# A Review on the Integration of Blockchain and Intelligent Learning Techniques for Threat Detection and Security Enhancement in IoT Networks

**Shamsudeen Mohammed S., Nwobodo-Nzeribe Nnenna Harmony., *Aghaizu Herman Chijioke**

**Department of Computer Engineering, Enugu State University of Science and Technology, Enugu, Nigeria**

***Corresponding Author**

**DOI: https://doi.org/10.51584/IJRIAS.2026.11070116**

**Received: 29 June 2026; Accepted: 04 July 2026; Published: 08 August 2026**

## ABSTRACT

The growth of the Internet of Things (IoT) has brought about security concerns owing to the massive global integration of diverse and constrained devices. Blockchain, Machine Learning (ML) and Deep Learning (DL) techniques have been proposed as effective ways to improve IoT security. This paper reviews the literature on the use of blockchain and smart learning techniques for security enhancement and threat detection in IoT networks. Blockchain offers a decentralized and immutable approach to secure data integrity, authenticating and controlling access to IoT devices, while ML and DL techniques allow intelligent monitoring of network data to detect anomalies and predict cyber-attacks. This study follows a systematic literature review approach, examining peer-reviewed journal articles and conference proceedings from 2019 to 2024. The analysis shows while blockchain, ML and DL technologies play a crucial role in enhancing IoT security, they each have limitations including scalability, computational overhead, data dependency and lack of flexibility against new cyber threats. Additionally, the majority of studies concentrate on either blockchain-based security or ML-based intrusion detection, with limited study on the integration of the two for real-time threat detection and mitigation. The study highlights this limitation and calls for the development of intelligent hybrid models that integrate blockchain technology with ML/DL to address scalability, adaptability and real-time security for IoT networks to ensure confidentiality, integrity and reliability.

**Keywords:** Internet of Things (IoT), Blockchain Technology, Machine Learning, Deep Learning, Cybersecurity

## INTRODUCTION

The Internet of Things (IoT) is a paradigm that extends the capabilities of the internet to a vast array of physical objects embedded with sensors, software, and connectivity. This integration allows devices from household appliances to industrial machinery to communicate and exchange data over the internet, creating a seamless network of interconnected objects. The core idea behind IoT is to enhance the functionality and efficiency of these devices by enabling them to interact with each other and with centralized systems, thereby automating tasks and improving decision-making processes.

In practice, IoT enables applications such as smart homes, where devices like thermostats, lighting systems, and security cameras can be controlled remotely and operate autonomously based on environmental inputs and user preferences. Similarly, in healthcare, IoT devices can monitor patient vitals in real-time, track medication adherence, and provide data-driven insights that enhance patient care. Industrial IoT (IIoT) applications include predictive maintenance and real-time monitoring of equipment, leading to increased operational efficiency and reduced downtime.

Blockchain technology operates as a decentralized and distributed digital ledger, recording transactions across multiple computers in a way that ensures the security, transparency, and immutability of the data (Jain et al, 2019). Blockchain systems, despite their robustness, are susceptible to a range of vulnerabilities that can

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

undermine their security and functionality. 51% attack is a major vulnerability in blockchain, where a malicious actor gains control of more than half of the network's mining power or stake. This control enables the attacker to manipulate the blockchain in various ways, such as reversing transactions, preventing new transactions from gaining confirmations, and double-spending coins (Abou et al., 2020). Vulnerability lies in smart contracts, which are prone to coding errors and bugs. Since smart contracts are immutable once deployed, any vulnerability in the code can be exploited by attackers, leading to significant financial losses and system breaches. Additionally, the transparency of blockchain transactions, while beneficial, can also pose privacy risks as transaction histories and patterns can be analyzed to reveal sensitive user information (Jain and Pandey, 2019).

To further strengthen IoT security, Machine Learning (ML) techniques have been introduced alongside blockchain. ML enables intelligent threat detection, anomaly identification, and adaptive security mechanisms, making it a valuable complement to blockchain's structural security features. Therefore, this study presents a comprehensive review of existing literature on the integration of blockchain technology and machine learning techniques for enhancing the security of IoT network systems, with the aim of identifying strengths, limitations, and study gaps.

## LITERATURE REVIEW

Kotel et al., (2023) presents a study on the application of blockchain-based approach for the security of Internet of Things (IoT) system. This study introduces a blockchain-based method that makes use of the Hyperledger Fabric blockchain technology to control access in smart homes. The suggested design, which consists of four layers which are the Cloud Storage Layer, Blockchain Platform Layer, Application Layer, and IoT Devices Layer is the study's main contribution. Mapping smart home qualities to Hyperledger Fabric attributes is an important consideration. This mapping makes it possible to create a customised, well-designed solution that can successfully handle the security needs of Internet of Things-based smart homes. The solution's evaluation confirms that it can support smart homes' security needs. To further enhance this study, two important topics might be looked into. Initially, study on the access control system may continue, with real-world testing to ascertain its feasibility and effectiveness.

Reddy (2023) studyed on the security of IoT using blockchain technology. The paper starts off by giving a summary of the IoT security issues that are currently being faced, highlighting the growing complexity and sophistication of cyberattacks that target IoT devices. Then, it presents blockchain technology as a revolutionary framework that can strengthen IoT networks' security posture. IoT security is addressed in relation to the fundamental concepts of blockchain, including decentralisation, immutability, and consensus procedures. A thorough examination of current blockchain-based IoT security solutions, from public blockchains to permission ledgers, along with an evaluation of their advantages and disadvantages, is one of the report's main features. The report concludes by recommending that a comprehensive and cooperative strategy to solve technological, regulatory, and usability problems was the key to the future of blockchain in IoT security.As developments proceed, the possibility of building strong, safe, and scalable blockchain-powered IoT ecosystems continues to be a bright future for both industries.

Bobde et al., (2024) presents a study on enhancing the security of industrial internet of things network through the integration of blockchain. In this method, data is first collected and compressed by sensor nodes, then it is encrypted using the ChaCha20-Poly1305 algorithm and sent to nearby aggregators. The private blockchain gateway, which processes and categorises data according to secrecy levels and decides whether to store it in cloud servers or the Interplanetary File System for increased protection, is an essential component of our system. The proof of authority consensus technique serves as an additional safeguard for the authenticity and integrity of the system. For device authentication, this system uses Zero Knowledge Proof challenges, which optimises data retrieval while carefully balancing security and accessibility. The primary platform utilised for this study's testing setup was Google Colab, a cloud-based Python programming environment that provides an adaptable framework for simulating an Internet of Things (IoT) blockchain network. The work concentrated on important criteria including data size, transmission durations, processing latency, and compression efficiency when evaluating the performance of our system. Notably, we saw an increase in processing latencies and transmission delays with a rise in data size from 10 KB to 100 KB.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

Mulani and Patil (2022) studyed on the use of blockchain-based approach for securing the access control of IoT systems. This paper presents a novel method that combines a multi-agent system with a blockchain to regulate the distribution of an Internet of Things (IoT) system's lightweight, decentralised, secure access management. The main goal of the proposal is to offer a hybrid meta-heuristic Cryptographic Ciphertext Policy-Attribute-based encryption (CCP-ABE) based on permission-secure blocks, which would facilitate efficient resource management while guaranteeing data privacy and access control of cloud data. The three stages of this architecture are (a) resource management and virtual cloud data collecting, (b) hybrid heuristic CCP-ABE, and (c) permission cloud blocks for security. In this instance, the Grasshopper Optimisation Algorithm and the Deer Hunting Optimisation Algorithm (DHOA) was combined to create a hybrid technique for attribute optimisation in CCP-ABE that will yield optimised copies of every attribute from the cloud data. By adjusting the encrypted keys for encryption and decryption, the suggested CCP-ABE-based transmission model secures reduced ciphertext size, computation cost, and encryption cost. It is found that the suggested model has improved by 14.2%.

Gugueoth et al., (2023) reviewed on the use of decentralized blockchain technique for securing the IoT security and privacy. This paper covers the taxonomy of various IoT security concerns and provides a quick overview of the works that have already been done to use Blockchain technology to improve IoT security. A detailed discussion of Blockchain's operation is included, along with a comparison of consensus algorithms and their security and privacy features. This study also covers the benefits, drawbacks, security measures, and performance assessment criteria of integrating blockchain technology with the Internet of Things. This review suggests that blockchain technology is one of the most promising innovations that can improve the security and privacy of Internet of Things data and help the Internet of Things be expanded for a wider range of uses. The concerns that have been found indicate that the use of Blockchain for IoT is still in its infancy, and there is a growing need for study projects that tackle the difficulties and complexities involved in integrating Blockchain with IoT.

Khordadpour and Ahmadi (2024) studyed on the enhancement of security and privacy in blockchain-based IoT environments through anonym auditing. This study explores the special problems and solutions related to the security of Internet of Things (IoT) systems based on blockchain technology, emphasising the use of anonymous auditing to strengthen security and privacy. The suggested security protocol is a vital component in strengthening these systems since it places a high priority on maintaining privacy and anonymous auditing. Our strategy is based on the application of privacy-enhancing techniques and the integration of technology such as Tor for anonymous auditing, which demonstrate a balanced approach to security and privacy. The study has shown our approach's resilience and effectiveness, which distinguishes it from other approaches. But as blockchain and IoT technologies advance, these security measures must also be expanded and improved upon constantly. Future studies will focus on improving the protocol's functionality to make sure it stays applicable and efficient in the rapidly changing world of blockchain-based Internet of Things applications.

Alharbi et al., (2022) studyed on the future trends of integrating blockchain technology with artificial intelligence for security of IoT networks. The goal of this study is to close the knowledge gap between blockchain and artificial intelligence (AI) so that studyers can combine the two to explore new avenues for solution development and strengthen IoT network security. The study employed a systematic approach to assess all pertinent literature on cybersecurity, with three primary stages involved: preparation, assessment, and reporting. The study examined current defensive models and applied a set of measures to assess the 22 studies that were chosen. Additionally, it separated the solutions into three classes: those based on blockchain, those based on artificial intelligence, and those that combine both blockchain and AI at the same time. The future directions this study pointed out will assist security experts in creating a safe blockchain and artificial intelligence integration for IoT networks. Improving the existing distributed IDS models and reducing their drawbacks is one of the fascinating study topics.

Singh et al., (2019) presents a secure and efficient IoT smart home architecture which is based on cloud computing and blockchain technology called SH-BlockCC. An Internet of Things smart house architecture built on blockchain and cloud computing is suggested in this article. The article describes how blockchain technology is used in a smart home network to manage device transactions. It also discusses how green cloud computing,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

which offers green services through a green broker, helps to lessen the suggested model's negative environmental effects. For the purpose of detecting denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks in smart home networks, a security analysis algorithm is described utilising the MCA algorithm. According to the system's outcome, the strategy was able to achieve 60 Mbps throughput in both normal and attack scenarios with a 30-second latency.

Sodhro et al., (2020) studyed towards the use of blockchain enables security technique for industrial internet of things based decentralized applications. The report recommends an algorithm and a provisional blockchain-enabled security framework to safeguard the IIoT system. In order to prevent hackers from listening in on sensitive industrial processes, the suggested algorithm uses a random initial and master key management mechanism. In addition, a unique blockchain-based security algorithm for IIoT systems is used to highly efficiently secure the entire process. The study has three primary contributions. Firstly, it suggests an intelligent decision-making approach for the sustainable, convergent, interoperable, and reliable IIoT system that is based on the Analysis Hierarchy Process (AHP).The AHP-based algorithm assists industry specialists in identifying more pertinent and crucial characteristics to further improve industry yield, such as reliability in line with packet loss ratio, convergence in mapping with delay, and interoperability in conjunction with throughput. A second viable cloud-based platform for the IIoT is suggested. The IIoT's performance and network measurements are finally traded off. As a result of the system, a Consistency Ratio (CR) of 0.007413 was obtained.

Ruzbahani (2024) studyed on harnessing the future of network security and privacy for AI-protected blockchain-based IoT environment. This study investigates how artificial intelligence plays a critical role in supporting blockchain-enabled Internet of Things systems, potentially representing a major advancement in the protection of data confidentiality and integrity across networks. This study assesses how blockchain systems improved by AI may affect IoT network privacy security. IoT devices frequently gather private information, therefore privacy is a top need. Without sacrificing the functionality of IoT systems, AI can help build new protocols that guarantee user anonymity and data privacy. This survey aims to provide a thorough knowledge of how blockchain technology boosted by AI can revolutionise network security and privacy in Internet of Things environments through in-depth examination and case studies. For studyers and practitioners in the subject, this work provides a roadmap.

Ali et al., (2021) presents the use of neural network approach for industrial IoT-based blockchain-enabled secure searchable encryption approach. The article presented a novel hybrid deep neural network approach-based Binary Spring Search (BSS) algorithm based on Group Theory (GT). The suggested method successfully finds the infiltration in the Internet of Things. At first, a blockchain-based approach was used to implement the privacy-preserving system. Because of its significance and value, especially in the context of the Internet of Medical Things (IoMT), the security of Patient Health Records (PHR) is the most important component of cryptography over the Internet. The suggested method updates different policies and offers a safe key revocation mechanism. The result of the system implementation reports that the system achieved an accuracy of 0.96, false positive rate of 0.002, false detection rate of 0.025, false negative rate of 0.022, a cost time <1 and execution time of 0.01seconds.

Xu et al., (2021) surveyed on embedding blockchain technology into IoT for security implementation. The state of the art in blockchain-based IoT security is methodically examined in this article, with a focus on blockchain-embedded IoT security features, challenges, technologies, techniques, and associated scenarios. One significant and expected advancement in the computational communication system is the integration and interoperability of blockchain with IoT. This article's objective is to present a thorough analysis of how blockchain technology can be used to enhance and provide IoT security and privacy. The investigation pinpointed issues with the system, including inconsistent block recording, unreliable data transfer, network bandwidth, consensus procedures, and IoT data processing performance. Then the work concluded by highlighting on future study trends in the technology such as interoperability of IoT, blockchain and 6G, double-chained IoT security scheme, integration of blockchain and edge computing for IoT security and new blockchain-based business mode.

Showkat and Qureshi (2023) studyed on the security architectures, consensus algorithms, enabling technologies, open issues and study directions of securing the internet of things with blockchain approach. A thorough

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

overview of current work on consensus-building, applications, security enhancement, machine learning integration, and computing platforms is provided. Blockchain (BC) is a critical enabling technology for the Internet of Things, and the work mentioned can facilitate it through Machine Learning (ML), Edge Computing (EC), and the Inter Planetary File System (IPFS). The chain's growth is limited by IPFS-enabled BCs that only store hashes on the BC, and the new IPFS software enforces Smart Contracts (SCs) to maintain the Access Control (AC) list. To facilitate BC applications in future mobile IoT systems, Mobile Edge Computing (MEC) is being explored as a viable strategy for reaching consensus for mobile users. The report highlights the potential applications of blockchain technology as well as the challenges encountered in integrating it with IoT. The issues identified in this study are resource constraints, scalability, cost, energy consumption and regulatory compliance issues.

Toka et al., (2021) studyed on securing IoT with blockchain technology. For data gathered from IoT devices, the Hyperledger Fabric blockchain network utilised in this study offers data security, data integrity, secrecy, and authentication. The suggested method makes advantage of the popular Message Queuing Telemetry Transport (MQTT) protocol for Internet of Things data transfer. The method is shown using a mock IoT device network and a basic demo Hyperledger network. The suggested method is examined from the perspective of network security aspects. It is demonstrated that the suggested method can significantly address the IoT security flaws based on the characteristics of the Hyperledger Blockchain network. Nevertheless, there is no performance assessment of the system's implementation in this study.

Al-Rakhami and Al-Mashari (2021) put up a plan for utilizing a variety of IoT components to foster confidence in supply chains. They used simulations to show how their approach may be applied. Nevertheless, the technique is not validated in real-world settings, suggesting that more study is necessary to verify its efficacy in genuine supply chain contexts. Blockchain technology's potential to protect data and communication in Internet of Things-enabled wireless body area monitoring systems (WBMS) was examined by Faika et al. (2019). Through experimental trials, their proof of concept was confirmed, demonstrating the potential of blockchain to improve security. However, one major drawback of blockchain technology is its tremendous processing overhead. Subsequent investigations ought to concentrate on tackling scalability concerns and refining blockchain technology for extensive WBMS implementations.

In order to enable anonymous authentication and safe data storage for sensors in the Industrial Internet of Things (IIoT), Li et al. (2021) created a group signature system that works with blockchain. Their strategy achieved the lowest possible computational and communication costs by utilizing smart contracts and proxy re-encryption. Group signature management and re-encryption key management are still difficult, nevertheless. To increase the scalability and effectiveness of their blockchain-based cloud storage system for IIoT sensors, more study is needed.

Edge Share, a blockchain-based data-sharing system intended for edge data-sharing across heterogeneous networks, was suggested by Lu et al. in 2021. This paradigm shows promise for improving the efficiency of data sharing by lowering scheme stress and transmission latency. Despite these benefits, the two-level overlay network architecture is difficult to manage. Practical implementation issues and the Edge Share framework's scalability remained the weakness. Krichen et al. (2022) compared a blockchain-based framework to traditional approaches and assessed it against security criteria. Their study revealed enhanced security characteristics compared to conventional methods. However, it was discovered that blockchain implementations might have scaling problems. To maximize blockchain's scalability and improve its compatibility with current security systems, more study is required.

## STUDY METHODOLOGY

This study employs a qualitative method using systematic literature review to explore the synergies between blockchain and machine learning techniques to improve IoT security. The study identified relevant study papers, conference proceedings and journals from reputable sources, such as IEEE Xplore, ScienceDirect, SpringerLink and Google Scholar, published between 2019 and 2024. The chosen resources were reviewed to discern the current blockchain-based IoT security systems, machine learning-based intrusion detection systems, and hybrid

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

approaches. The literature review was conducted through thematic synthesis, in which the results were categorised under the following themes: security improvement, scalability, privacy protection and performance efficiency. This process allowed us to identify gaps in the study, limitations of current solutions and trends in this study area, which can be used to develop enhanced security frameworks for IoT systems.

## Concepts Of Blockchain Technology, Machine Learning And Deep Learning Techniques For Threat Detection And Their Limitations

Among the most prominent approaches adopted in recent study are blockchain technology, machine learning (ML), and deep learning (DL), each offering distinct capabilities for enhancing threat detection and system resilience. Blockchain provides a decentralized and tamper-resistant infrastructure for secure data management, while ML techniques enable data-driven classification and anomaly detection based on learned patterns. Deep learning further extends these capabilities by automatically extracting complex features from large datasets for more accurate detection of sophisticated attacks. However, despite their advantages, each of these technologies is associated with notable limitations such as scalability constraints, high computational requirements, data dependency, and adaptability challenges. This section therefore examines the fundamental concepts of blockchain, ML, and DL techniques in threat detection, as well as their inherent limitations within IoT security environments.

### Blockchain Technology and its Threats

Blockchain systems, despite their robustness, are susceptible to a range of vulnerabilities that can undermine their security and functionality. 51% attack is a major vulnerability in blockchain, where a malicious actor gains control of more than half of the network's mining power or stake. This control enables the attacker to manipulate the blockchain in various ways, such as reversing transactions, preventing new transactions from gaining confirmations, and double-spending coins (Abou et al., 2020). Vulnerability lies in smart contracts, which are prone to coding errors and bugs. Since smart contracts are immutable once deployed, any vulnerability in the code can be exploited by attackers, leading to significant financial losses and system breaches. Additionally, the transparency of blockchain transactions, while beneficial, can also pose privacy risks as transaction histories and patterns can be analyzed to reveal sensitive user information (Jain and Pandey, 2019).

Another critical vulnerability is the susceptibility to Sybil attacks, where a single entity creates multiple fake identities to gain disproportionate influence over the network. This can disrupt consensus mechanisms, leading to potential network partitioning and security breaches. Phishing and social engineering attacks are also prevalent in the blockchain space, where attackers deceive users into revealing their private keys or sensitive information, resulting in unauthorized access to their assets (Sundareswaran and Sasireka, 2022). Furthermore, the reliance on cryptographic algorithms poses a long-term risk, as advancements in quantum computing could potentially break these cryptographic safeguards, compromising the integrity and security of blockchain systems. These vulnerabilities highlight the importance of continuous security assessments, the adoption of advanced cryptographic techniques, and the implementation of robust network protocols to safeguard blockchain ecosystems (Panwar et al., 2021).

### Types of Blockchain Attacks

It is crucial to understand the various potential attacks that can target blockchain systems. These threats differ significantly from those faced by traditional computer networks. Attackers often focus on manipulating the consensus process to alter registry data. Figure 1 presents the several types of attacks and they are further discussed below as they can threaten blockchain integrity (Jain et al., 2021):

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

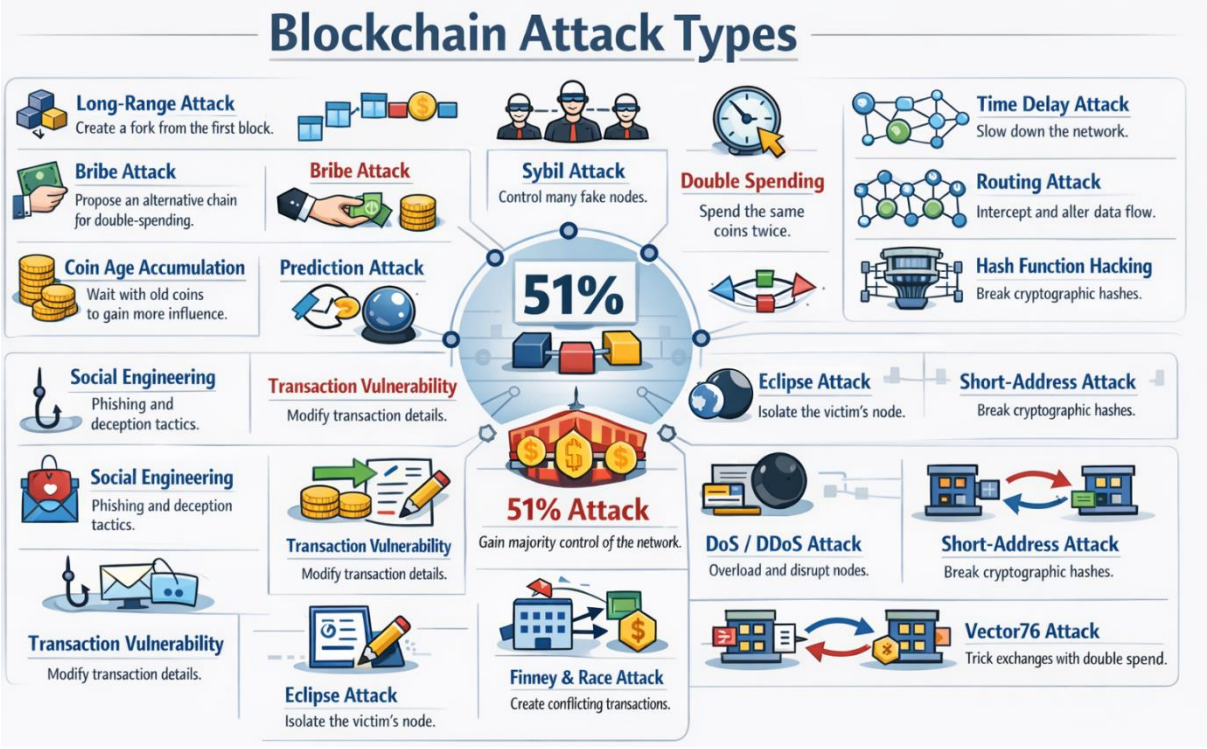


Figure 1: Blockchain Attack Types

1) **Long-Range Attack:** In a Proof of Stake (PoS) system, an attacker with significant computing power might attempt to create an alternative blockchain starting from the first block. This attack is challenging in Proof of Work (PoW) systems due to the substantial computational power required.

2) **Bribe Attack:** Attackers may try double-spending by making a payment, waiting for it to be confirmed, and then proposing an alternative blockchain that excludes the initial payment. They might offer incentives to users who support their fraudulent version of the blockchain.

3) **Coin Age Accumulation Attack:** This attack targets systems that use coin age to measure user stake. An attacker with a small percentage of total coins can wait until their coin age exceeds the average, increasing their chances of validating multiple blocks and potentially executing double-spending.

4) **Prediction Attack:** Attackers build a private chain of blocks to collect more fees and attempt double-spending. This attack is difficult in PoW and Delegated Proof of Stake (DPoS) systems due to their design, which makes precomputation challenging.

5) **Sybil Attack:** An attacker controls multiple nodes within the network, disconnecting users from the public network and connecting them only to fraudulent blocks. This isolates the users and can lead to double-spending and other malicious activities (Jain et al., 2021).

6) **Double Spending Attack:** In PoS systems, the minimal resources needed for chain formation allow attackers to attempt double-spending more easily compared to PoW systems, where substantial resources are required.

7) **DoS/DDoS Attack:** Overloading a transaction processing node with excessive data can disrupt its operations. While the Bitcoin network has some defenses against these attacks, they are becoming increasingly sophisticated.

8) **51% Attack:** If an attacker controls more than half of the network's computing power, they can manipulate the blockchain's consensus process, enabling them to reverse transactions and double spend.

9) **Time Delay Attack:** By creating a high computational load, attackers can slow down network operations, hindering data transfer, message exchanges, and block formation. This disrupts the normal functioning of the blockchain.

10) **Routing Attack:** This attack interferes with the client-provider interaction, allowing the attacker to control data flow within the network. This can isolate nodes and delay transaction propagation.

11) **Hash Function Hacking:** Advances in quantum computing could potentially compromise the robustness of current cryptographic hash functions like SHA-256 and ECDSA, threatening the security of blockchain systems.

12) **Social Engineering and Phishing Attack:** Attackers trick users into revealing sensitive information by posing as a trustworthy entity, often through email or instant messaging. This can lead to unauthorized access to user accounts and funds.

13) **Transaction Vulnerability:** Bitcoin transactions can be altered in a way that changes the transaction hash while keeping the signature valid, enabling potential fraud by modifying transaction parameters after they are signed.

14) **Transaction Flexibility:** An attacker changes the unique identifier of a Bitcoin transaction before it is confirmed, making it appear as though the transaction did not occur. This can lead to double-spending and other fraudulent activities.

15) **Eclipse Attack:** By controlling numerous IP addresses, an attacker can isolate a victim node, preventing it from seeing legitimate transactions. This isolation can be exploited for double spending and other malicious actions.

16) **Short-Address Attack:** Exploiting incorrectly padded arguments in the Ethereum Virtual Machine (EVM), attackers can redirect funds to their own addresses by sending malformed addresses to victims.

17) **Finney Attack:** An attacker pre-mines a block containing a transaction and then creates a conflicting transaction before releasing the pre-mined block, invalidating the conflicting transaction and enabling double-spending.

18) **Race Attack:** An attacker creates two conflicting transactions simultaneously, one sent to the victim and the other to the network, aiming for the victim to accept the transaction before it is invalidated, leading to double-spending.

19) **Vector76 Attack:** Combining elements of Finney and Race attacks, an attacker uses two nodes to create conflicting transactions, tricking an exchange service into confirming a high-value transaction that is later invalidated.

**Blockchain on IoT and Cyber Attacks**

The integration of blockchain technology with the Internet of Things (IoT) offers a promising approach to addressing the cybersecurity challenges that plague IoT networks. IoT devices, which range from smart home gadgets to industrial sensors, are inherently vulnerable due to their widespread distribution, limited computational resources, and often weak security protocols (Dheeraj and Gurubharan, 2018). Blockchain's decentralized and immutable ledger can enhance the security of IoT systems by providing a transparent and tamper-proof record of all transactions and interactions. This ensures that data exchanged between IoT devices can be securely authenticated and verified, reducing the risk of data tampering and unauthorized access (Wani et al., 2021).

One of the primary benefits of using blockchain in IoT is its ability to eliminate single points of failure. Traditional centralized systems are susceptible to attacks that can compromise the entire network if a central server is breached. Blockchain, on the other hand, distributes data across a network of nodes, making it

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue VII July 2026

significantly harder for attackers to alter or destroy data. This decentralized architecture enhances the resilience of IoT networks against Distributed Denial of Service (DDoS) attacks, where attackers overwhelm a system with traffic to disrupt its normal operations. With blockchain, the distributed ledger ensures continuous operation even if some nodes are compromised (Abou et al. 2020).

Moreover, blockchain's use of consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), further secures IoT networks by requiring the majority of network participants to agree on the validity of transactions. This makes it exceedingly difficult for malicious actors to manipulate the system without controlling a significant portion of the network's resources. Additionally, blockchain's cryptographic techniques ensure the integrity and confidentiality of data. Each block in the chain contains a cryptographic hash of the previous block, creating a secure linkage that prevents data alteration. This immutability is crucial for maintaining trust in the data generated and shared by IoT devices (Jain and Pandey, 2019).

However, integrating blockchain with IoT also presents several challenges. The computational requirements of blockchain, particularly in consensus mechanisms like PoW, can be demanding for IoT devices with limited processing power and energy resources. This necessitates the development of more lightweight blockchain solutions tailored for IoT environments, such as IoT-specific consensus protocols or hybrid blockchain architectures (Sundareswaran et al., 2020). Additionally, the scalability of blockchain networks remains a concern, as the increasing number of IoT devices can lead to a surge in the volume of transactions that need to be processed and recorded on the blockchain. Addressing these scalability issues is essential to ensure that blockchain can effectively support the growing IoT ecosystem (He et al., 2021).

**Artificial Neural Networks (ANNs)**

Artificial Neural Networks (ANNs) are computational models inspired by the human brain's neural networks. They consist of interconnected layers of nodes, or neurons, that process and transmit information. These networks can learn complex patterns and make predictions based on data (Nwobodo-Nzeribe, and Inyiama, 2014). ANNs are used in various applications, including image and speech recognition, natural language processing, and autonomous systems (Wani et al., 2021). The learning process in ANNs involves adjusting the weights of connections based on the error between the predicted and actual outputs, typically using algorithms like back-propagation. The versatility and power of ANNs have made them a cornerstone of modern machine learning and artificial intelligence (Inyiama and Nwobodo-Nzeribe, 2014).

**Feature Selection in ANNs**

Feature selection is a crucial step in the development of Artificial Neural Networks (ANNs). It involves identifying and selecting the most relevant features from the input data that contribute to the model's predictive performance (Faika et al., 2019). Effective feature selection can reduce the dimensionality of the data, improve model accuracy, and reduce training time. Techniques for feature selection include filter methods, wrapper methods, and embedded methods (Ibrahim et al., 2022). Filter methods use statistical techniques to assess the relevance of features independently of the learning algorithm (Dawadi et al., 2023). Wrapper methods evaluate feature subsets by training and testing the model with different combinations of features (Jain et al., 2021). Embedded methods incorporate feature selection into the model training process, such as using regularization techniques that penalize the inclusion of irrelevant features. By focusing on the most significant features, ANNs can achieve better generalization and performance on unseen data (Wani et al., 2021)..

**Optimization of ANNs**

Optimization in Artificial Neural Networks (ANNs) refers to the process of adjusting the model's parameters to minimize the error between predicted and actual outcomes (Ferrag et al., 2023; Inyiama and Nwobodo-Nzeribe, 2014). This involves selecting the appropriate learning rate, choosing the right optimization algorithm, and tuning hyperparameters (Panwar et al., 2021). Common optimization algorithms include stochastic gradient descent (SGD), Adam, RMSprop, and AdaGrad (Ma et al., 2020; Tama et al., 2019; Tuan et al., 2020). These algorithms aim to find the optimal weights of the neural network by iteratively updating them based on the gradient of the loss function (Othman et al., 2023). Hyperparameter tuning, such as adjusting the number of

hidden layers, neurons per layer, and activation functions, is also essential for optimizing ANN performance (Paul and Rao, 2022; Banafaa et al., 2022). Techniques like grid search, random search, and Bayesian optimization can be used to find the best hyperparameter settings (Ahmad et al., 2022; Dong et al., 2019). Proper optimization ensures that the ANN converges to a solution that accurately represents the underlying patterns in the data, leading to improved model performance and reliability (Jiang et al., 2023; Khan et al., 2023).

**Applications and Challenges of ANNs and Study Gap**

ANNs are widely used across various fields due to their ability to model complex, non-linear relationships as shown in Figure 2.


Figure 1: General Applications of ANN

- In healthcare, ANNs assist in disease diagnosis and drug discovery by analyzing vast amounts of medical data.
- In finance, they are used for predicting stock prices, detecting fraud, and managing risk (Mumtaz et al., 2023).
- In autonomous systems, such as self-driving cars, ANNs process sensor data to make real-time decisions.

However, ANNs also face challenges, including:

- The need for large amounts of labeled data for training, the difficulty in interpreting their decision-making processes, and
- The risk of overfitting when the model is too complex for the given data (Yin et al., 2023).
- Additionally, training ANNs can be computationally intensive, requiring significant processing power and time.

Despite these challenges, ongoing study and advancements in hardware and algorithms continue to expand the capabilities and applications of ANNs (Niranjanamurthy et al., 2019).

In the context of cybersecurity and IoT systems, recent studies such as Ruzbahani (2024) have explored the use of artificial intelligence to enhance blockchain-based IoT security frameworks. However, most of these studies primarily focus on improving data security and privacy without adequately addressing the susceptibility of blockchain-enabled IoT systems to evolving and real-time cyber-attacks. This represents a critical gap in existing study. Therefore, there is a need for an intelligent and adaptive security framework that integrates machine learning techniques with blockchain technology to enable real-time monitoring, detection, and mitigation of cyber threats in IoT environments while ensuring data confidentiality, integrity, and system reliability.

## CONCLUSION

This study has provided an overview of blockchain, ML and DL technologies used for improving security in IoT systems. It explored the vulnerabilities of IoT systems, despite their many benefits in smart homes, health care and industrial automation systems, to cyber attacks, given their distributed nature and limited resources. The paper also discussed the use of blockchain in decentralized and secure data storage, and also its drawbacks, such as scalability, computational overhead, and vulnerability to attacks like 51% attack and smart contract attacks. Furthermore, the study examined how ML and DL play a role in threat detection strategies such as pattern analysis, anomaly detection, and predictive modelling, but also highlighted their shortcomings including data dependency, high computational requirements, and limited effectiveness in combating emerging cyber threats.

Overall, the use of blockchain in combination with ML and DL offers a potential solution to enhance IoT security by providing decentralized data management together with advanced threat detection techniques. But current literature shows there are considerable gaps, especially in the development of real-time, scalable and adaptive security solutions to address dynamic cyber threats. Existing approaches are mostly concerned with data protection or detection separately, with little emphasis on holistic and real-time security frameworks. Hence, it is important to explore hybrid approaches that integrate blockchain with machine learning to design smart, efficient and scalable security solutions to provide confidentiality, integrity and reliability in IoT networks.

## ACKNOWLEDGEMENT

The authors would like to acknowledge the assistance of an artificial intelligence agent (Google Gemini, Copilot, and Anthropic) in the creation and refinement of the figures and diagrams presented in this manuscript. The AI tool helped generate initial drafts of the architectural illustrations and block diagram, which were subsequently reviewed, modified using the Microsoft PowerPoint application and approved by the authors. The authors take full responsibility for the final content and integrity of all figures.

### Language Editing Declaration

The authors used Grammarly solely to improve the grammar, spelling, punctuation, sentence clarity, and readability of the manuscript. The tool was not used to generate scientific content, interpret results, perform data analysis, or formulate the study's conclusions. The authors take full responsibility for the accuracy, originality, and integrity of the manuscript.

## REFERENCES

1. Abou El Houda, Z., Hafid, A., & Khoukhi, L. (2020, June). BrainChain, A machine learning approach for protecting blockchain applications using SDN. In 2020 IEEE International Conference on Communications (ICC) (pp. 1–6). IEEE. https://doi.org/10.1109/ICC40277.2020
2. Ahmad, T., Zhu, H., Zhang, D., Tariq, R., Bassam, A., Ullah, F., AlGhamdi, A. S., & Alshamrani, S. S. (2022). Energetics systems and artificial intelligence: Applications of Industry 4.0. Energy Reports, 8, 334–361. https://doi.org/10.1016/j.egyr.2021.11.254
3. Alajlan, R., Alhumam, N., & Frikha, M. (2023). Cybersecurity for blockchain-based IoT systems: A review. Applied Sciences, 13(7), 7432. https://doi.org/10.3390/app13137432
4. Albakri, A., Alabdullah, B., & Alhayan, F. (2023). Blockchain-assisted machine learning with hybrid metaheuristics-empowered cyber attack detection and classification model. Sustainability, 15(18), 13887. https://doi.org/10.3390/su151813887
5. Alharbi, S., Attiah, A., & Alghazzawi, D. (2022). Integrating blockchain with artificial intelligence to secure IoT networks: Future trends. Sustainability, 14(23), 16002. https://doi.org/10.3390/su142316002
6. Ali, A., Almaiah, M., Hajjej, F., Pasha, M., Fang, O., Khan, R., Teo, J., & Zakarya, M. (2022). An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network. Sensors, 22(2), 572. https://doi.org/10.3390/s22020572

7. Almaraz-Rivera, G., Perez-Diaz, J., & Cantoral-Ceballos, A. (2022). Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models. Sensors, 22(9), 3367. https://doi.org/10.3390/s22093367
8. Alohali, M. A., Elsadig, M., Al-Wesabi, F. N., Al Duhayyim, M., Hilal, A. M., & Motwakel, A. (2023). Optimal deep learning-based ransomware detection and classification in the Internet of Things environment. Computer Systems Science and Engineering, 46, 3087–3102.
9. Aresu, M., Ariu, D., Ahmadi, M., Maiorca, D., & Giacinto, G. (2015). Clustering Android malware families by HTTP traffic. In Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALWARE) (pp. 128–135). IEEE.
10. Averin, A., & Averina, O. (2019). Review of blockchain technology vulnerabilities and blockchain-system attacks. In 2019 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) (pp. 1–6). IEEE. https://doi.org/10.1109/FarEastCon.2019.8934243
11. Banafaa, M., Shayea, I., Din, J., Azmi, M. H., Alashbi, A., Daradkeh, Y. I., & Alhammadi, A. (2022). 6G mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities. Alexandria Engineering Journal, 64, 245–274. https://doi.org/10.1016/j.aej.2022.08.005
12. Bobde, Y., Narayanan, G., Jati, M., Raj, R., Cvitic, I., & Perakovic, D. (2024). Enhancing industrial IoT network security through blockchain integration. Electronics, 13(4), 687. https://doi.org/10.3390/electronics13040687
13. Cui, L., Su, X., Ming, Z., Chen, Z., Yang, S., Zhou, Y., & Xiao, W. (2020). CREAT: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing. IEEE Internet of Things Journal, 9(18), 14151–14161. https://doi.org/10.1109/JIOT.2020.3012567
14. Dawadi, B. R., Adhikari, B., & Srivastava, D. K. (2023). Deep learning technique-enabled web application firewall for detection of web attacks. Sensors, 23(7), 2073. https://doi.org/10.3390/s23042073
15. Dheeraj, J., & Gurubharan, S. (2018). DDoS mitigation using blockchain. International Journal of Research in Engineering, Science and Management, 1(10), 622–626.
16. Dong, S., & Sarem, M. (2019). DDoS attack detection method based on improved KNN in software-defined networks. IEEE Access, 8, 5039–5048. https://doi.org/10.1109/ACCESS.2019.2963318
17. Dwivedi, Y. K., et al. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges. International Journal of Information Management, 66, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542
18. Eghmazi, A., Ataei, M., Landry, R. J., & Chevrette, G. (2024). Enhancing IoT data security: Using blockchain to boost integrity and privacy. IoT, 5(1), 20–34. https://doi.org/10.3390/iot5010002
19. Ferrag, M. A., Maglaras, L., & Benbouzid, M. (2023). Blockchain and artificial intelligence as enablers of cyber security in IoT and IIoT applications. Journal of Sensor and Actuator Networks, 12(40). https://doi.org/10.3390/jsan12020040
20. Gugueoth, V., Safavat, S., Shetty, S., & Rawat, D. (2023). A review of IoT security and privacy using decentralized blockchain techniques. Computer Science Review, 50, 100585. https://doi.org/10.1016/j.cosrev.2023.100585
21. He, G., Si, Y., Xiao, X., Wei, Q., Zhu, H., & Xu, B. (2021). Preventing IoT DDoS attacks using blockchain and IP address obfuscation. In 2021 IEEE WCSP (pp. 1–5). IEEE.
22. Ibrahim, R. F., Abu Al-Haija, Q., & Ahmad, A. (2022). DDoS attack prevention for IoT devices using Ethereum blockchain technology. Sensors, 22(18), 6806. https://doi.org/10.3390/s22186806
23. Inyiama, H. C., & Nwobodo-Nzeribe, H. N. (2014). Designing intelligent process control system using fuzzy neural network. International Journal of Scientific and Engineering Research, 5(9), 1202–1220.
24. Jiang, T., Shen, G., Guo, C., Cui, Y., Xie, B. (2023). BFLS: Blockchain and federated learning for cyber threat intelligence sharing. Computer Networks, 224, 109604. https://doi.org/10.1016/j.comnet.2023.109604
25. Khan, A. A., Laghari, A. A., Li, P., et al. (2023). Blockchain, artificial intelligence, and IIoT in SMEs digitalization. Scientific Reports, 13, 1656. https://doi.org/10.1038/s41598-023-28988-2
26. Khordadpour, P., & Ahmadi, S. (2024). Security and privacy enhancing in blockchain-based IoT environments via anonym auditing. arXiv preprint arXiv:2403.01356.
27. Kotel, S., Sbiaa, F., Kamoun, R., & Hamel, L. (2023). A blockchain-based approach for secure IoT systems. Procedia Computer Science, 225, 3876–3886. https://doi.org/10.1016/j.procs.2023.10.383

28. Li, H., Dang, R., Yao, Y., & Wang, H. (2023). Approaches for detecting smart contract vulnerabilities in Web 3.0. Blockchains, 1(1), 3–18. https://doi.org/10.3390/blockchains1010002
29. Li, Z., Sun, L., Yan, Q., et al. (2016). Droidclassifier: Efficient adaptive mining for Android malware detection. In IEEE International Conference on Security and Privacy in Communication Systems.
30. Ma, Z., Zhang, J., Guo, Y., et al. (2020). Blockchain-based key management mechanism for VANET. IEEE Transactions on Vehicular Technology, 69(6), 5836–5849. https://doi.org/10.1109/TVT.2020.2975461
31. Manikumar, D., & Maheswari, B. (2020). Blockchain-based DDoS mitigation using machine learning techniques. In ICIRCA 2020 (pp. 794–800). IEEE. https://doi.org/10.1109/ICIRCA48905.2020.9183092
32. Mishra, S. (2023). Blockchain and machine learning-based hybrid IDS. Electronics, 12(16), 3524. https://doi.org/10.3390/electronics12163524
33. Mulani, U., & Patil, M. (2022). Securing IoT system access control using blockchain-based approach. International Journal of Intelligent Systems and Applications in Engineering, 10(3s), 33–39.
34. Mumtaz, G., et al. (2023). Cyber incident classification using ML techniques. IEEE Access.
35. Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. (2019). Blockchain technology analysis: Pros, cons and SWOT. Cluster Computing, 22, 14743–14757.
36. Othman, S. B., et al. (2022). Privacy-preserving IoT healthcare data aggregation. Computer & Electrical Engineering, 101, 108025.
37. Panwar, V., Sharma, D. K., Kumar, K. V. P., et al. (2021). Optimization of machining processes using GA. Materials Today: Proceedings.
38. Reddy, C. (2023). Blockchain in IoT security. Doctoral thesis, ICFAI University.
39. Ruzbahani, A. (2024). AI-protected blockchain-based IoT environments. arXiv preprint arXiv:2405.13847.
40. Singh, S., Ra, I., Meng, W., et al. (2019). SH-BlockCC smart home architecture. International Journal of Distributed Sensor Networks, 15(4). https://doi.org/10.1177/1550147719844159
41. Sodhro, A., Pirbhulal, S., Muzammal, M., & Zongwei, L. (2020). Blockchain-enabled security for IIoT systems. Journal of Grid Computing. https://doi.org/10.1007/s10723-020-09527-x
42. Toka, K., Dikilitas, Y., Oktay, T., & Sayar, A. (2021). Securing IoT with blockchain. ISPRS Archives. https://doi.org/10.5194/isprs-archives-XLVI-4-W5-2021-529-2021
43. Tuan, T. A., Long, H. V., Son, L. H., et al. (2020). Botnet detection using machine learning. Evolutionary Intelligence, 13, 283–294. https://doi.org/10.1007/s12065-019-00222-8
44. Ullah, F., et al. (2022). Cyber-threat detection using hybrid ML models. Sensors, 22(15), 5883. https://doi.org/10.3390/s22155883
45. Wani, S., Imthiyas, M., Almohamedh, H., et al. (2021). DDoS mitigation using blockchain. Symmetry, 13(2), 227. https://doi.org/10.3390/sym13020227
46. Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452–10473. https://doi.org/10.1109/JIOT.2021.3053839
47. Yin, H. L., et al. (2023). Experimental quantum secure network with digital signatures. National Science Review, 10, nwac228. https://doi.org/10.1093/nsr/nwac228