Iraqi Journal for Computers and Informatics
Available online: https://ijci.uoitc.edu.iq/index.php/ijci
Volume 52, issue 1. 2026

Print ISSN: 2313-190X, Online ISSN: 2520-4912

Innovative strategies for IoT security using AI and blockchain: a comprehensive review

Athraa Hamed Juber* [a], Baraa I. Farhan [b]
[a] *Computer Science, College of Education of Pure Science, University of Wasit, Wasit, Iraq.*
[b] *Computer Science, College of Education of Pure Science, University of Wasit, Wasit, Iraq.*

ARTICLE INFO

***Keywords**:*

Internet of Things, blockchain technology, Secure IoT, AI and Blockchain integration, Cybersecurity.

ABSTRACT

The Internet of Things (IoT) is an emerging technological revolution, where devices communicate with each other over the internet to receive communications and information. These devices generate massive amounts of information. As industries increasingly rely on IoT devices, the need for technologies to enhance data security and privacy has emerged. This data faces significant security challenges, such as cyberattacks or data tampering. Therefore, it is imperative to develop effective protection for this data. This study aims to review the role of artificial intelligence (AI) and blockchain technology in enhancing IoT security by integrating these two technologies. The combination of AI and IoT represents a tremendous revolution in the rapidly evolving field, given its ability to simplify tasks easily and efficiently. AI analyzes and classifies data, detects threats and malicious attacks, while blockchain technology provides an additional layer of protection for the IoT through decentralized storage that prevents data tampering and ensures its integrity and confidentiality. In this study, we present a structured and systematic review of research published between 2021 and 2025, focusing on the role of AI and blockchain in securing IoT data. The results demonstrate that integrating AI with blockchain technology improves IoT security by detecting attacks early, reducing vulnerabilities, and preventing unauthorized access or data tampering. However, the evolving nature of attacks and challenges calls for further research to find or develop solutions capable of addressing future challenges to ensure security and reliability in data exchange between devices

1. INTRODUCTION

The Internet of Things is a huge technological revolution and has become part of our daily lives and is included in all fields, including industrial, medical, smart cities and agriculture, where devices communicate with each other through the Internet and provide smart services. These devices generate a huge amount of information Therefore, it has become necessary to secure this data preservation infrastructure in addition, IOT devices exchange and analyze data, facilitating decision-making processes and improving efficiency in managing operations [1]. With many devices connected to the Internet, one of the biggest challenges in securing the Internet of Things is the huge number of devices and the diversity of their operating systems and protocols. Each device is a potential entry point that attackers can exploit Hacking a single device may have consequences including unauthorized access, data manipulation, lack of efficiency in early detection of hacks or cyber-attacks, and data management problems. Therefore, it is necessary to provide protection for this data to continue services without disruption or forgery [2]. Therefore, protection has become necessary, and modern technologies must be used, such as the use of artificial intelligence, which is used to know and protect this data and detect attacks launched by attackers These devices also analyze and protect this data, make decisions, detect suspicious or anomalous activities, and predict vulnerabilities, which improves security [3]. The

E-mail address:
std.2024205.a.jebur@uowasit.edu.iq [a]
bfarhan@uowasit.edu.iq [b]

Corresponding* : *Athraa Hamed Juber*

Received 15 September 2025, Accepted 10 November 2025

DOI: 10.25195/ijci.v52i1656.

other technology is blockchain, which is used to store and exchange data and information between more than one device that relies on blocks linked together using encryption. This makes the system resistant to data tampering, so it provides high security. Its goal is to make the data not subject to modification or manipulation, and it is characterized by transparency, high security, and decentralization [4]. Therefore, the integration of artificial intelligence and blockchain is one of the innovations that greatly enhances security and the efficiency of operations and data because the blockchain stores each operation permanently and transparently and prevents any manipulation or unauthorized access. Using intelligence algorithms, we analyze this data automatically to classify patterns Anomalous or suspicious information that indicates fraud or attacks. In addition, the benefit of the merger is to enhance trust and transparency between the parties and ensure continuous data protection and early detection of threats in real time [5] Although previous studies have dealt with securing the Internet of Things using blockchain or intelligence separately, there are major challenges facing it and there is a lack of research that integrates both technologies to enhance security, this study aims to:

1- Review previous studies that addressed integrating AI and blockchain technologies in securing the Internet of Things (IoT) and compare their performance with traditional methods.
2- Explore how to integrate both technologies to provide a secure and integrated IoT system.
3- Compare the types of data used to secure the Internet of Things (IoT).

Section Two: Introduction to the Internet of Things (IoT), security challenges, and common This study is organized as follows: Section Three: Blockchain technology and its characteristics, Section Four: Integrating blockchain with the Internet of ,attacks Things, Section Five: Artificial intelligence (AI), its types, and applications in cybersecurity, Section Six: Integrating AI with blockchain to enhance IoT security, Section Seven: Conclusions and future recommendations

2. The Internet of Things

The Internet of Things is considered a more advanced technology and this technology is constantly developing the Internet [6]. Different physical devices are connected to the Internet and can communicate and exchange information between them [7]. The Internet of Things industry needs to keep pace with the security standard and institutions must include security in Internet devices [8] and contain large quantities of data that must be protected from electronic attacks [9]. It is exposed to a group of cyber-attacks, including violations Data, the network, its hacking, and many other attacks that exploit security vulnerabilities inside devices [10]. The Internet of Things integrates software, interfaces, protocols, and data flow [11]. The Internet of Things consists of several interconnected layers, perception, network, application these layers are illustrated in figure 1

1.Perception layer: Also called the physical layer, it consists of sensors and its goal is to collect data and transfer it to the network layer

2.Network layer: It is also known as the transport layer and its function is to transport and process data. It is characterized by the presence of gateways

3.Application layer: The customer receives the requested service and it contains the user interface, and its importance lies in providing services and ensuring confidentiality, integrity, and data availability [12].

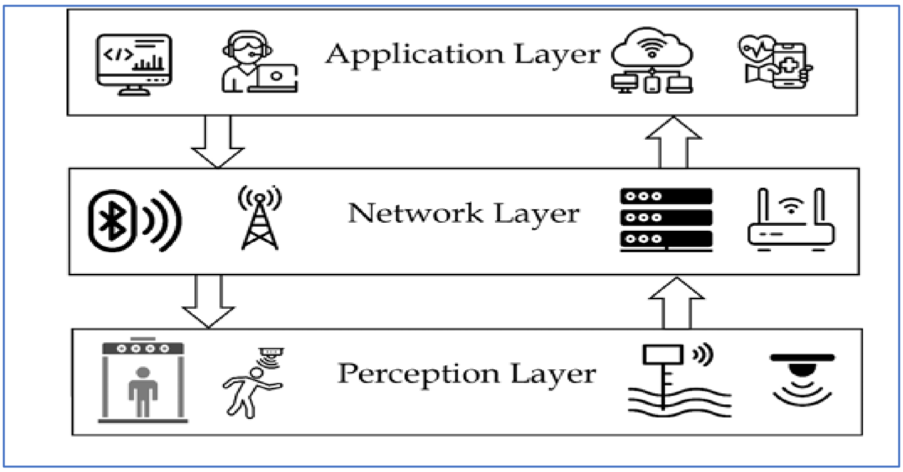

Fig 1. Three-layer architecture: perception layer, network layer, and application layer. [13]

2.1Challenges of the Internet of Things

Internet of Things systems need protection for integration Availability and confidentiality. There are several challenges that hinder its spread and adoption. The most prominent of these challenges is the absence of unified protocols, which reduces the ability of different devices to communicate, disconnection, and lack of continuity of service due to a weak network or the device is unable to work properly. This reduces the reliability of the system as well as scalability. The more devices there are, the more problems they may face, limited power and batteries. Most devices are small and their batteries are weak and limited and cannot run large programs as well as managing big data, because devices generate a lot of data, and analyzing and storing it requires special resources and software [14]. There are also challenges at the level of devices, data, or networks, and they include a group of vulnerabilities that must be addressed.

A. Hardware Challenges

1- Securing devices from theft attempts or unauthorized access.
2- Weaknesses in the code or the presence of vulnerabilities that attackers can exploit.
3- Verification and authentication, which means applying strong authentication methods such as two-step verification to verify the identity of the user or device and detect weak points [15].

B. Network Level Challenges

1- Securing data during its transmission over the network to ensure confidentiality and data integrity using secure communication protocols.
2- Use of intrusion detection systems. Configure the firewall to protect against denial-of-service attacks [16].

C. Data Level

1- Protect data from unauthorized access by encryption to convert data from plain text to incomprehensible text to maintain data confidentiality.
2- Ensuring that data remains complete, accurate, integrated and reliable during the creation, storage, transportation and processing stages to prevent tampering and maintain its confidentiality.
3- Store and transfer data securely to protect it from hacking and malicious attacks [17][18].

2.2. Attacks on the Internet of Things

IoT systems face significant cyber security challenges due to their distributed nature and the large number of connected devices. In this section, these attacks can be classified into six main categories, as shown in Figure 2. The most prominent attacks targeting the IoT will be reviewed: hardware attacks (shown in Table 1), cloud attacks (shown in Table 2), application attacks (shown in Table 3), data attacks (shown in Table 4), software attacks (shown in Table 5), and network attacks (shown in Table 6).

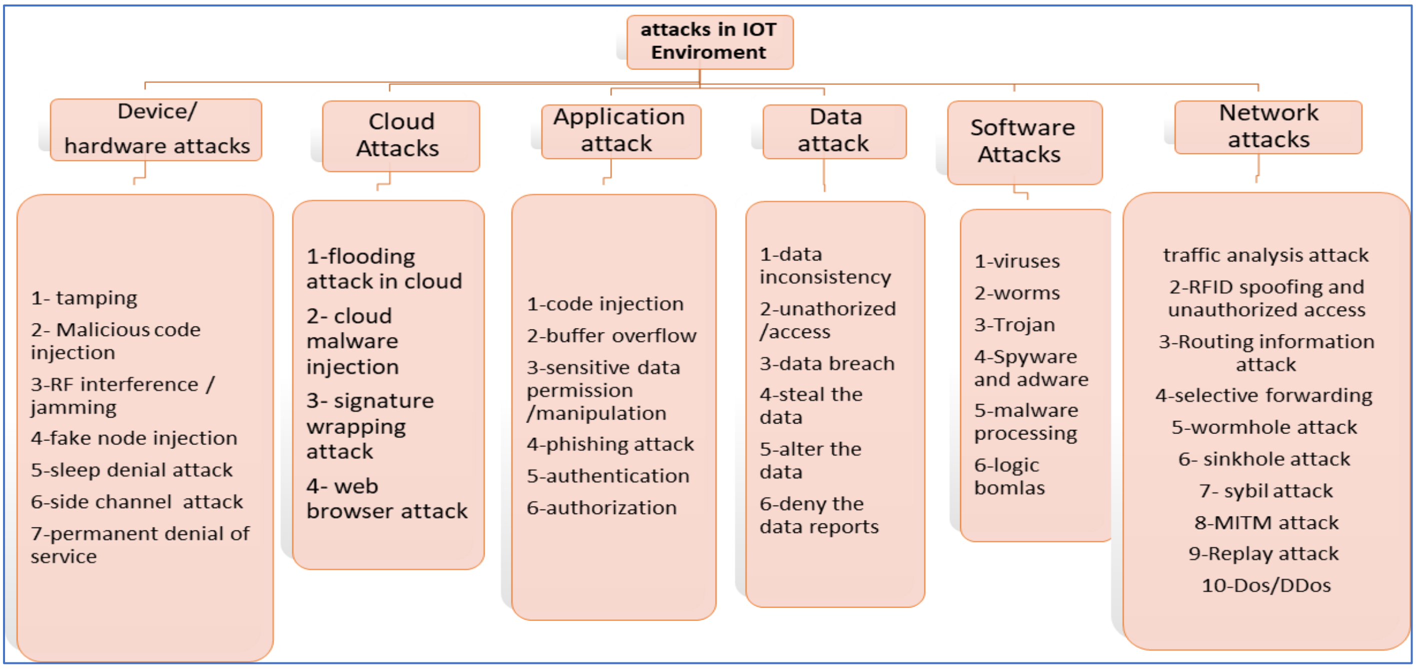

Fig. 2. The classification of (IoT) attacks illustrates the different types and categories of security threats.

1-Device / Hardware Attacks

Hardware attacks are among the most prominent attacks that affect Internet of Things devices. Table 1 shows the most important of these attacks

Table 1: Types of hardware attacks on IoT devices and corresponding defense mechanisms

Ref	Attack	Description	Outcome	Defense
[19]	Tampering	Physically altering IoT devices or connections	DFID tampering hardware manipulation	Use tamper -resistant hardware physical protection mechanisms
[19]	Malicious code injection	Injection harmful code into physical devices	Device compromise foothold for further attacks	Firmware validation secure boot mechanisms
[20]	RF interference /jamming	Noise signals disrupt WSN and RFID communication	Dos attacks connectivity loss	Spread spectrum techniques

[20]	Fake node injection	Insertion of fake nodes between real ones	Manipulated data flow	Node authentication, trust management systems
[21]	Sleep denial attack	Keeps battery-powered devices awake	Battery drains reduced lifespan	Rate limiting, energy-efficient protocols
[22]	Side-channel attack	Exploiting timing, power, or fault info to extract keys	Decryption of sensitive data	Hardware shielding, noise injection, secure cryptographic
[23]	Permanent Dos (P DoS)	Corrupting BIOS/firmware with malware	Device permanently disabled	Firmware integrity checks secure updates

2-Cloud Attacks

It is one of the most prominent security threats to IoT, as it targets storage services and cloud applications and affects data confidentiality. Table 2 shows the most important of these attacks

Table 2: Types of Cloud Attacks hardware attacks on IoT system and corresponding defense mechanisms

Ref	Attack	Description	outcome	Defense
[24]	Flooding Attack	SYN requests overload server. resources	Resource exhaustion, Dos	SYN cache, SYN cookies
[25]	Cloud Malware Injection	Malicious VMs or apps injected into cloud	Service compromise, data unavailability	Hash verification, service instance validation
[26]	Signature Wrapping Attack	SOAP/XML signature manipulation	Data integrity compromise	WS-Security policy enforcement Content
[27]	Web Browser Attack (XSS)	Injecting malicious scripts via websites	Data leakage, unauthorized actions	Content filtering, vulnerability detection tools

3- Application attack

It is one of the most prominent security threats to the Internet of Things, exploiting vulnerabilities in applications to affect performance. Table 3 shows the most important of these attacks

Table 3: Types of applications - level attacks in IoT systems and corresponding defense mechanisms

Ref	**Attacks**	**Description**	**Outcome**	**Defense**
[26]	Injection	Malicious code inserted via programming flaws	Data theft, malware spread	Input validation, secure coding practices
[28]	Buffer Overflow	Memory overflows exploited	Code execution, data corruption	Bounds checking. memory-safe languages
[29]	Unauthorized Access to Data	Exploiting weak authorization models	Sensitive data theft, manipulation	Fine-grained access control, role-based authorization
[27]	Phishing	Masquerading as legitimate users/orgs	Credential theft, data breach	Email filtering, user awareness training
[27]	Authentication&Authorization Weakness	Over-privilege, weak auth methods	Device compromise, unauthorized control	Multi-factor authentication, proper privilege management

4 -Data attack

It is one of the most prominent security threats to the Internet of Things, threatening data confidentiality. Table 4 shows the most important of these attacks

Table 4: Types of Data - Level Attacks in IoT Systems and Corresponding Defense Mechanisms

Ref	Attack	Description	Outcome	Defense
[30]	Data Inconsistency	Corruption of stored/in-transit data	System failures, wrong decisions	Data validation, redundancy checks
[31]	Unauthorized Access	Illegal access to sensitive info	Data theft, manipulation	Access control, encryption
[32]	Data Breach	Illegal use of private data	Privacy violations, leaks	Encryption, monitoring
[33]	Data Theft	Unauthorized acquisition of sensitive data	Financial loss, identity theft	Strong authentication, endpoint protection

[33]	Data Alteration	Tampering with data during transmission	Manipulated outputs, malicious code injection	Encryption, integrity checks
[34]	Deny Data Reports	Restricting access to reports	System unavailability, incomplete data	Role-based access, monitoring

5- Software Attacks

It is one of the most prominent security threats to the Internet of Things, targeting operating systems and software and affecting data. Table 5 shows the most important of these attacks

Table 5: Types of software attacks on IoT devices and corresponding defense mechanisms

Ref	Attack	Description	Outcome	Defense
[19]	Viruses	Malicious software alters system	DoS/DDoS, Data theft	Antivirus, patch management
[19]	Worms	Worms Self-propagating programs	Device compromise, Botnet formation	Network monitoring, anomaly detection
[35] [36]	Trojan Horses	Hidden malware like Mirai	Botnet creation, DDoS	Firmware updates, malware detection
[19]	Spyware	Secret monitoring of users	Data theft, surveillance	Anti-spyware tools, secure software policies
[19]	Adware	Malicious ads and unwanted installations	System slowdown, unwanted access	Ad-blocking, malware prevention
[19]	Malware	General malicious	Data compromise	Endpoint protection
[19]	Logic Bomb	Hidden code triggered under conditions	Data deletion, sabotage	Code review, insider threat monitoring

6- Network attacks

It is one of the most prominent security threats to the Internet of Things, targeting communication between devices and affecting data availability. Table 6 shows the most important of these attacks

Table 6: Types of network attacks on IoT devices and corresponding defense mechanisms

Ref	Attack	Description	Outcome	Defense
[37]	Traffic Analysis	Sniffing data in transit	Sensitive data leakage	Encryption, traffic padding
[38]	RFID Spoofing	Forging RFID signals	Impersonation, data theft	Mutual authentication, cryptographic protection
[38]	RFID Unauthorized Access	Illegal RFID data access	Identity theft, fraud	Access control, secure RFID protocols
[39]	Routing Information Attack	Forging/modifying routing info	Network disruption	Secure routing protocols, authentication
[40]	Selective Forwarding	Dropping/altering selected packets	Data loss, delays	Multipath routing intrusion detection
[41]	Sinkhole Attack	Compromised node attracts traffic	Traffic manipulation	Node trust verification, anomaly detection
[42]	Wormhole Attack	Tunneling packets across network	Eavesdropping. disruption	Packet leashes. distance bounding
[43]	Sybil Attack	Node uses multiple fake identities	Resource exhaustion	Identity verification. trust management
[44]	MITM Attack	Intercepting device communications	Data theft. manipulation	Encryption. session key exchange
[45]	Replay Attack	Reusing captured valid	Dos/DDoS, fraud	Timestamps nonce-

		messages		based authentication
[46]	Dos/DDoS	Over whelming target with traffic	Service unavailability	Rate Limiting anomaly detection

2.3.Challenges and Attacks IoT: A Critical Analysis

By reviewing Tables 1-6, which explain the types of attacks in the Internet of Things environment and the payment mechanisms for them, it can be said that DDoS/DoS and MITM network attacks represent the most influential and dangerous attacks on network reliability and service availability, and they are also the most common in the Internet of Things [47], while software attacks (Logic Bombs, code injection) threatens the confidentiality and integrity of data, especially when activated in circumstances that are difficult to detect early [48]. Attacks on physical devices and side attacks are also less common, but they cause significant damage when successful [49]. New studies confirm the importance of protecting data from tampering or leakage, as this protection is important and essential to ensure the continuity of service in Internet of Things environments [50]. Based on the above observations, it is clear that securing the Internet of Things requires an integrated security approach that combines network protection, data, software, supported by intelligence and blockchain technologies to ensure comprehensive security for practical work environments [51]

3. Blockchain

It is difficult to find a unified definition of blockchain, so some may define it as a decentralized programming system that allows transactions to be tracked and recorded without the need for a central authority in addition, it relies on algorithms and mechanisms, including (pos)(pow), to ensure that data is not tampered with and to achieve compatibility. The blockchain is characterized by security, transparency, and non-tampering. It is also known as a database characterized by low cost and transparency [52]. It is also known as a decentralized ledger used in Bitcoin transactions that are linked to each other via hashing, as it consists of a chain of blocks [53]. It has the following characteristics:

A. Transparency: All recorded transactions can be verified and accessed by anyone, meaning that nothing can be changed or tampered with without everyone's knowledge

B. Security: One of the important and basic characteristics because it relies on consensus and encryption techniques to maintain the integrity of transactions

C. Non-tampering: Also known as stability, this property is achieved by linking blocks together with encryption to ensure that any change in one block will affect all blocks and be detected

D. Decentralization: Work is done without a central authority and decisions are made by several participants, thus reducing points of failure and enhancing security and trust [54].

3.1 Types of Blockchain

Blockchain can be classified into four main types according to its operating nature and usage scenario) see figure3)

1. **Public Blockchain**: An open system that allows any online user to join and participate in verifying transactions and prevents tampering with records. Its most prominent applications are Bitcoin and Litecoin.
2. **Private**: A closed, single-party network where permissions and accessibility are limited is used in applications such as voting and supply chain management.
3. **Consortium:** Managed by semi-centrally organized organizations and used in sectors such as banks and government agencies .
4. **Hybrid**: Combines public and private, where some data can be restricted to a private network and published to a public network for verification and increased transparency [55][56].

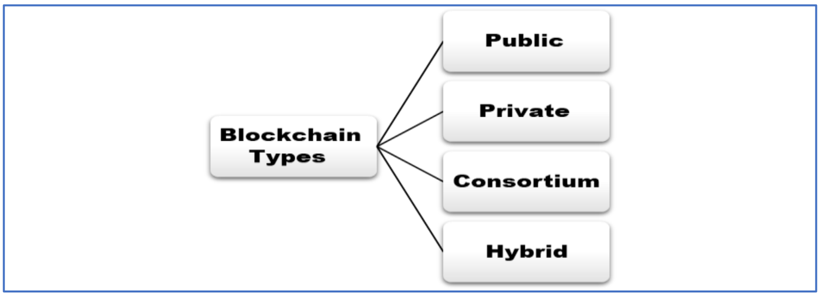

Fig.3. Types of Blockchains, showing Public, Private, and Consortium Blockchains

3.2 Integrating Blockchain with the Internet of Things

Blockchain is one of the most prominent and important solutions for the security of the Internet of Things because it secures the network, improves transaction speed, reduces device authentication costs, data integrity, and ensures privacy. It will reduce the risk of cyber-attacks and relies on its decentralization, non-manipulation or change, and transparency, all of which contribute to enhancing security. Blockchain is an effective solution against security threats, eliminates points of failure, and protects big data using continuous updates, encryption, and traceability by following up on everything Easily transact and verify its data, ensuring easy access to data. Most Internet of Things devices communicate with each other automatically and can be expanded and secured via blockchain [57][58]

4.Artificial Intelligence

In this section, we provide an overview of artificial intelligence, which is a branch of computer science that aims to build systems capable of displaying intelligence similar to humans. The possibility of intelligence is to reduce the need for human intervention in the work environment and increase efficiency. Artificial intelligence technologies include big data analysis, threat detection, decision-making, and natural language processing. Intelligence is an advanced field, and its features also include the ability to detect zero-sum attacks and analyze patterns Adapting to changes in the network [59].

1.4 Learning Mechanisms in Artificial Intelligence

A-Machine learning: It uses a statistical method that enables machines to learn and improve without the need for programming. It is used for classification, detection, and prediction[60]. Machine learning is divided into 4 sections

1 -**Supervised learning**: The model learns from parameter data containing rollers and outputs. The goal of this type is to teach the algorithm to discover the relationship between them to predict new results [61].
2 **- Unsupervised**: It does not require parameterized or classified data that trains the algorithm to detect B patterns in the same data.
3 -**Semi-supervised**: It combines the previous two types by using classified and unclassified data to train the model on data classified in small quantities and unclassified in larger quantities to reduce the cost of classifying and improve the accuracy of the model [62].
4 -**Reinforcement learning**: This type of learning learns from experience and error and does not know the previous results. The programmer learns through experience and receives feedback, such as rewards or punishments for his work, in order to update and improve his work and obtain better results. He does not need classified data, but rather learns from his direct interaction with his work environment [63][64].
As mentioned above, machine learning can be classified into several types. The main types of machine learning algorithms are summarized in **Table** 7

Table 7 Machine Learning Algorithm Classifications

Classification	Algorithm	Description / How it Works
Supervised Learning [65]	Linear Regression - Logistic Regression - -Decision Trees - Random Forest - Support Vector Machine (SVM) - Naive Bayes - k-Nearest Neighbors (KNN) -	Predict continuous values e.g. house prices - non-spam emails.Binary classification, e.g., spam vs - Create tree-like models for classification or prediction - Combine multiple decision trees to improve accuracy and reduce - overfitting -Find the best separation boundary between classes - theorem'Classify data based on Bayes - -Classify data based on closest Ask anything -
UN Supervised Learning [65]	K-Means - Analysis (PCA) Principal Component - Hierarchical Clustering - Generative Adversarial Networks (GANs -	Cluster data into groups based on similarity - Reduce dimensionality while preserving variance - Create hierarchical clusters forming a tree structure - Neural networks that generate new data samples -
Semi Supervised [66]	Self-Training - Co-Training - Graph-Based SSL - Semi-Supervised SVM(S3VM) -	Use small labeled data + large unlabeled data to iteratively improve - model Train two models on different feature sets and label unlabeled data - collaboratively .Construct a graph from labeled and unlabeled data to propagate label - Extend SVM to leverage unlabeled data for better classification -

Reinforcement Learning [67]	Q-Learning - Deep Q-Networks (DQN) - Alpha Dev -	Learn optimal policies via rewards in an environment - Combine deep neural networks with Q-Learning for improved - performance Discover faster sorting algorithms using deep reinforcement learning -

B-Deep learning: It is an advanced and sophisticated branch of machine learning that uses multi-layer neural networks, processes big data, detects advanced attacks, learns from data without the need to extract features, is used in language processing and speech recognition, and is also divided into four types, such as machine learning. Deep learning techniques can create direct communication between devices, the Internet, and things without the need for humans, which allows them to communicate and work together [68][69].

1. Supervised learning
2. Unsupervised learning
3. Semi- supervised learning
4. Deep reinforcement

As mentioned above, deep learning includes several techniques. The main types of deep learning algorithms are summarized in Table 8

Table 8 Deep learning classifications

Category	algorithm	Main functions
Supervised [70]	- CNN - DNN - RNN - LSTM	- A network for recognizing patterns in images or spatial data that uses convolution layers to extract features and bowling to reduce dimensions - A deep neural network for prediction or classification by learning the relationships between inputs and outputs - Network for processing sequential data - Solves fading and bursting problems in gradients suitable for predicting time series and texts
Unsupervised [71]	- DBN - RBM - Deep Autoencoders	- A multi-layer network that learns the probability distribution of data incrementally and is used to detect patterns without supervision - Dimensionality reduction and data organization - Learning a compact representation of data by reconstructing inputs is used to discover patterns or extract features without labeled data
Semi supervised [72]	- GAN	- It consists of two networks: a generator to generate fake data and a discriminator to distinguish real data from fake data. The goal is to improve the generator so that it is difficult for the discriminator to distinguish between them, and through this he produces new, realistic data
Deep reinforcement [73]	- Deep Q-Networks (DQN) - Policy Gradient - Actor-Critic	- Approximating the value function using a neural network to choose the best action in each case to maximize the reward in the long run - Learn a policy directly by modifying neural network parameters to maximize the expected reward - Actor selects actions Critic estimates the reward for each action, which increases learning stability in reinforcement learning environments

4.2 The Role of Artificial Intelligence in Securing the Internet of Things

Intelligence plays an important role in securing the Internet of Things devices because the Internet of Things is a widespread model that connects devices and things to the Internet to provide efficient and new services and will generate huge data. This data needs to be secured and analyzed. The role of intelligence comes using its techniques, including machine or deep learning. Through this, the concept of (AIOT) appeared. Here comes the role of intelligence in detecting attacks and anomalies and predicting potential threats and mitigating them without the need for humans [74]. Intelligence can To manage security solutions by relying on the SOC pattern and vulnerability results to ensure a security approach to confront cyber-attacks and ensure the safety and confidentiality of data during its transmission over networks. Intelligence contributes to improving security by using deep learning and natural language processing and significantly reduces human errors and speeds up its response time [75]. However, it also faces challenges, including data collection and storage, because data is large and spread in many places, making it difficult to manage and time Responding because intelligence needs time to process data in systems that need immediate decisions. This causes serious slowness, weak processing, and network congestion because millions of devices send their data and the network will slow down. This is why the need arose to integrate with the blockchain [76].

4. 3 Integrating Artificial Intelligence and Blockchain to Secure the Internet of Things

With the rapid expansion of the use of the Internet of Things in various sectors such as health, smart agriculture, cities and many others, the security of these devices and the data they contain has become important. However, some intelligence systems rely on central data processing, which is why they are vulnerable to hacking and manipulation. Therefore, it is necessary to integrate artificial intelligence and blockchain technologies. It is a powerful and effective solution to address many of the challenges facing Internet of Things systems. It allows the integration of AI and blockchain Taking advantage of the features of each of them: While intelligence needs reliable data to make accurate decisions, blockchain ensures the security and transparency of this data without the need for a central authority, blockchain stores this data in a secure and reliable manner, and intelligence collects and analyzes data. These two technologies help build safer and more reliable IoT systems, enhance transparency, and reduce dependence on the intermediary [77] [78].

4.4 Comparative analysis of AI, Blockchain, and integration approaches

Table 9 shows a comparison between discrete artificial intelligence and discrete blockchain and the approach to integrating them based on real-life cases and confirmed performance measures from previous studies. The table shows the benefits and limitations of each approach, showing that integration improves accuracy and security, despite increased complexity and latency compared to each technology individually.

Table 9: Comparison of AI, blockchain, and embedded systems in terms of performance and challenges

ref	Category	Application Scenario	Performance Results/Metrics	Main Advantage	Challenges
[79]	AI only	Medical decision support	Accuracy=%85.7 Sensitivity=%86.3 Specificity=85.7%	Fast analysis and intelligent decision support	Nature of the black box" and limited interpretability
[80]	Blockchain only	Public Blockchain networks	Performance constraints, limited TPS, transaction delays	High security and transparency	Scalability limitations and high latency
[81]	Integrated AI + Blockchain	Cyber-attack detection	Accuracy improved from 85.2%to 93.4% with AI +Blockchain integration	Combines AI accuracy, blockchain security, and traceability	Higher complexity and latency compared to AI alone

5 . Conclusion

The Internet of Things (IoT) faces numerous security challenges and risks, as threats can negatively impact systems and the quality of associated services. Therefore, robust mechanisms are needed to ensure security, privacy, and reliability. Integrating AI with blockchain technology offers a promising approach, as AI analyzes big data and makes decisions, while blockchain technology ensures data integrity and transparency in a decentralized manner. This review highlights recent studies on the integration of blockchain and AI to enhance IoT security and encourages researchers to explore new strategies to leverage these technologies and improve the performance and security of smart applications.

REFERENCES

[1] M. Katib and M. Ragab, “Blockchain Assisted Hybrid Harris Hawks Optimization Based Deep DDoS Attack Detection in the IoT Environment,” Mathematics, vol. 11, no. 8, p. 1887, Apr. 2023. DOI: 10.3390/math11081887.

[2] M. A. Al Kabir, W. Elmedany, and M. S. Sharif, “Securing IoT devices against emerging security threats: Challenges and mitigation techniques,” *Journal of Cyber Security Technology*, vol. 7, no. 4, pp. 199–223, 2023, Doi: 10.1080/23742917.2023.2228053

[3] N. M. M. Said, S. M. Ali, N. Shaik, K. M. J. Begum, A. A. A. E. Shaban, and B. E. Samuel, “Analysis of Internet of Things to Enhance Security Using Artificial Intelligence Based Algorithm,” Journal of Internet Services and Information Security, vol. 14, no. 4, pp. 590–604, Nov. 2024. DOI: 10.58346/JISIS. 2024.I4.037

[4] P. Thatcherite and A. Thatcherite, “Zero Trust Block: Enhancing Security, Privacy, and Interoperability of Sensitive Data through Zero Trust Permissioned Blockchain,” Big Data and Cognitive Computing, vol. 7, no. 4, p. 165, Dec. 2023. DOI: 10.3390/bdcc7040165

[5] N. El Akrami, M. Hanine, E. S. Flores, D. G. Aray, and I. Ashraf, “Unleashing the Potential of Blockchain and Machine Learning: Insights and Emerging Trends from Bibliometric Analysis,” IEEE Access, vol. 11, pp. 78879 78903, 2023. DOI: 10.1109/ACCESS.2023.3298371

[6] J. Chen, S. Xu, K. Liu, S. Yao, X. Luo, and H. Wu, “Intelligent Transportation Logistics Optimal Warehouse Location Method Based on Internet of Things and Blockchain Technology,” Sensors, vol. 22, no. 4, p. 1544, 2022. DOI: 10.3390/s22041544

[7] N. L. Rane, S. P. Choudhary, and J. Rane, “Artificial Intelligence (AI), Internet of Things (IoT), and blockchain powered chatbots for improved customer satisfaction, experience, and loyalty,” International Journal of Blockchain Technology and Applications, vol. 3, no. 1, pp. 7 23, Feb. 2025. DOI: 10.18178/IJBTA.2025.3.1.7 23

[8] K. Gloss, “6 IoT Security Layers to Shape the Ultimate Defense Strategy,” TechTarget, 2021. [Online]. Available: https://www.techtarget.com/iotagenda/tip/6-IoT-security-layers-to-shape-the-ultimate-defense-strategy. [Accessed: May 9, 2023]

[9] K. Al Hwaitat, M. A. Almaiah, A. Ali, S. Al Otaibi, R. Shishakly, A. Lutfi, and M. Alrawad, “A new blockchain-based authentication framework for secure IoT networks,” Electronics, vol. 12, p. 3618, 2023. DOI: 10.3390/electronics12213618

[10] R. Mohammadi Ruzbahani, “AI Protected Blockchain based IoT Environments: Harnessing the Future of Network Security and Privacy,” M.S. thesis, University of Calgary. [Online]. Available: https://arxiv.org/abs/2405.13847

[11] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, “Addressing security and privacy issues of IoT using blockchain technology,” IEEE Internet of Things Journal, vol. 8, pp. 881 888, 2020. DOI: 10.1109/JIOT.2020.2967394

[12] S. A. Ansar, S. Saxena, S. Arya, et al., “Security in IoT Layers: Emerging Challenges with Countermeasures,” in Lecture Notes in Networks and Systems, Springer, Apr. 2023. DOI: 10.1007/978 981 19 7892 0_44

[13] N. W. Khan, M. S. Alshehri, M. A. Khan, S. Almakdi, N. Moradpoor, A. Alazeb, S. Ullah, N. Naz, and J. Ahmad, “A hybrid deep learning based intrusion detection system for IoT networks,” Mathematical Biosciences and Engineering (MBE), vol. 20, no. 8, pp. 13491 13520, Jun. 2023. DOI: 10.3934/mbe.2023602

[14] S. A. Laghari, H. Li, A. A. Khan, Y. Shoulin, S. Karim, and M. A. Kaim Khani, “Internet of Things (IoT) applications security trends and challenges,” Discover Internet of Things, vol. 4, no. 1, p. 36, Dec. 2024. DOI: 10.1007/s43926 024 00090 5

[15] M. Golec, S. S. Gill, R. Bahsoon, and O. Rana, “BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and Industry 4.0,” IEEE Consumer Electronics Magazine, vol. 11, no. 2, pp. 51 56, Mar. 2022. DOI: 10.1109/MCE.2022.3151477

[16] J. Atutxa, J. Astorga, M. Barcelo, A. Urbieta, and E. Jacob, “Improving efficiency and security of IIoT communications using in network validation of server certificate,” Computers in Industry, vol. 144, Jan. 2023, Art. no. 103802. DOI: 10.1016/j.compind.2022.103802

[17] M. R. Alagheband and A. Mashatan, “Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT: Taxonomy, capabilities, and objectives,” Internet of Things, vol. 18, May 2022, Art. no. 100492. DOI: 10.1016/j.iot.2022.100492

[18] U. Farooq, M. Asim, N. Tariq, T. Baker, and A. I. Awad, “Multi mobile agent trust framework for mitigating internal attacks and augmenting RPL security,” Sensors, vol. 22, no. 12, p. 4539, Jun. 2022. DOI: 10.3390/s22124539

[19] S. S. Sivaraju, V. Mani, A. Umaamaheshvari, P. D. Banu, T. Anuradha, and S. Srithar, “An attack resistant physical unclonable function smart optical sensors for Internet of Things for secure remote sensing,” Measurement: Sensors, vol. 29, Oct. 2023, Art. no. 100882. DOI: 10.1016/j.measen.2023.100882

[20] E. Hammad and A. Farraj, “A physical layer security approach for IoT against jamming interference attacks,” in Proc. IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Sep. 2021, pp. 1 6. DOI: 10.1109/CCECE52104.2021.9588750

[21] R. R. Jenifer and V. S. J. Prakash, “Detecting denial of sleep attacks by analysis of wireless sensor networks and the Internet of Things,” The Scientific Temper, vol. 14, no. 4, pp. 1412 1418, Dec. 2023. DOI: 10.58414/SCIENTIFICTEMPER.2023.14.4.52 scientifictemper.com+1

[22] J. Woo, D. Seo, Y.-S. Kim, N. Lee, Y. Cassuto, and Y. Kim, “Mutual Information Minimization for Side Channel Attack Resistance via Optimal Noise Injection,” arXiv preprint arXiv:2504.20556, Apr. 2025. [Online]. Available: https://arxiv.org/abs/2504.20556

[23] S. Abaimov, “Understanding and Classifying Permanent Denial of Service Attacks,” Journal of Cybersecurity and Privacy, vol. 4, no. 2, pp. 324 339, May 2024. DOI: 10.3390/jcp4020016

[24] N. Singh, R. Buyya, and H. Kim, “Securing Cloud Based Internet of Things: Challenges and Mitigations,” Sensors, vol. 25, no. 1, Art. no. 79, Jan. 2025. DOI: 10.3390/s25010079

[25] T. Gaber, A. El Ghamry, and A. E. Hassanien, “Injection attack detection using machine learning for smart IoT applications,” Physics and Communication, vol. 52, Jun. 2022, Art. no. 101685

[26] S. K. Sahu, “Exploring security threats and solution techniques for IoT,” Frontiers in Artificial Intelligence, vol. 7, Art. no. 1397480, May 2024. DOI: 10.3389/frai.2024.1397480

[27] J. S. Yalli, “Authentication schemes for Internet of Things (IoT) networks,” ScienceDirect, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2542660524004104

[28] M. Youssef, M. Abdelrazek, and C. Karmakar, “Use of ensemble learning to detect buffer overflow exploitation,” IEEE Access, vol. 11, pp. 52009–52025, 2023. DOI: 10.1109/ACCESS.2023.3279280

[29] M. You, “An adaptive machine learning framework for access control decision making,” M.S. thesis, Inst. Sustain. Ind. Liveable Cities, Victoria Univ., Melbourne, VIC, Australia, 2022. [Online]. Available: https://vuir.vu.edu.au/43688/

[30] Y. Jiang, J. Liu, Z. Li, and X. Zhang, “Evaluating the data inconsistency of open source IoT platforms: A case study,” in Proc. 2021 IEEE Int. Conf. Ind. Internet (ICII), 2021, pp. 1–8. DOI: 10.1109/ICII52235.2021.00010

[31] M. Aljabri, A. A. Alahmadi, R. M. A. Mohammad, F. Alhaidari, M. Aboulnour, D. M. Alomari, and S. Mirza, “Machine learning based detection for unauthorized access to IoT devices,” J. Sens. Actuator Netw., vol. 12, no. 2, p. 27, Mar. 2023. DOI: 10.3390/jsan12020027

[32] Y. Duan, Q. Zhou, K. Nguyen, and I. Ha, “Privacy protection for smart IoT devices: A privacy preserving scheme using edge computing,” IEEE Internet of Things Journal, vol. 9, no. 3, pp. 1446–1456, Feb. 2022. DOI: 10.1109/JIOT.2021.3132172

[33] S. Ruj, J. Stankovic, and A. Nayak, “Privacy preserving data aggregation in IoT based smart metering,” Computer Communications, vol. 172, pp. 131–144, Apr. 2021. DOI: 10.1016/j.comcom.2021.01.006

[34] X. Liu, J. Wang, and H. Zhang, “Access control and availability in secure IoT systems: A blockchain enabled approach,” IEEE Internet of Things Journal, vol. 10, no. 7, pp. 6125–6138, Apr. 2023. DOI: 10.1109/JIOT.2022.3225678

[35] H. Kanaker, N. AbdelKarim, S. A. B. Awwad, N. H. A. Ismail, J. Zraqou, and A. M. F. Al Ali, “Trojan horse infection detection in cloud-based environment using machine learning,” Int. J. Interact. Mobile Technol. (iJIM), vol. 16, no. 24, pp. 81–106, Dec. 2022. DOI: 10.3991/ijim. v16i24.35763

[36] M. Sulaiman, A. Khan, A. Negash Ali, G. Laouini, and F. Sameer Alshammari, “Quantitative analysis of worm transmission and insider risks in air gapped networking using a novel machine learning approach,” IEEE Access, vol. 11, pp. 111034–111052, 2023. DOI: 10.1109/ACCESS.2023.3289567

[37] N. Malek Ghaïni, E. Akbari, M. A. Salahuddin, N. Limam, and R. Boutaba, “Deep learning for encrypted traffic classification in the face of data drift: An empirical study,” Computers & Networks, vol. 225, p. 109648, 2023. DOI: 10.1016/j.comnet.2023.109648

[38] Z. Akiirne, A. Sghir, and D. Bouzidi, “UDAP: Ultra lightweight dot product-based authentication protocol for RFID systems,” Cybersecurity, vol. 7, Art. no. 68, 2024. DOI: 10.1186/s42400 024 00252 6

[39] S. Rabhi, T. Abbes, and F. Zarai, “IoT routing attacks detection using machine learning algorithms,” Wireless Personal Communications, vol. 128, no. 3, pp. 1839–1857, Feb. 2023. DOI: 10.1007/s11277 022 10022 7

[40] R. Khan, N. Tariq, M. Ashraf, F. A. Khan, S. Shafi, and A. Ali, "FL DSFA: Securing RPL Based IoT Networks against Selective Forwarding Attacks Using Federated Learning," Sensors, vol. 24, no. 17, Art. no. 5834, 2024. DOI: 10.3390/s24175834

[41] H. Shahid and H. Ashraf, "Hop count-based detection scheme for sinkhole attack in wireless sensor networks," in Proc. 2025 Int. Conf. Comput. Commun. Networks, 2025, pp. 1–6, Springer. DOI: 10.1007/978-981-97-4540-1

[42] Y. Al Sawafi, A. Touzene, and R. Hedjam, "Hybrid deep learning-based intrusion detection system for RPL IoT networks," J. Sens. Actuator Netw., vol. 12, no. 2, p. 21, 2023. DOI: 10.3390/jsan12020021

[43] J. Hassan, A. Sohail, A. I. Awad, and M. A. Zaka, "LETM-IoT: A lightweight and efficient trust mechanism for Sybil attacks in Internet of Things networks," Ad Hoc Networks, vol. 163, Art. no. 103576, Oct. 2024. DOI: 10.1016/j.adhoc.2024.103576

[44] N. Sivasankari and S. Kamalakkannan, "Detection and prevention of man-in-the-middle attack in IoT network using regression modeling," Adv. Eng. Softw., vol. 169, Art. no. 103126, Jul. 2022. DOI: 10.1016/j.advengsoft.2022.103126

[45] S. Lazzaro, V. De Angelis, A. M. Mandalari, and F. Buccafurri, "Is your kettle smarter than a hacker? A scalable tool for assessing replay attack vulnerabilities on consumer IoT devices," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom), Biarritz, France, Mar. 2024. DOI: 10.1109/PerCom59722.2024.10494466

[46] M. Anjum, A. K. Dutta, A. Elrashidi, S. Shahab, A. Aldrees, Z. A. Shaikh, and A. Aljohani, "GraphFedAI framework for DDoS attack detection in IoT systems using federated learning and graph-based artificial intelligence," Scientific Reports, vol. 15, Art. no. 28050, Aug. 2025. DOI: 10.1038/s41598-025-10826-0

[47] M. Ibrahim and M. Darus, "DDoS Attack Analysis on IoT Device for Smart Home Environment and A Proposed Detection Technique," JOIV: International Journal on Informatics Visualization, vol. 8, no. 4, pp. 2104 2110, Dec. 2024. DOI: 10.62527/joiv.8.4.2175

[48] A. K. B. Arnob, "An Enhanced LSTM Approach for Detecting IoT Based DDoS Attacks Using Honeypot Data," International Journal of Computational Intelligence Systems, vol. 18, no. 1, 2025. DOI: 10.1007/s44196-025-00741-7

[49] R. Vennapureddy and T. Srinivasulu, "Pragmatic Study of Botnet Attack Detection in an IoT Environment," E3S Web of Conferences, vol. 591, 09012, 2024. DOI: 10.1051/e3sconf/202459109012

[50] S. Verma, Q. Wang, and E. W. Bethel, "Intelligent IoT Attack Detection Design via ODLLM with Feature Ranking based Knowledge Base," arXiv preprint, 2025. DOI: 10.48550/arXiv.2503.21674

[51] Z. ElSayed, A. Abdelgawad, and N. Elsayed, "CryptoDNA: A Machine Learning Paradigm for DDoS Detection in Healthcare IoT, Inspired by Cryptojacking Prevention Models," The International FLAIRS Conference Proceedings, vol. 38, no. 1, 2025. DOI: 10.32473/flairs.38.1.138680

[52] S. Alrubei, E. Ball, and J. M. Rigelsford, "Securing IoT-blockchain applications through honesty-based distributed proof-of-authority (HDPoA)," White Rose Research Online, 2021. [Online]. Available: https://eprints.whiterose.ac.uk/id/eprint/176157/1/2021085616.pdf

[53] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/en/bitcoin-paper. [Accessed: Oct. 10, 2023]

[54] E. O. Udeh, P. Amajuoyi, K. B. Adeusi, and A. O. Scott, "The role of blockchain technology in enhancing transparency and trust in green finance markets," Finance & Accounting Research Journal, vol. 6, no. 6, pp. 825–850, Jun. 2024. DOI: 10.51594/farjv6i6.1181

[55] F. Tong, S. Shen, S. Hosseinzadeh, et al., "Blockchain-assisted secure intra/inter-domain authorization and authentication," IEEE Internet of Things Journal, vol. 10, no. 9, pp. 7762–7776, May 2023. DOI: 10.1109/JIOT.2023.3212345

[56] J. Damre, A. Kharche, S. Jungade, V. Sanap, and S. A. Bachwani, "Blockchain: Types and benefits," Int. J. Comput. Sci. Eng., vol. 12, no. 1, pp. 569–573, Feb. 2022. [Online]. Available: https://rjpn.org/ijcspub/papers/IJCSP22A1066.pdf. [Accessed: Oct. 10, 2023]

[57] S. R. Channivally, "Blockchain in Internet of Things (IoT) Security," ResearchGate, Nov. 2023. DOI: 10.13140/RG.2.2.18730.59841. [Online]. Available: https://www.researchgate.net/publication/375834795_Blockchain_in_Internet_of_Things_IOT_Security. [Accessed: Oct. 10, 2023]

[58] M. Aljumah, M. Alzain, and M. Abdullah, "Blockchain-inspired distributed security framework for IoT networks," Scientific Reports, vol. 15, no. 2, pp. 101–115, 2025. DOI: 10.1038/s41598-025-93690-2. [Online]. Available: https://www.nature.com/articles/s41598-025-93690-2

[59] C. H. Hoffmann, “Is AI intelligent? An assessment of artificial intelligence, 70 years after Turing,” Technol. Soc., vol. 68, p. 101893, 2022. DOI: 10.1016/j.techsoc.2022.101893. [Online]. Available: https://doi.org/10.1016/j.techsoc.2022.101893

[60] H. Wu, “Feature-weighted naive Bayesian classifier for wireless network intrusion detection,” Security and Communication Networks, vol. 2024, Jan. 2024, Art. no. 7065482. DOI: 10.1155/2024/7065482

[61] M. Wazid, A. K. Das, V. Chamola, and Y. Park, “Uniting cyber security and machine learning: Advantages, challenges and future research,” ICT Express, vol. 8, no. 3, pp. 313–321, Sep. 2022. DOI: 10.1016/j.icte.2022.04.007

[62] L. Hao and Y. Xu, “Semi-supervised learning-based occupancy estimation for real-time energy management using ambient data,” IEEE Internet of Things Journal, vol. 10, no. 20, pp. 18426–18437, Oct. 2023. DOI: 10.1109/JIOT.2023.3280361

[63] X. Ma, H. Xu, H. Gao, M. Bian, and W. Hussain, “Real-time virtual machine scheduling in industry IoT network: A reinforcement learning method,” IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 2129–2139, Feb. 2023. DOI: 10.1109/TII.2022.3211622

[64] D. H. Abdulazeez and S. K. Askar, “Offloading mechanisms based on reinforcement learning and deep learning algorithms in the fog computing environment,” IEEE Access, vol. 11, pp. 12555–12586, 2023. DOI: 10.1109/ACCESS.2023.3245678

[65] E. Oye, E. Frank, and J. Owen, “Unsupervised and supervised models in machine learning,” ResearchGate, Dec. 17, 2024. [Online]. Available: https://www.researchgate.net/publication/387136555_Unsupervised_and_Supervised_Models_in_Machine_Learning [Accessed: Sep. 7, 2025]

[66] S. Majumder, “On the value of 'co-training' for semi-supervised software defect predictors,” arXiv preprint arXiv:2211.05920v2, Nov. 2022. [Online]. Available: https://arxiv.org/pdf/2211.05920v2 [Accessed: Sep. 7, 2025]

[67] M. Ghasemi and D. Ebrahimi, “Introduction to Reinforcement Learning,” arXiv preprint arXiv:2408.07712, 2024. [Online]. Available: https://arxiv.org/abs/2408.07712 [Accessed: Sep. 7, 2025]

[68] D. Thakur, J. K. Saini, and S. Srinivasan, “DeepThink IoT: The strength of deep learning in Internet of Things,” Artificial Intelligence Review, vol. 56, no. 12, pp. 14663–14730, Dec. 2023. DOI: 10.1007/s10462-023-10513-4

[69] V. B. Kumaravelu, V. V. Gudla, A. Murugadass, H. Jadhav, P. Prakasam, and A. L. Imoize, “A deep learning-based robust automatic modulation classification scheme for next-generation networks,” Journal of Circuits, Systems and Computers, vol. 32, no. 4, Art. no. 2350067, Mar. 2023. DOI: 10.1142/S0218126623500676

[70] G. Duncan, “Improving the performance of supervised deep learning for modeling genomic sequence–function relationships,” BMC Bioinformatics, vol. 25, no. 1, p. 202, 2024. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/38588559/ [Accessed: Sep. 7, 2025]

[71] Y. Liu, Y. Zhou, K. Yang, and X. Wang, “Unsupervised deep learning for IoT time series,” IEEE Internet of Things Journal, vol. 10, no. 16, pp. 14285–14306, Aug. 2023. DOI: 10.1109/JIOT.2023.3243391

[72] R. Ozdemir, “On the enhancement of semi-supervised deep learning for image classification,” Computers in Biology and Medicine, vol. 167, p. 104992, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0957417424009710 [Accessed: Sep. 7, 2025]

[73] P. Venkateswara Rao, V. B., Manjeet, A. Kumar, M. Mittal, A. Verma, and D. Dhabliya, “Deep Reinforcement Learning: Bridging the Gap with Neural Networks,” International Journal of Intelligent Systems and Applications in Engineering (IJISAE), vol. 12, no. 15s, pp. 576–586, 2024. [Online]. Available: http://www.ijisae.org [Accessed: Sep. 7, 2025]

[74] M. Ruzbahani, “Enhanced Blockchain-Enabled Security Framework for IoT Networks: Integrating AI and Privacy-Preserving Mechanisms for Scalable and Secure Smart Ecosystems,” Innovation and Integrative Research Center Journal, vol. 3, no. 4, pp. 288–302, Apr. 2025. [Online]. Available: https://iircj.org/wp-content/uploads/30.-Enhanced-Blockchain-Enabled-Security-Framework-for-IoT-Networks-Integrating-AI-and-Privacy-Preserving-Mechanisms-for-Scalable-and-Secure-Smart-Ecosystems.pdf

[75] M. Ruzbahani, “AI-Protected Blockchain-based IoT environments: Harnessing the Future of Network Security and Privacy,” Innovation and Integrative Research Center Journal, vol. 3, no. 4, pp. 288–302, Apr. 2025. [Online]. Available: https://iircj.org/wp-content/uploads/30.-AI-Protected-Blockchain-based-IoT-environments-Harnessing-the-Future-of-Network-Security-and-Privacy.pdf

[76] L. Ye, Z. Wang, Y. Liu, P. Chen, H. Li, H. Zhang, M. Wu, W. He, L. Shen, Y. Zhang, Z. Tan, Y. Wang, and R. Huang, “The challenges and emerging technologies for low-power artificial intelligence IoT systems,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 68, no. 12, pp. 4821–4834, Dec. 2021. DOI: 10.1109/TCSI.2021.3095622

[77] H. Yu, X. Zhang, Y. Li, and Z. Wang, “Privacy-preserving distributed identity system for IoT using blockchain,” Journal of Cybersecurity and Privacy, vol. 2, no. 1, pp. 45–60, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667295225000248

[78] A. G. Kuznetsov, A. Lyasnikov, and S. V. Ivanov, “On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security,” IEEE Access, vol. PP, no. 99, pp. 1–1, Jan. 2024. DOI: 10.1109/ACCESS.2023.3349019

[79] Y. Zhan, X. Zhang, L. Li, et al., “Diagnostic Accuracy of Artificial Intelligence Methods in Medical Imaging for Pulmonary Tuberculosis: A Systematic Review and Meta-Analysis,” Journal of Clinical Medicine, vol. 12, no. 1, p. 303, 2023. DOI: 10.3390/jcm12010303

[80] A. L. Bulgakov, A. V. Aleshina, S. D. Smirnov, A. D. Demidov, M. A. Milyutin, and Y. Xin, “Scalability and Security in Blockchain Networks: Evaluation of Sharding Algorithms and Prospects for Decentralized Data Storage,” Mathematics, vol. 12, no. 23, p. 3860, 2024. DOI: 10.3390/math12233860

[81] S. Goundar and I. Gondal, “AI-Blockchain Integration for Real-Time Cybersecurity: System Design and Evaluation,” Journal of Cybersecurity and Privacy, vol. 5, no. 3, p. 59, 2025. DOI: 10.3390/jcp5030059