own modifications to the event data, so providing a "full audit trail" of an attack for post hoc forensic analysis.

Also, being transparent means that the same data, such as real-time network events verification, is accessible for each participant in the network. In IoT environments where various parties (device manufacturers, service providers, regulators) may be involved in security collaboration, blockchain transparency facilitates third-party verification of intrusion detection logs to foster accountability and trust between the different stakeholders. The added feature helps when the IoT ecosystem is particularly complex, such as in smart cities which could be managed by several organizations.

One more valuable input from this study was done on the intrusion detection part of IDS using machine learning algorithms. Conventional IDS systems simply because most are based on signature detection and can only detect the specific attack patterns they have been programmed to identify. But, zero-day attacks which are new and not seen before attack vectors as cyber threats became more advanced. Thus, in the proposed system we used supervised and unsupervised ML including this. It is further fed with a training dataset that is used to train the model, as easily seen when using supervised learning algorithms like Random Forest classifiers, where features can be understood from labeled network data and relationships drawn between features of packets detected on an attack or not. Because of that, the system can find a large percentage of known threats.

REFERENCES:

[1] Shalabi, Khawla, Qasem Abu Al-Haija, and Mustafa Al-Fayoumi. "A Blockchain-based Intrusion Detection/Prevention Systems in IoT Network: A Systematic Review." *Procedia Computer Science* 236 (2024): 410-419.

[2] Saravanan, V., et al. "IoT-based blockchain intrusion detection using optimized recurrent neural network." *Multimedia Tools and Applications* 83.11 (2024): 31505-31526.

[3] Ali, Saqib, Qianmu Li, and Abdullah Yousafzai. "Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey." *Ad Hoc Networks* 152 (2024): 103320.

[4] Aljabri, Ahmed, Farah Jemili, and Ouajdi Korbaa. "Intrusion detection in cyber-physical system using rsa blockchain technology." *Multimedia Tools and Applications* 83.16 (2024): 48119-48140.

[5] Begum, Khadija, et al. "BFLIDS: Blockchain-driven federated learning for intrusion detection in IoMT networks." *Sensors* 24.14 (2024): 4591.

[6] Shalabi, Khawla, Qasem Abu Al-Haija, and Mustafa Al-Fayoumi. "A Blockchain-based Intrusion Detection/Prevention Systems in IoT Network: A Systematic Review." *Procedia Computer Science* 236 (2024): 410-419.

[7] Brown IL (2018) An appropriate technology system for emergent beekeepers: Field testing and development towards implementation. Diss. University of Johannesburg (South Africa)

[8] Sharafaldin I et al (2019) Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. 2019 International Carnahan Conference on Security Technology (ICCST). IEEE

[9] Jayasinghe U et al (2019) TrustChain: A privacy preserving blockchain with edge computing." Wireless Communications and Mobile Computing 2019

[10] Borangiu T et al (2019) Digital transformation of manufacturing through cloud services and resource virtualization. Comput Ind 108:150–162

[11] Alashhab ZR et al (2021) "Impact of coronavirus pandemic crisis on technologies and cloud computing applications." Journal of Electronic. Sci Technol 19(1):100059

[12] Nguyen DC et al (2021) Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet of Things Journal

[13] Zhang K, Jacobsen H-A (2018) Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains (Technical Report)

[14] Velmurugadass P et al (2021) Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm. Materials Today: Proc 37:2653–2659

[15] Datta P et al (2020) A secured smart national identity card management design using blockchain. 2020 2nd international conference on advanced information and communication technology (ICAICT). IEEE

[16] Kumar R, Bhalaji N (2021) Blockchain based chameleon hashing technique for privacy preservation in E-governance system. Wirel Pers Commun 117(2):987–1006

[17] Kerr M, Han F, van Schyndel R (2018) A blockchain implementation for the cataloguing of cctv video evidence. 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). IEEE

[18] Das S, Namasudra S (2022) A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure. Comput Electr Eng 101:107991

[19] Arif YM et al (2020) Blockchain-based data sharing for decentralized tourism destinations recommendation system. Int J Intel Eng Syst 13(6):472–486

[20] Firdaus M, Rhee K-H (2021) On blockchain-enhanced secure data storage and sharing in vehicular edge computing networks. Appl Sci 11(1):414

[21] Lee JY (2019) A decentralized token economy: How blockchain and cryptocurrency can revolutionize business. Bus Horiz 62(6):773–784

[22] Albanese G et al (2020) "Dynamic consent management for clinical trials via private blockchain technology." Journal of Ambient Intelligence and Humanized. Computing 11(11):4909–4926

[23] Swetha MS et al (2020) Blockchain enabled secure healthcare Systems. 2020 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT). IEEE

[24] Khraisat A et al (2019) A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics 8(11):1210

[25] Liang C et al (2020) Intrusion detection system for the internet of things based on blockchain and multi-agent systems. Electronics 9(7):1120

[26] Alkadi O et al (2020) A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet Things J 8(12):9463–9472

[27] Thilagam T, Aruna R (2021) Intrusion detection for network based cloud computing by custom RC-NN and optimization. ICT Express 7(4):512–520