(Online) ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Review Article*
Vol. 13, No. 4, October 2025, pp.805-824

A review paper: Blockchain security with IoT devices and deep-learning methods

Laith F. Jumma[1], Leila Sharifi[2], Parviz Rashidi[3]
[1] Computer Engineering Department, Urmia University, Urmia, Iran
[2] Computer Engineering Department, Urmia University, Urmia, Iran
[3] Information Technology and Computer Engineering Department, Urmia University of Technology, Urmia, Iran

Corresponding author E-mail: l.sharifi@urmia.ac.ir

ABSTRACT

Internet of Things (IoT) is changing the face of modern world by interconnecting billions of devices, transforming human life and revolutionizing innovation in various domains such as healthcare, transportation, and smart cities. However, the widespread deployment of IoT applications is dramatically hindered by the aforementioned remaining challenges, which mostly relate to the security, privacy, and trustworthiness of data. This work also discusses their limitations including: small computing power, use of insecure communication protocols, weak authentication, lack of encryption and susceptibility to Distributed Denial of Services (DDoS) attacks. Blockchains A blockchain is a decentralized, tamper-resistant authority which exhibits high levels of security, which could help solve the mentioned security problems of the IoT ecosystems. Blockchain can provide trust through data immutability, transparency and consensus and hence can be employed to provide security and reliability to IoT communication and storage. But integrating blockchain directly in low-resource IoT systems has certain issues like added latency, increased bandwidth usage and additional computational overhead. The objective of this paper is to present a detailed review of the synergy between the architecture of blockchain, the IoT systems and deep learning techniques, and the way that they can be collaboratively utilized for improving data security, trustworthiness, and decision-making in IoT networks. Specifically, we examine existing blockchain-based deep learning frameworks by categorizing them based on four major criteria: blockchain type (public, private, consortium), deep learning approach (e.g., CNN, GAN, DRL), consensus protocols, and datasets used for model training and validation. Furthermore, the paper analyzes the strengths and limitations of these integrated frameworks in addressing real-world IoT challenges. The review highlights how blockchain enhances the trustworthiness and traceability of deep learning outputs, while deep learning models can contribute to intelligent threat detection, adaptive control, and data-driven automation in IoT networks. Finally, we outline current research gaps and propose future research directions that focus on optimizing blockchain-deep learning frameworks for scalability, energy efficiency, and real-time performance in large-scale IoT deployments.

Keywords: Blockchain, deep learning, IoT, security.

1. Introduction

The Internet of Things (IoT) is reshaping the face of technology, allowing objects from common household appliances, medical appliances, industrial equipment and other to interconnect, sense, process and communicate over the internet. This paradigm shift will enable the hitherto unimaginable levels of automation, efficiency and real time decision-making in areas as diverse as smart healthcare, intelligent transport, energy grids and defense. Yet, the proliferation of IoT devices also engenders intricate security and privacy challenges. The same characteristic, which renders IoT innovative (i.e.,

distributed architecture, autonomous communication, and heterogeneity) is also the causes that make it susceptible to various cyber threats and operational constraints.

At the root of these challenges is the problem of how to protect user data and device integrity in the resource-constrained worlds of computation, memory and power. IoT devices are generally implemented and conceptualized to be low-priced, small, and feature-rich, so that there is little room for them to include rigorous encryption, authentication, and anomaly detection mechanisms. Energy efficiency requirements and limited hardware resources also limit the use of standard security mechanisms. The situation is made worse by the piecemeal development of IoT solutions—multiple vendors, stacks, and standards that result in poor interoperability and fragmented security implementations. As shown by previous work [1], such problems motivate a new way of fostering cyber-attacks, e.g. data forging, packet sniffing, eavesdropping, unauthorized access, or malware installation.

In order to address these weaknesses, many researchers have proposed the use of blockchain technology as a decentralized security system for the IoT. The blockchain, a tamper-resistant and cryptographically related distributed record, provides inherent security characteristics, such as the immutability of the data, the consensus-based validation and the traceability of the transactions. With no reliance on a central coordinating or trusted party, as provided by the blockchain protocol, peer to peer devices can trustless communicate and coordinate their actions. For instance, Raj et al. [2] proposed a simple communication system for IoT devices based on blockchain technology using the Ethereum blockchain, in which the smart contracts are used to enforce rules and ensure data exchange among intelligent agents. Loukil et al. [3] generalized this idea and introduced a privacy-preserving scheme, based similarly on the Ethereum test networks. Their infrastructure makes use of smart contracts to control device access and log behavior helps to detect compromised devices for isolating them from the network to make the system more resilient.

Apart from communication, blockchain is also suggested as a decentralized storage solution. Gochhayat et al. [4] proposed a blockchain-encrypted cloud storage architecture to solve the central point of failure problem in the existing centralized storage systems. Implemented on cost-effective Mystico blockchain, their scheme is capable of high throughput (700–800 transactions/ s) and exhibits linear scalability with respect to the number of nodes. These features deem blockchain an appealing infrastructure for secured massive IoT data processing, particularly in industrial monitoring, supply chain, and health informatics, where numerous integration points, and vulnerabilities do exist.

Despite the appealing advances, the integration of blockchain in the IoT architectures is far from trivial. These security benefits are not without side effects: the cryptographic overhead, network bandwidth, and energy costs, which can be beneficial in an unrestricted network in general but harmful in a constrained IoT environment. Liang and Ji [5] also mention similar drawbacks in their survey; the static public key being employed for node identity in blockchain network may reveal a kind of usage patterns and result in privacy leak. They also highlight that blockchain systems are insecure against majority (51%) attacks where adversarial nodes controlling the process of reaching consensus. Moreover, the delay caused by block propagation and mining makes real-time guarantee abased data processing of IoT applications more difficult. Furthermore, the cryptographic overhead and consensus algorithm complexity make it difficult for low-power devices to access the blockchain all the time.

To address these two-fold constraints IoT boundaries and blockchain overlays recent works considered deep learning (DL) as a complementary technology. Deep learning models such as (1) convolutional neural networks (CNNs), (2) generative adversarial networks (GANs) and (3) deep reinforcement learning (DRL) have developed promising applications in anomaly detection, predictive maintenance, traffic prediction and threat intelligence. These models are expected to impart autonomous and intelligent security decision- making. When combined with a blockchain, DL systems would have access to immutable, trustable datasets, while the blockchain would enjoy the intelligent, train-able filtering and classification of the DL models. The objective of this review article is to systematically study and categorize some of these endeavors in the literature, which investigate the amalgamation of blockchain and deep learning for improving security, privacy, and autonomy in the context of IoT. The paper discusses how blockchain's decentralization and trust services can provide DL models with authentication, tamper-evident data and how DL algorithms can be used to monitor, control, and optimize blockchain-supported IoT systems. We focus on four different dimensions: (a) blockchain type (public, private or consortium), (b) type of deep learning model, (c) type of consensus protocol, and (d) data sets used for training and validation.

The purpose of this survey is to give researchers, developers, and companies an organized view of the recent progress, technical publications, technical trends and open issues of this emerging area. Drawing on academic literature, the article synthesizes available information to highlight promising methods for implementation of secure and smart IoT systems. It

also draws attention to important research challenges that are still open, including the absence of an energy-efficient consensus, scalability for big networks, and real-time inference on limited hardware. The paper ends with future directions, namely, to make lightweight blockchain-DL framework that is most suitable in the real practice of IoT.

2. Literature review

The Internet of Things (IoT) has given rise to a new paradigm in data production and real-time connections yet poses fundamental challenges in preserving the security and privacy of distributed environments. As the number of connected devices skyrockets, the current predominantly electronic-based solutions are unable to handle the potential threats from impersonation attacks, leaked keys, and software hacking. In that context, there have been investigations regarding the combination of blockchain and deep learning for decentralized security and intelligent threat detection, which is a promising solution for these issues. This section briefly evaluates the most relevant related work in three key areas: (1) security and privacy issues in IoT scenarios, (2) the enabling functionality of blockchain technology for the protection of digital assets (i.e., Bitcoin), and (3) the emerging meeting point between blockchain and deep learning (DL) tools when designing secure, scalable, and autonomous IoT environments.

2.1. Security and privacy in IoT

As the environment of IoT works with huge internet-connected device networks that provide various services through sharing enormous sensitive information in real-time, it is a vast ecosystem of smart connected devices which continually gather information and sharing control in it. The sheer size, diversity and resource limitation of most IoT devices are imposing great security and privacy challenges. Most of these systems work in privacy-sensitive domains, including homes, healthcare and industry, hence, becoming lucrative targets for cyber-attacks.

To cope with this, authors in [5] present a privacy zoning-based system that categorizes data in different sensitivity layers and executes context-aware policy checks on the data before access is authorized. An interior Home Security Hub verifies requests to access devices and enforces zone-based control policies to deny unsolicited communications on behalf of private devices. This zoning model is a strong value added as it dramatically reduces the lateral movement, that malicious people can do within a same smart home network.

Meanwhile, [6] showed that in general, commercially available IoT devices do not have rudimentary security features, such as secure communication or authenticated access control. To fill this gap, they proposed the concept of the Security Management Provider (SMP) with static or dynamic content-based access restrictions for secure data and device sharing. Their model, however, is not yet mature for user's privacy protection, TN for example, the external communication or data released case still a challenge to them. Authors in [7] provided an extensive study of IoT security threats, with a focus on smart homes. They discussed threats at various levels such as sensor-level and insecure aggregation of data, and unsecured gateways. The research highlighted the inherently interconnected nature of IoT vulnerabilities this finds single weakest device, which can potentially be exploited and become the weakest link to undermine the whole system security posture. From the perspective of privacy preservation, [8] introduced a technique named Safe Answers, which aims at reducing personal data disclosure by at least aggregating or anonymizing the user answers before releasing them to the service providers. Sometimes their solution adds noise or data multiplication to cover a true input and so it goes on and on, to compromise privacy." Unfortunately, this trade-off between privacy and data accuracy can have adverse influence on the dependability of intelligent services, particularly for applications requesting disciplined and accurate real-time inputs (e.g. for smart lighting, HVAC or emergency systems).

2.2. Bitcoin blockchain (BC) and IoT integration

The Bitcoin blockchain (BC) is the first and most popular application of the distributed ledger technology. It serves as an indelible chain of blocks, one in which every block holds verified transactions. In the decentralized system of Bitcoin, the nodes with changing public keys partake in the task of validating and forwarding data. Dedicated nodes, known as miners, append new blocks by solving cryptographic puzzles via the Proof of Work (PoW) consensus algorithm. Given that the BcB possesses some fundamental properties such as immutability, decentralization, anonymity and integrity, it has been suggested to leverage the BcB as an underlying infrastructure for improving the security of IoT. 4) Eliminating central point of failure: with no need for trust, central authorities, blockchain could lower the threat of single-point failure, while providing tamper-resistant record of audit trail for device communication and data transactions. For instance, [9] presented a multi-tier BC architecture of secure data sharing between IoT devices and third parties like businesses and consumers. Despite providing an original design for trustless data exchange, the model assumes that IoT devices can perform complex

tasks, which is not practical especially for low-power IoT sensors. The resource cost of PoW mining also serves as a great obstacle, due to its need for high computation and power cost, and could not be satisfied by lightweight IoT devices. Furthermore, embedding BC in the IoT ecosystems faces the challenges in network latency, network bandwidth utilization and scaling problems. Requirements to synchronize distributed ledgers on thousands of devices introduce communication overhead and hinder the responsiveness of the system. Such considerations point out the need for lightweight blockchain versions or for other consensus mechanisms that are more convenient in IoT settings.

3. Classification of methodology

In a structured manner, it is important to classify the different approaches that have been used in the literature to integrate blockchain and deep learning in context of IoT Security. This categorization helps to provide a clear understanding, for instance, on how blockchain architectures, consensus mechanisms and deep learning models have been adjusted to suit the needs in terms of secure scalable and intelligent IoT systems. In this section, we compare the previous methods along consensus approaches, blockchains used, model architecture, learning strategies, data privacy methods, and application domains. We propose organized categories for these approaches that form a detailed basis to evaluate their strengths, limitations, and future directions on blockchain-enabled deep learning for IoT security.

3.1. Blockchain-based deep learning

Blockchain technology has emerged as a powerful enabler for enhancing the security, transparency, and reliability of deep learning (DL) applications, particularly in distributed and sensitive environments such as the Internet of Things (IoT). One of its key contributions lies in enabling the secure sharing and reuse of deep learning models across multiple nodes without the risk of tampering or unauthorized modification. In many real-world scenarios, DL models are trained on sensitive datasets such as patient health records, biometric data, or industrial monitoring logs which require high levels of trust and integrity during training, validation, and deployment phases. Blockchain addresses these needs by providing a decentralized infrastructure that ensures audibility, data verification, result attestation, provenance tracking, and traceability of data ownership and model usage, while also supporting fairness in collaborative machine learning processes [10].

Deep learning models function by learning hierarchical patterns from large volumes of input data and outputting probabilistic predictions. While these models excel at handling raw, unstructured data, their accuracy and robustness are highly dependent on the quality, integrity, and consistency of the input data. In traditional centralized settings, the data pipelines feeding into deep learning systems may be susceptible to corruption, leakage, or bias. Blockchain mitigates these risks by offering an immutable ledger where all data entries are securely recorded, transparently accessible, and cryptographically linked. This makes it practically impossible to manipulate data once it has been committed to the chain, thus providing a trustworthy foundation for data-driven AI systems.

The key features of blockchain that synergize with deep learning to enhance application performance and resilience are summarized in Table 1 [11]. These include decentralization, transparency, immutability, and traceable transaction history. Additionally, Figure 1 illustrates the major categories and use cases that benefit from this integration. These typically involve systems that demand autonomous operation, secure data sharing, collaborative training, or sensitive decision-making. The inherent immutability of blockchain data storage also protects DL models from data poisoning, noise injection, or adversarial manipulation, thereby improving the reliability and precision of their predictions.

The fusion of blockchain and deep learning unlocks new potential for building intelligent, decentralized, and verifiable systems. Tasks that previously required centralized control, human oversight, or trusted intermediaries can now be automated using blockchain-backed DL models. In this joint framework, deep learning can process and analyze rich, real-time data streams, while blockchain ensures that all interactions, decisions, and data exchanges are tamper-proof and traceable. This mutual reinforcement creates a resilient digital ecosystem where decision-making becomes not only smarter but also more secure and auditable.

Some of the most notable benefits of integrating blockchain technology with deep learning include:

Data Security: Blockchain ensures a high level of data integrity and confidentiality by distributing records across multiple nodes in the network. In private blockchain implementations, sensitive data can be securely stored and accessed only by authorized participants using encrypted private keys. This setup prevents unauthorized access and provides a verifiable chain of custody for the data. When deep learning algorithms operate on such verified and trusted data sources, the resulting decisions become more trustworthy, accurate, and verifiable [12].

Automated Decision-Making: Blockchain's peer-to-peer (P2P) architecture supports decentralized and autonomous decision execution. Smart contracts can trigger specific DL model responses automatically when certain conditions are met. Moreover, blockchain allows each model's predictions and decision-making steps to be traced and verified, enabling the auditing of AI decisions and reinforcing trust in the automation process [10, 13].

Cumulative Intelligence and Voting-Based Judgments: In distributed intelligent systems, such as deep reinforcement learning agents or swarm robotics, autonomous entities frequently make decisions based on collective observations. The integration of blockchain allows these agents to record and exchange observations securely, leading to voting-based decision systems where consensus can be reached through verifiable data sharing. This is particularly useful in dynamic environments where decisions must adapt in real-time to evolving contexts [14, 15].

Robustness and Trust Enhancement: In various high-stakes scenarios such as medical diagnostics, financial forecasting, or autonomous driving—deep learning models can outperform humans in terms of speed and accuracy. However, the trustworthiness of these models often comes under scrutiny due to the black-box nature of their internal operations. By integrating DL systems with blockchain, the entire data lifecycle, model updates, and decision logic can be recorded immutably, enhancing accountability and stakeholder trust. Furthermore, the decentralized nature of blockchain reduces the risk of single points of failure and increases the robustness of AI-driven systems in critical applications [16].

In conclusion, the combination of blockchain and deep learning creates a mutually reinforcing technological synergy. Blockchain secures the data pipeline and decision-making process, while deep learning brings intelligence, automation, and adaptability to blockchain-enabled systems. This integration is particularly promising for applications where privacy, autonomy, auditability, and resilience are non-negotiable requirements, such as in healthcare, finance, energy, and IoT-driven infrastructures.

Table 1. Summarizing briefly the blockchain and deep learning capabilities that can be used to enhance based software

Deep learning	Blockchain	Possible Results
Scalable	Immutable	Flexible approaches to learning
Layered	Transparent	Model of collaboration updated
Resource intensive	Integrity	increased scaleability
Data intensive	Cybersecurity	better data security

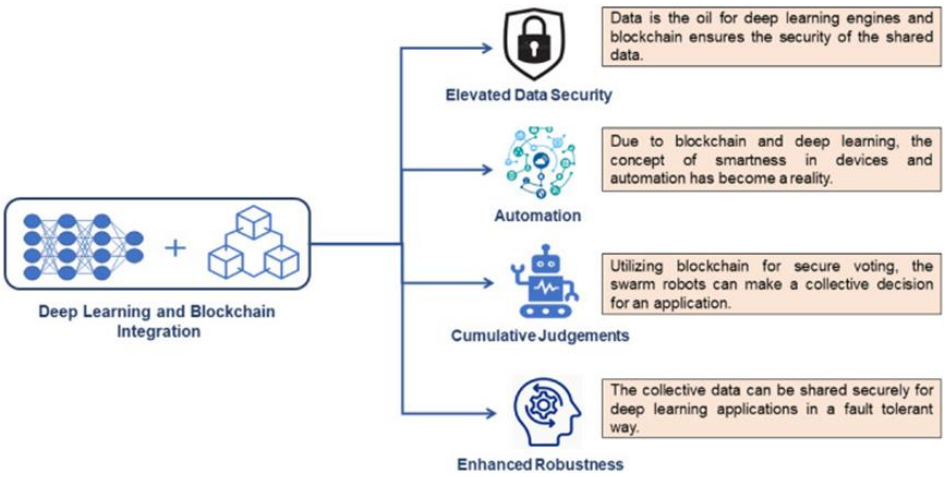

Figure 1. The combination of deep learning and blockchain technology produced benefits

Blockchain with deep learning frameworks classification

The major advantages which have the potential to attain through the fusion of deep learning techniques with blockchain are:

- Decision-making automation.
- Data protection.
- Precise forecasting.
- Effective manage of data-marketing.

This part provides a thematic classification to categorize the available union of deep learning and blockchain technologies according to criteria. Figure 2 identified parameters emphasize the similarities and contrasts across cutting-edge blockchain based on deep learning systems. Below is a brief description of the chosen parameters and their technological specifics.

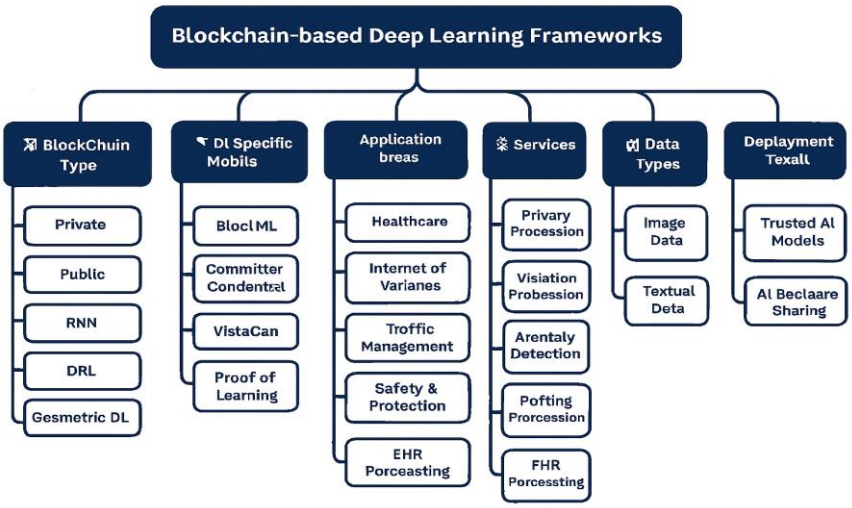

Figure 2. Classification of deep learning with blockchain-based frameworks

3.2. Blockchain types

Blockchain technologies used in current deep learning frameworks can be classified into three main categories based on their structural and operational characteristics: public, private, and consortium (federated) blockchains. This classification plays a significant role in determining the effectiveness, scalability, and security of blockchain-based deep learning systems, especially in Internet of Things (IoT) environments where latency, data throughput, and access control are critical factors.

One of the key advantages of blockchain integration with deep learning is the ability to leverage time-specific modalities. These enable time-sensitive decision-making in real-time applications such as autonomous driving, remote sensing, healthcare monitoring, and smart manufacturing. Blockchain ensures the reliability and integrity of the data feeding into deep learning models in these scenarios, helping to maintain their effectiveness under temporal constraints.

Public Blockchains are fully decentralized and open to anyone who wishes to participate. Every node has equal rights to validate transactions and access data. Public blockchains, such as Ethereum and Bitcoin, offer high transparency and trust but often suffer from scalability issues, higher energy consumption, and slower transaction rates. Nevertheless, they are favored in environments where full transparency and trustlessness are critical [17].

Private Blockchains, by contrast, are controlled by a single organization. They offer better performance in terms of transaction speed and resource consumption but at the cost of decentralization. Private blockchains are suitable for applications where control, privacy, and speed are more important than public verifiability. Deep learning models that require access to secure, controlled data sources—such as in banking, health care, or enterprise settings—can benefit from private blockchain integration [18].

Consortium (or Federated) Blockchains represent a hybrid approach, combining features of both public and private systems. In a consortium blockchain, a group of pre-approved institutions or nodes governs the blockchain network collectively. This structure offers a balance between decentralization and performance. Access to data may be public or restricted, but only trusted members have the authority to validate and commit transactions. As a result, consortium blockchains are more scalable than public blockchains and more decentralized than private ones, making them particularly well-suited for collaborative deep learning environments where multiple stakeholders—such as hospitals, universities, or logistics providers—need to jointly access, verify, and share data while preserving trust and control [19], [20].

In deep learning-enhanced IoT ecosystems, consortium blockchains are often the preferred choice due to their ability to enforce controlled participation, support data privacy, and reduce the risks of single-point failure, while still benefiting from collective consensus. Their higher transaction validation rates compared to public blockchains also help in reducing latency, which is essential for real-time deep learning predictions and model updates.

3.3. Deep learning models

The gathered data is processed by a deep learning model, which identifies patterns that can be used in various use cases. Deep-learning models that are used for decision making in many application domains are divided into five main types based on the configuration of neural network layers. An overview of deep learning models that have produced patterns and made judgments using data from blockchains is provided below.

Neural convolutional network Convolution Neural Network (CNN), or ConvNet, analyzes an image to recognize the items, give the weights of the objects, and categorize them under the context. It also makes it possible to find occurrences of things in the processed image [21]. convolution neural network has been used by the deep learning frameworks built on blockchain to classify photos, segment instances in various use scenarios and identify objects. Furthermore, because CNN uses flexible filters to identify the qualities of the image, blockchain-based studies benefit from the algorithm's minimal preprocessing time requirement.

Networks of generative adversaries (GAN) The generative model can produce original data and learns unsupervised patterns. More specifically, it is a type of deep learning modelling that uses convolutional neural networks. The GAN model is built with a generator network and a discriminator network. The discriminator learns to categorize the input as valid or fraudulent while the generator creates fresh samples.[21]

Deep reinforcement learning (DRL) helps expert systems comprehend the data more precisely by drawing inspiration from theories of human behavior based on behavioral ecology. DRL models make up the environment in which intelligent agents act to learn. Agents are also implicitly rewarded or punished based on their actions. Reinforced learning-based models reward actions that result in the intended outcome [22, 23].

3.4. Scope of applications

In the healthcare sector, patient data is extremely crucial. Researchers use the healthcare data that comes from clinicians reviewing images and scans to train deep learning models for the prediction of communicable and non-communicable diseases like COVID-19 and cancer, as well as to find new methods of disease diagnosis, enhance clinical trials, and improve the quality of healthcare services [24, 25, and 26]. The healthcare data includes details on diseases, symptoms of illnesses, and patient medical histories. This information aids deep learning models in predicting the patient's health in the future. The healthcare industry has the highest standards for the security and accuracy of such data because it directly affects human life. Yet, storing data in this manner leaves centralized systems vulnerable to attack. Blockchain technology can therefore be very useful in maintaining all the data in this circumstance because it is naturally decentralized and provides a defense against threats to data security. Additionally, blockchain ensures that the data won't be accidentally or purposefully lost.

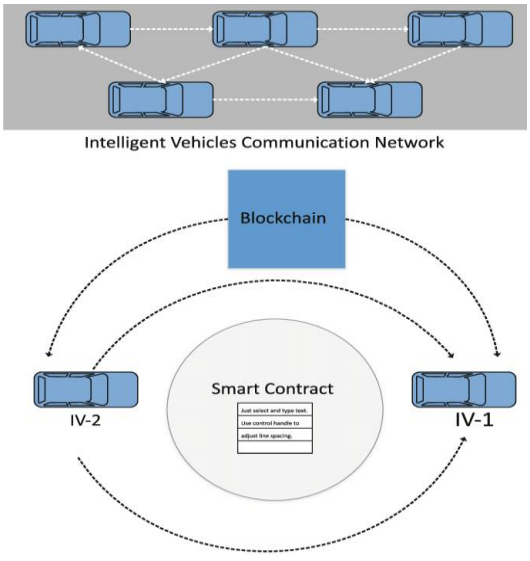

Figure 3. (V2V) and (V2I) communication technology based on blockchain

On the internet, the networking capabilities of current gadgets have quickly increased as the Internet of Things (IoT) becomes increasingly popular as vehicle instrumentation technology [24]. Modern transportation systems frequently include gadgets, sensors, and intelligent software in their vehicles to allow them to connect and exchange data. The data

can be safely shared among the entities, as shown in Figure 3, by implementing blockchain on the Internet of Vehicles (IoV) network [27]. Intelligent transportation systems' V2V communication mode makes a vehicle to exchange information with others. Based on this information, vehicles determine various actions, such as the best course of action. To increase efficiency, convenience, and public safety, vehicles can communicate the data they collected with roadside devices, including lane markings, lighting, RFID readers, and cameras [28].

As a result of increased carbon dioxide emissions, traffic control is a pressing issue in many urban areas [29]. One of the most well-liked strategies for foreseeing traffic volumes with real-time data is crowdsourcing. Yet, concerns regarding human safety and centralized data storage may make current crowdsourcing alternatives more viable.

Defense and security are two areas where blockchain technology is widely used and relevant because of its security feature of data immutability. Blockchain's unique qualities, like its ability to store data decentralized, can be used in securing a wide range of use cases. Nevertheless, data integrity can still be compromised via a 51% attack on the blockchain [29]. Such assaults can be thwarted by employing machine learning techniques on data. In addition, malware detection and identification are aided by signatures, which serve as the digital fingerprint of malicious code.

3.5. Frameworks for deep learning based on blockchain

The integration of blockchain technology with deep learning has paved the way for a new generation of secure, decentralized, and trustworthy AI frameworks, especially in domains where data privacy, traceability, and model integrity are critical. This section provides an overview of state-of-the-art blockchain-supported deep learning systems and evaluates them based on their design, application, and technical merits reported in the literature.

3.5.1 Secure deep learning in healthcare

In domains like pharmacogenomics, where genetic data guides precision medicine, privacy-preserving computation is essential. A blockchain-enabled deep learning framework for ovarian cancer prediction was introduced in [30], enabling secure collaboration among affiliated institutions. Patient records and genomic data are encrypted and accessed through a distributed blockchain ledger, ensuring compliance with privacy regulations. The system was validated using CRYPTO++ and demonstrated efficient performance in encryption and decryption latency, making it suitable for time-sensitive diagnostics.

3.5.2 AI model provenance and trust

The authenticity and traceability of AI models are critical to maintaining trust in autonomous systems. Blockchain enables logging of the entire model lifecycle—from data acquisition and training to versioning and ownership [31], [32]. This traceability mechanism helps mitigate data poisoning attacks and unauthorized alterations. In [33], authors emphasized that such provenance tracking is particularly vital in smart grids and critical infrastructure, where erroneous predictions can have severe consequences.

3.5.3 Federated learning enhanced by blockchain

Federated learning (FL) allows AI models to be trained locally on edge devices while preserving user data privacy. Blockchain augments FL by securely recording training contributions, model updates, and validation scores on a decentralized ledger [10]. As depicted in Figure 4, each device updates a global model via a consensus-driven blockchain network, ensuring transparency and preventing malicious model updates or adversarial attacks [34], [35]. This architecture has been effectively applied in e-health systems, autonomous transportation, and Industry 4.0 environments, where both trust and auditability are essential.

3.5.4 Cross-domain applications

As shown in Figure 5, blockchain-integrated deep learning is being widely adopted across various sectors:

- Healthcare: Privacy-preserving neural networks for patient data classification, chronic disease prediction, and medical imaging [36], [37].
- Smart Transportation Systems: Fraud-resistant toll collection, secure vehicle-to-vehicle (V2V) communication, and autonomous traffic control [38].
- Cybersecurity: Blockchain-enhanced frameworks for malware classification, intrusion detection, and DDoS mitigation using adversarial learning [39].

- Industrial IoT (IIoT): Tamper-proof firmware updates, device trust scoring, and automated fault detection and response in distributed systems [40].

Each of these applications leverages a common architectural paradigm: a distributed deep learning engine deployed over a blockchain-based infrastructure, ensuring privacy, authenticity, collaboration, and operational robustness without a centralized authority.

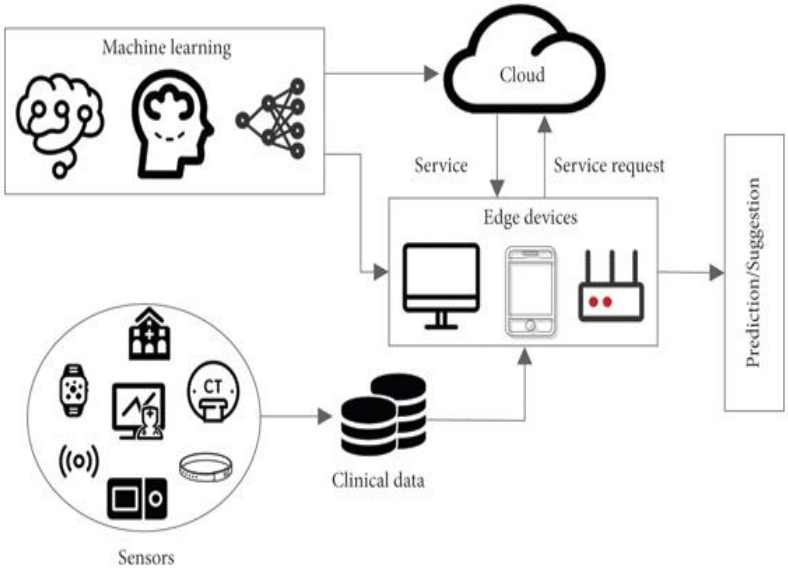

Figure 4. Blockchain-based federated learning

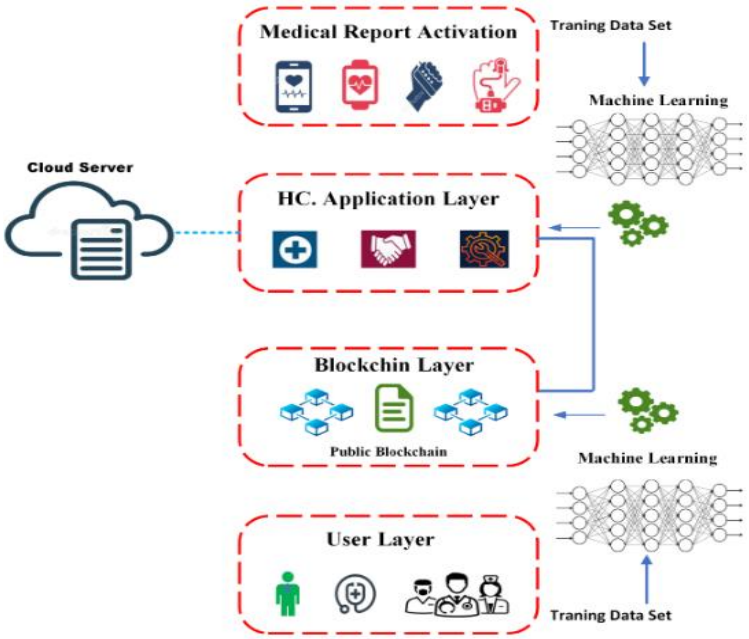

Figure 5. The results of combining blockchain with deep learning in different fields, focusing on the system's parts and the people who use them [6]

4. Results and discussion

This article outlines several current IoT system issues and the advantages of blockchain technology. Although the penetration test did find a few minor security flaws, overall security was very high. Several research publications were looked at concerning IoT vulnerabilities. Figure 6 provides an overview of the assessed biases in the chosen studies. A full circle in this diagram represents each featured research paper. Each process stands for a particular preference that has been evaluated, and the various colors show assessment allocation. If so, the assessments may be low, medium, high or not applicable.

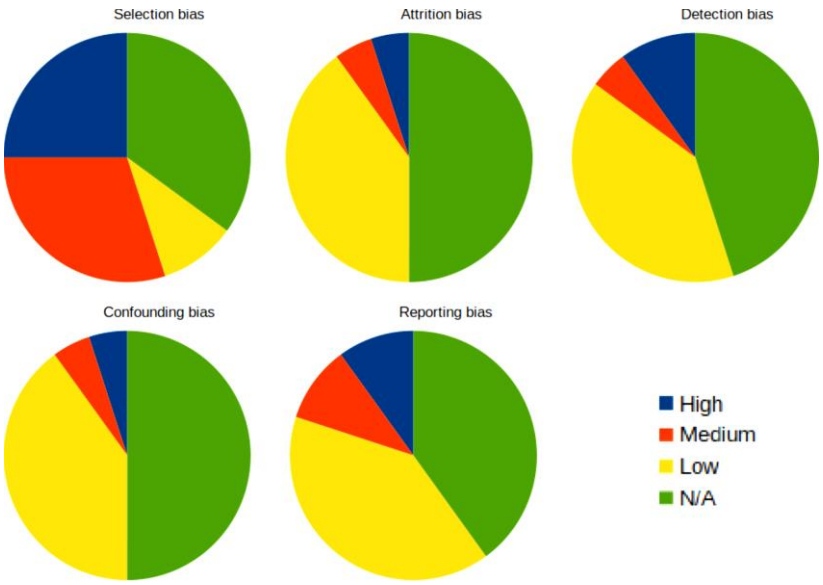

Figure 6. Biases in publications that have been reviewed [5]

Figure 7 presents a consolidated visualization of the various security flaws identified across all examined research articles. Each threat was extracted from the studies through a manual content analysis process, wherein keywords and reported vulnerabilities were coded and aggregated. These threats are arranged on the y-axis, while the x-axis quantifies the number of times each threat was mentioned or discussed across the reviewed literature. The Distributed Denial-of-Service (DDoS) attack emerged as the most frequently reported security issue, appearing prominently in a large number of sources. Several studies also made specific references to the Mirai botnet, which exploits insecure IoT configurations and default credentials to propagate and launch large-scale attacks. In addition to DDoS, other frequently cited threats included insecure data storage, weak authentication, and inadequate firmware update mechanisms.

Many of the vulnerabilities identified were not isolated, but rather interrelated or cascading in nature. For example, the existence of hardcoded credentials often correlated with insecure interfaces or the lack of proper authorization controls. Before proceeding with classification, similar vulnerabilities were grouped together based on semantic and technical similarity. This step was essential to avoid redundancy and ensure a consistent mapping process.

To structure the analysis and evaluate the distribution of vulnerabilities, we adopted the OWASP IoT Top 10 as a standardized framework for classification. The OWASP project is a widely recognized and authoritative source in the cybersecurity community, and its IoT Top 10 provides a taxonomy of the most critical risks specific to Internet of Things systems. Using this model, each identified vulnerability was matched to its corresponding OWASP category (e.g., “Insecure Network Services,” “Lack of Device Management,” or “Insecure Data Transfer and Storage”). Figure 8 illustrates the resulting distribution, showing how the reported vulnerabilities were spread across the OWASP categories. The data for this figure was obtained by calculating the frequency with which each OWASP category appeared across the coded threats in the reviewed studies.

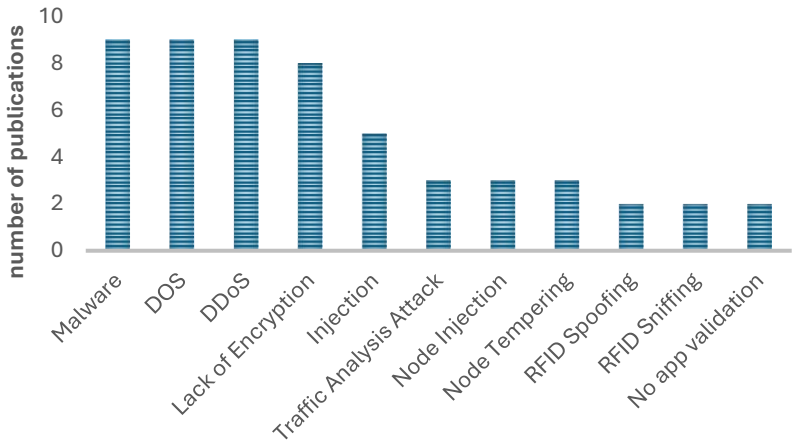

Figure 7. All identified security flaws and assaults

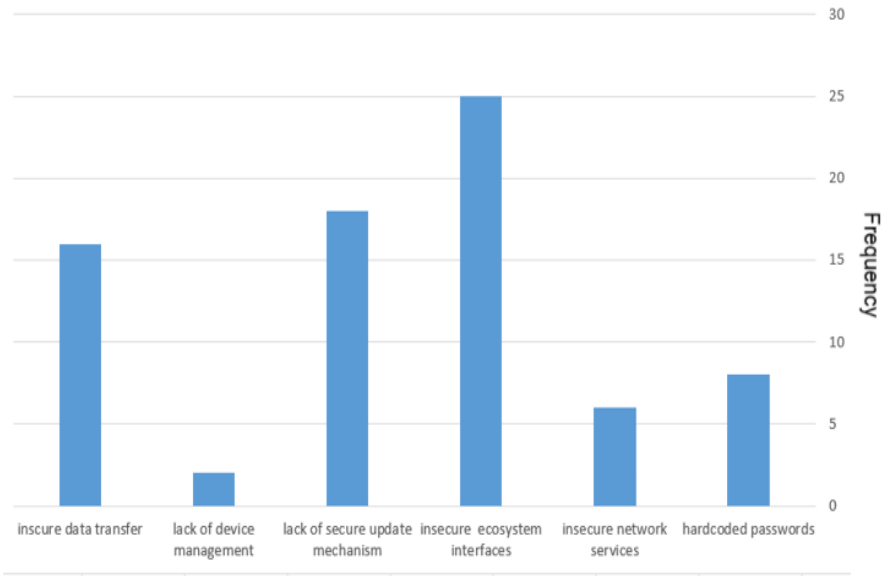

Figure 8. Frequency of all identified security concerns and attacks

Researchers have found that the Mirai malware is a popular topic for their studies. But this is a significant difficulty because it is so easy to exploit. Weak, difficult-to-guess passwords are a hallmark of the malware. Malware can then use default passwords to infect more IoT firmware and spread from there. Devices can be safeguarded by mandating more complex passwords, even in the face of severe threats like botnet attacks and the subsequent infection of Mirai malware. While the device would be protected from infection, it could still be vulnerable to a distributed denial of service (DDoS) assault from other open devices [3,7,33,39].

This group includes the IoT dangers that are most frequently discussed. Threats to input data validation are a common occurrence. Malicious input can, for instance, induce DoS and authentication bypass in various IoT devices. Several publications examine multiple components, including mobile UI, and analyze them statically to find these vulnerabilities. Lack of verification in various ways is another frequent problem identified in the research. Typically, the present authentication in vulnerable devices must be revised. [34, 37]. Few academic publications examine insecure update processes, although many of the papers we analyzed refer to the IoT's fundamental integrity problem. Introducing malicious files into a system is a serious matter, and there are many techniques for tricking vulnerable Internet of Things devices into trusting harmful software. [30, 34] The measures to mitigate this are being developed. Development of secure systems within the development

In order to assess the practical difficulty of exploiting the identified vulnerabilities, we evaluated their exploitation complexity, as reported or implied by the authors of the primary studies. Where explicit complexity levels were provided (e.g., “low effort,” “requires physical access”), we used those directly; in cases where such data was absent, qualitative assessments were inferred based on technical context and standard threat modeling frameworks. These assessments were then normalized using a five-point Likert-type scale ranging from 0 (very low complexity) to 5 (very high complexity). Figure 9 visualizes the average exploitation difficulty of each vulnerability, with the x-axis representing the mean complexity rating and the y-axis listing the threat categories.

Complementing this, Figure 10 displays the average severity or impact potential of the exploits. This rating captures the degree of harm or disruption that successful exploitation of each vulnerability could cause—ranging from minor privacy breaches to full device takeover or service disruption. The severity ratings were synthesized using either directly reported values from the source articles or approximated using standard cybersecurity scoring systems such as CVSS (Common Vulnerability Scoring System) where applicable. Like Figure 9, a 0–5 scale was used, with higher values indicating more critical risks.

Together, these figures offer a comprehensive perspective on the current landscape of IoT vulnerabilities as reported in the literature. The combination of frequency, complexity, and severity metrics enables a multi-dimensional understanding of the threats, helping researchers and practitioners prioritize security measures based not only on how common a vulnerability is, but also how dangerous and easy it is to exploit. These insights form the basis for the later sections of this paper, where potential mitigation strategies using blockchain and deep learning are discussed in detail.

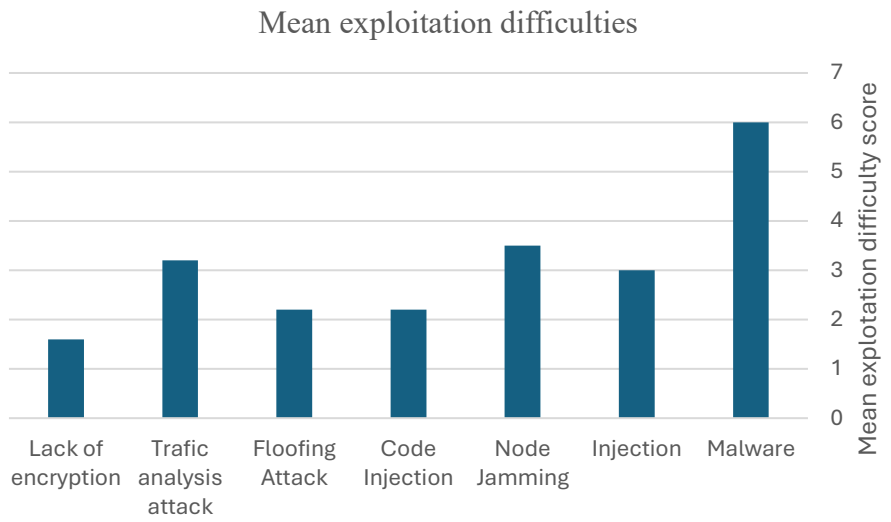

Figure 9. All identified security flaws and assaults

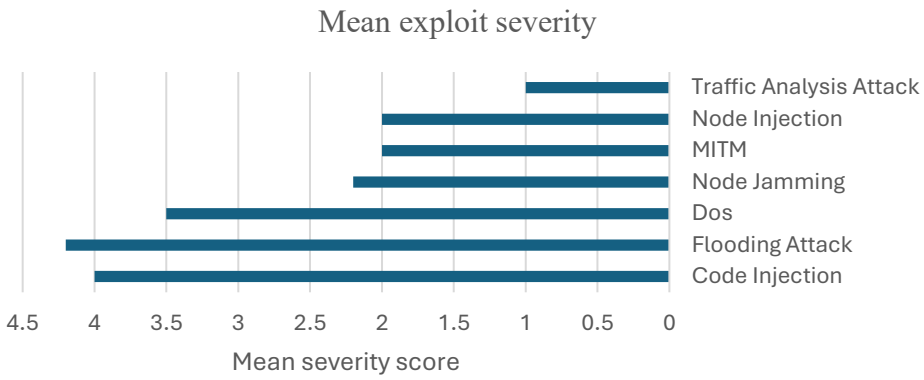

Figure 10. Mean exploit severity

To gain a holistic understanding of IoT vulnerabilities, it is essential to evaluate not only their frequency and severity but also the practical challenges associated with exploiting or mitigating them. Therefore, in this analysis, we introduce a criticality index that combines two key dimensions: (1) the weighted severity of each vulnerability, and (2) the complexity or difficulty of exploitation, both derived from the reviewed literature. This composite measure allows us to rank vulnerabilities based on both their potential impact and operational challenge, providing a more nuanced and actionable classification scheme.

Figure 11 presents a graphical representation of this merged assessment. The y-axis illustrates the overall criticality score for each vulnerability category, reflecting the severity and difficulty of managing each issue when both dimensions are considered in tandem. This score was computed using a bias-weighted aggregation of the average severity and complexity values (as depicted in Figures 9 and 10), normalized to ensure comparability across the OWASP IoT Top 10 vulnerability categories. The x-axis lists the ten OWASP categories, such as "Insecure Network Services" and "Insufficient Update Mechanisms."

Each bar in the figure shows the relative importance or risk ranking of the corresponding category, based on its criticality percentage. Categories that scored high in both severity and ease of exploitation were given greater weight in the final ranking. For instance, vulnerabilities that are both common and highly damaging—yet also easy to exploit—were assigned the highest criticality levels, signaling the need for immediate mitigation in real-world IoT systems.

The data used to generate these scores were synthesized from all reviewed studies, which are listed in Table 2. This table includes references to the original research articles that discussed the vulnerabilities, as well as the sources from which severity and complexity estimations were derived. Together, Figure 11 and Table 2 form the foundation for the threat prioritization approach used in the subsequent sections of this paper.

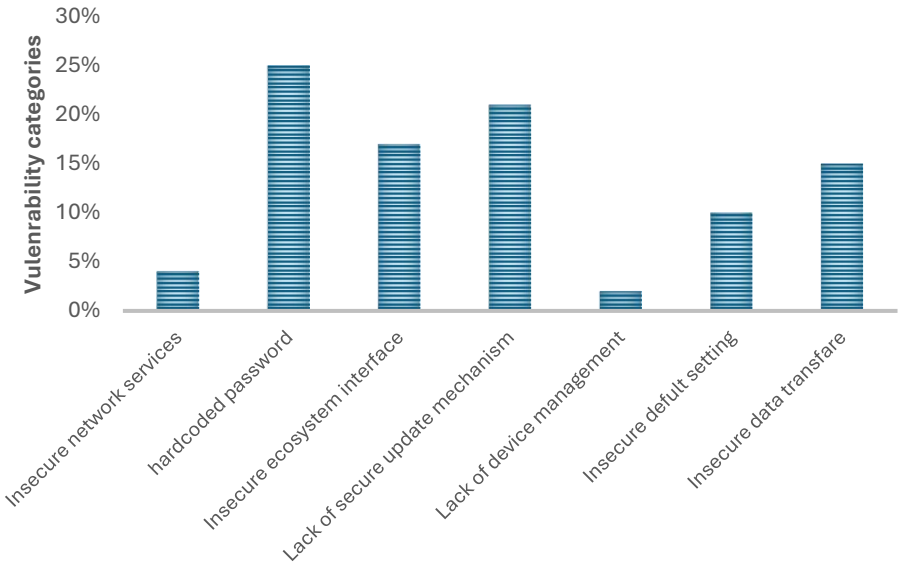

Figure 11. The vulnerability classes' criticality

Table 2. Sources utilized to handle IoT threat

Threats	Sources
Hardcoded, weak, or predictable passwords	[30, 31, 32, 33, 34, 35, 36, 37]
Services on insecure networks	[38, 39, 37, 40,37,41]
Insufficient physical hardening	[38, 39, 42]
Insecure default settings	[30, 39]
Insufficient secure update mechanisms	[38, 39, 42, 43, 44]
Usage of outmoded or insecure components	[38, 39]
inadequate privacy protection unsafe data storage and transfer	[38,39, 40]

Blockchain technology offers a wide range of benefits that significantly enhance the security posture of IoT systems. These advantages, documented across various domains in the existing literature, demonstrate blockchain's potential in transforming how data is protected, managed, and verified across distributed networks. While some studies concentrate on blockchain's general security benefits, others specifically evaluate its contributions to the IoT ecosystem, where the need for trustless, secure, and decentralized mechanisms is more pronounced due to the vast number of heterogeneous devices and their operational constraints. The key insights from these studies are elaborated in the following subsections, each outlining a distinct benefit of integrating blockchain with IoT. One of the key advantages of blockchain in IoT applications is the lack of reliance on central authorities or third parties. And with blockchain, since so much of it is decentralized, every IoT device can transact, validate data, and talk to all the other devices on its own. This prevents the necessity of an access point or an external server to control communication or confirm transactions, leaving a single point of failure there or improving system robustness [45].

These capabilities make IoT devices able to self-organize and communicate with each other in a trustless setting, freeing the development and deployment of new devices within already established networks. Second, the dependable IoT systems in the future can be more dynamic and self-managed, which can form connections dynamically without confirmation from the outside [40]. It also accelerates how quickly new products can be deployed by simplifying communication protocols and reducing reliance on centralized infrastructure. Thus, reducing the time-to-market of new IoT applications, which will result in faster and more agile production pipelines for manufacturing [41]. Furthermore, the device independence adds robustness to IoT ecosystems which can become more resilient to targeted cyber-attacks aimed at centralized control structures. Blockchain achieves a level of autonomy in the system because it distributes trust and processing tasks in the network and, as a result, enhances the security and dependability of the whole system.

Decentralization De-centralization is one of the most important aspects of the blockchain and is a critical element for the security, scalability and resiliency of IoT systems. Centralized designs like the ones often employed in IoT, where centralized servers or cloud infrastructure are used to control communication with devices, validate data, and store it. Although this architecture can be straightforward, it presents significant security risks, especially that single key weaknesses which are the single failure points, where a single central node breakdown or breach may cause the entire network to stop functioning incorrectly and lead to compromise of all users' data [15].

Decentralized type of blockchain removes such dependency, since both writing data and verification of that one is divided using P2P (Peer to Peer) network. This distributed nature has the advantage of preventing a single point of failure and it provides for system resiliency as well as redundancy as no one entity owns the data streams. The blockchain integrated Iot hosts a copy of the ledger across all nodes and empowers each of them to participate in validation eliminating fear of interference, data loss, or malpractices by centralized intermediary are held [32], [34], [39].

This is of particular importance in the IoT landscape, encompassing billions of devices operating independently on a large scale. Multi-source access (including distributed parallel, high throughput and simultaneous access) is an advantage inherent to decentralization, being a natural solution to bottlenecks imposed by a many-to-one communication flow often present in centralized systems [7], [10]. Accordingly, it facilitates efficient data communications and supports instant decisions at the edge of the network.

Furthermore, the inclusion of decentralized cloud storage using blockchain is an interesting alternative to traditional cloud backends. Not only are these decentralized storage designs scalable, but they are also secure by construction. With Secure On-prem your company reduces operational risks, secures sensitive IoT data, and lowers infrastructure costs by not depending on a third-party cloud provider. Like any P2P network, when the number of nodes participating in the blockchain network increases, the network's computing power and storage capacity grow simultaneously, thus the blockchain network also can be evolved in horizontal scale while maintaining performance and security [10], [12].

A side effect of decentralization is that deployment cycles can be faster because no lead time is needed and there are fewer infrastructure needs. No central controller is necessary, making it possible for IoT networks to self-organize, self-heal, and be always-on, there-by enabling true missions-critical operation in hostile or disconnected environments. The resulting flexibility makes decentralized blockchain systems especially interesting for mission-critical IoT applications, including smart grid, industrial automation, and remote sensing.

In conclusion, what does decentralization mean for blockchain-based IoT systems:

- Removes the points of failure,
- More scalable and resilient,
- Minimizes production and maintenance costs,
- It provides access to distributed and instantaneous data,
- Allows devices to autonomously and trustlessly coordinate.

These advantages together improve IoT network architecture and security, making a blockchain a revolutionary technology for future IoT ecosystems.

Integrity, authenticity and confidentiality of the transactions are the standards of developing blockchain-based IoUT. The most effective way to achieve secure and reliable transactions is the direct use of smart contracts – self-executing code stored on the blockchain which automatically implements previously agreed rules and logic among parties involved [15]. These contracts get rid of the need for middlemen (like agents, notaries, etc.), mitigate the risk of human error, and make sure that once the conditions for the contract get satisfied, they will automatically trigger the transaction previously programmed. For IoT, the use of smart contracts is an effective way to automate the process of sensor input verification, controlling access of devices and secure payments between machines.

To strengthen the privacy and non-repudiation of transaction data, the transaction is cryptographically signed when the transaction is stored in the blockchain [34]. Cutting edge cryptographic technologies--SHA-256 hashing for data integrity, and elliptic curve cryptography (ECC) for digital signatures—means any alteration of your data is detected and the whole system is compromised. This significantly reduces the ability of adversaries to tamper with transaction data unnoticed by the entire network.

In addition to those, to enhance security and privacy concerns, particularly in sensitive IoT applications such as healthcare or industrial monitoring, blockchain systems exploit public-private key cryptography to hide users numbers. Every

participating node is given a unique, one-time use public key which it uses as "pseudonymous identity" to make transactions. Such a procedure offers privacy on the blockchain by guaranteeing that on-chain transactions can be fully visible and traceable by the network, but the real-world identity of the user remains obfuscated (unless disclosure is desired) [40]. Having the public keys refreshed on a regular basis provides an extra level of security against linkage attacks, in which attackers try to associate multiple transactions to reveal user patterns and identities.

It is this confluence of automated logic enforcement (enabled by smart contracts), cryptographic protections (by way of encrypting and hashing) and anonymity (by means of key-based identity management) that creates a robust security architecture for blockchain-enabled IoT networks. It ensures secure, decentralized, and trusted machine-to-machine (M2M) communications, while reducing common cyber threats like the man-in-the-middle (MITM) attack, spoofing, and data tampering.

One of the main strengths of blockchain for distributed IoT is that it enables asynchronous communication, which is referred to as auto synchronization. In some conventional systems the other part of a transaction has to be online or in a responsive status when a transaction is engaged or executed. But in a blockchain context that constraint goes away. It is possible to go-ahead with transaction recording and authentication without such a recipient's real-time participation while the network is facilitated to survive and to operate with or without synchronous participation [5].

Such a capability is particularly advantageous in the context of IoT ecosystems, in which devices may temporarily lose connectivity, may be of low power, or can be offline for long periods. When a transaction begins, it is transmitted across the network, confirmed through consensual algorithms, and eternally written to the distributed ledger. All valid nodes in the network have access to the transaction data regardless of an active or offline status of the sender or receiver. Then the recipient can extract the related data from the blockchain ledger and synchronize at any appropriate time without losing or delaying any important information [42].

Technically, this auto synchronization is facilitated by the immutable and decentralized nature of the blockchain, that ensures that all involved nodes produce copies of the ledger in the same way. As every block includes in its hash the hash of its preceding block and all confirmed transactions, upon rejoining, each node can synchronize the blockchain by checking the most recent blocks' headers and syncing the copy of the chain stored at its site. In addition, this methodology improves fault tolerance and survivability in IoT networks. It's a way to decrease reliance on constant connectivity, which makes the system more hardened against node failures and network disruptions or when devices are offline. This is especially important in real-world environments, such as those with remotely located sensors, mobile vessels, or battery-powered IoT devices where network performance cannot be assumed.

To summarize, auto synchronization provides data persistence, operational elasticity and geo distributed query access in blockchain powered IoT infrastructures. It enables both devices and users to interact with the network asynchronously, mitigating the latency limits and enhancing accessibility of the distributed systems in general. Enforcing trust and guaranteeing legitimacy in IoT systems is a fundamental aspect for designing reliable, secure and resilient systems. The blockchain, with its private key-based cryptographic communication scheme and its immutable nature, makes both data integrity as well as node authentication possible.

Every player or thing in a blockchain-based IoT network is identified by a unique public/secret key pair. Only nodes that have been verified and authorized can request or accept transactions in this key-based identity system. As soon as it is verified and added to blockchain, a transaction is permanent and it cannot be changed, cancelled, or deleted. It is this immutable and tamper resistant aspect of the blockchain transactions that is central to the veracity of communication on the network [7, 10, 15].

Not only do you confirm identity and trust, but you benefit indirectly from the security model — all transactions are immutable and can be traced back to a cryptographically signed signature. This discourages bad actors from trying illegitimate access and manipulation, as any such fraudulent action would either be denied through the consensus mechanism, or would be immediately visible publicly on the ledger. Additionally, immutability provided by blockchain helps to prevent brute force attacks—such as those carried out by the Mirai botnet—that commonly use weak device credentials in order to access and take hold of IoT devices. Unauthorized nodes or compromised devices are unable to engage in communication on a blockchain without authentic cryptographic keys and in this way, such attacks become worthless.

Furthermore, the trust enabled through blockchain even preserves data confidence and privacy, especially when encryption is coupled with immutability. Taillib [43] argues that even if an eavesdropping attacker eavesdrops a communication

channel, the encryption of transaction data and the impossibility of modifying data in a non-repudiable way, will stop the attacker extracting any significant information or taking a step towards some action.

In conclusion, the blockchain supports the veracity and identity of devices in IoT systems by:

Secure: Enhanced through Public Key Infrastructure (PKI) for identity verification,

- Allowing to make irreversible and accountable transactions,
- Tamper proof and unauthorised communication prohibited,
- The ability to keep the secrets, protected from spying.

These properties make blockchain a strong security foundation for contemporary IoT systems, in which integrity, non-repudiation, and resistance to attack are key requirements.

The notion of privacy in blockchain-based IoT applications materializes as a combination of transparency and tamper-resistance within which all operations are transparently auditable, traceable but resistant against unauthorized tampering. All transactions are traceable and permanently engraved on the blockchain as well, timestamped, cryptographically signed and publicly visible to the authorized network users. This openness allows users transparency and accountability, where any interaction could be verified by any node in the system [5].

As the blockchain is an append only file, and each block is cryptographically linked to the last one, it's infeasible for an attacker to change any transaction without detection thanks to the compute requirement. This protocol design is successful in preventing Man-in-the-Middle (MitM) attacks on the communication network, if any adversary tries to modify the data in the communication channel. In the case of the client server model, MitM attacks are primarily due to Vulnerabilities in communication protocols or lack of adequate encryption. However, in a blockchain network, such tampering would be easily detected because of consensus validation and because the record is maintained at multiple nodes that all have synchronized copies of transaction history [5].

In addition, since all transactions are visible to all participating nodes, the network effectively acts as a kind of watchdog, bringing anomalies to the attention of participating nodes in real-time. If a doctored transaction were added, it either would have to match the hash, in which case the corresponding transaction would have to be altered, or else it would disrupt the block's structure. This cooperative checking increases the trustworthiness and reliability of the exchanged data in the IoT system [39].

Note that while transaction details are visible, the participants are pseudonymous due to cryptographic key-pair generation. This achieves a middle ground of openness and privacy in that transactions are visible and provable without leaking IOV or endpoint data.

To sum up, the flexibility blockchain technology provides in IoT applications allows:

- Traceable in terms of transparent and unalterable visible transaction records,
- MitM and tampering protection through a decentralized verification,
- Identifying thread anomalies at an early stage through joint monitoring,
- There are privacy protection features, such as pseudonymized identities.

This transparency plus confidentiality in two layers is fundamental not only for trust creation but also for secure operation in decentralized IoT networks. It can be accompanied with fractal devices [46, 47], diplexers [48] and cellular communication networks [49, 50].

5. Conclusions

The rapid development of the Internet of Things (IoT) has posed many severe security and privacy challenges with the consideration that IoT systems are decentralized, heterogeneous and resource limited. We started by reviewing the capabilities of blockchain and whether it can provide an efficient and scalable solution to address these challenges. By virtue of its unique properties (including being immutable, operating under a decentralized consensus, enabling cryptographic verification, and facilitating smart contract automation), blockchain is a promising platform to improve trust, security, and transparency of IoT networks.

In this paper, we investigated how different blockchain mechanisms handle critical IoT shortcomings such as resources constrained in computers, communication and attacks (DDoS, spoofing and data tampering). We particularly focused on

the analysis of blockchain-based frameworks that incorporate deep learning mechanisms for smart decision-taking and automatic security reinforcement. We compared existing implementations of blockchain and identified the trade-offs between performance, security, and scalability, which provides the means to determine what models are best for specific use-cases in IoT.

We also looked at the potential of smart contracts, auto synchronization, identity verification, and data provenance to support the development of secure blockchain-IoT. This review demonstrates that although blockchain technology brings many benefits for DL applications, the current solutions experience energy efficiency, transaction throughput and interoperability issues -even more than when employed in a massive way for large scale of distinctive IoT devices.

Blockchain and the IoT integration is still in its infancy and will require several further developments to demonstrate its value: A few of these requirements that need to be met in order to realize the potential include Splitting up high cost BC transactions, bringing down exponentially huge power consumption areas, and lowering computer memory usage.

Finally, blockchain, deep learning, and IoT confluence provide a solid base for secure, smart, and decentralized digital world. Further research and developments in this inter-disciplinary field will be crucial to realize its full potential in critical applications including healthcare, smart-cities, autonomous vehicles, and industrial control systems.

Declaration of competing interest

The authors declare that they have no known financial or non-financial competing interests in any material discussed in this paper.

Authors' contributions

Laith F. Jumma conceptualized the review framework, led the literature analysis on blockchain security protocols, and coordinated the overall manuscript preparation. Leila Sharifi conducted systematic reviews of IoT device vulnerabilities and contributed to the synthesis of deep-learning integration strategies. Parviz Rashidi performed critical evaluation of recent hybrid architectures, refined the technical sections, and oversaw citation accuracy and formatting. All authors contributed equally to the discussion, writing, and final approval of the manuscript.

Funding information

The authors declare that they have received no funding from any financial organization to conduct this research.

References

[1] S. Shin and Y. Seto, "Development of IoT security exercise contents for cyber security exercise system," in *Proc. 13th Int. Conf. Human System Interaction (HSI)*, 2020, pp. 1–6.

[2] A. Raj, K. Maji, and S. D. Shetty, "Ethereum for Internet of Things security," *Multimedia Tools Appl.*, vol. 80, no. 22, pp. 33779–33800, 2021. https://doi.org/ 10.1007/s11042-021-10715-4.

[3] F. Loukil, C. Ghedira-Guegan, K. Boukadi, A. N. Benharkat, and E. Benkhelifa, "Data privacy based on IoT device behavior control using blockchain," *ACM Trans. Internet Technol.*, vol. 21, no. 1, Jan. 2021. https://doi.org/ 10.1145/3424304.

[4] S. P. Gochhayat, E. Bandara, S. Shetty, and P. Foytik, "Yugala: Blockchain-based encrypted cloud storage for IoT data," in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 483–489. https://doi.org/ 10.1109/Blockchain.2019.00071.

[5] A. Arabo, I. Brown, and F. El-Moussa, "Privacy in the age of mobility and smart devices in smart homes," in *Proc. IEEE Int. Conf. Privacy, Security, Risk and Trust (PASSAT) and Int. Conf. Social Computing (SocialCom)*, 2012, pp. 819–826. https://doi.org/ 10.1109/SocialCom-PASSAT.2012.117.

[6] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart home IoT devices," in *Proc. IEEE 11th Int. Conf. Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015, pp. 163–167. https://doi.org/ 10.1109/WiMOB.2015.7347956.

[7] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014. https://doi.org/ 10.1007/s11276-014-0761-7.

[8] Y.-A. de Montjoye, E. Shmueli, S. S. Wang, and A. S. Pentland, "openPDS: Protecting the privacy of metadata through SafeAnswers," *PLoS One*, vol. 9, no. 7, 2014. https://doi.org/ 10.1371/journal.pone.0098790.

[9] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of Empowered IoT Users," in *Proc. IEEE 1st Int. Conf. Internet-of-Things Design and Implementation (IoTDI)*, 2016, pp. 13–24. https://doi.org/ 10.1109/IoTDI.2016.11.

[10] K. Sarpatwar et al., "Towards enabling trusted artificial intelligence via blockchain," in *Policy-based Autonomic Data Governance*, Berlin, Germany: Springer, 2019, pp. 137–153. https://doi.org/ 10.1007/978-3-030-17653-2_9.

[11] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 127–149, 2019. https://doi.org/ 10.1109/ACCESS.2018.2885763.

[12] B. Marr, "Artificial intelligence and blockchain: 3 major benefits of combining these two mega-trends," *Forbes*, Mar. 2018. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/03/02/artificial-intelligence-and-blockchain-3-major-benefits-of-combining-these-two-mega-trends/

[13] D. Campbell, "Combining AI and blockchain to push frontiers in healthcare," *Forbes*, Nov. 2018. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/11/20/combining-ai-and-blockchain-to-push-frontiers-in-healthcare/

[14] E. Castelló Ferrer, "The blockchain: A new framework for robotic swarm systems," *Adv. Intell. Syst. Comput.*, pp. 1037–1058, Oct. 2018. https://doi.org/ 10.1007/978-3-319-97982-3_90.

[15] K. Hassan, F. Tahir, M. Rehan, C. K. Ahn, and M. Chadli, "On relative-output feedback approach for group consensus of clusters of multiagent systems," *IEEE Trans. Ind. Electron.*, early access. https://doi.org/ 10.1109/TIE.2023.3245678.

[16] D. Magazzeni, P. McBurney, and W. Nash, "Validation and verification of smart contracts: A research agenda," *Computer*, vol. 50, no. 9, pp. 50–57, 2017. https://doi.org/ 10.1109/MC.2017.3641637.

[17] "Open source P2P digital currency." [Online]. Available: https://bitcoin.org

[18] D. D. Wood, "Ethereum: A secure decentralised generalised transaction ledger," 2014. [Online]. Available: https://ethereum.org

[19] T. T. A. Dinh et al., "BLOCKBENCH: A framework for analyzing private blockchains," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*, 2017, pp. 1085–1100. https://doi.org/ 10.1145/3035918.3064033.

[20] Z. Li et al., "Consortium blockchain for secure energy trading in industrial Internet-of-Things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3690–3700, 2018. https://doi.org/ 10.1109/TII.2018.2799527.

[21] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, 2017. https://doi.org/ 10.1145/3065386.

[22] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, 1997. https://doi.org/ 10.1162/neco.1997.9.8.1735.

[23] M. M. Bronstein, J. Bruna, Y. LeCun, A. Szlam, and P. Vandergheynst, "Geometric deep learning: Going beyond Euclidean data," *IEEE Signal Process. Mag.*, vol. 34, no. 4, pp. 18–42, 2017. https://doi.org/ 10.1109/MSP.2017.2693418.

[24] A. Merlina, "BlockML: A useful proof of work system based on machine learning tasks," in *Proc. 20th Int. Middleware Conf. Doctoral Symp.*, 2019. https://doi.org/ 10.1145/3366626.3368124.

[25] F. Bravo-Marquez, S. Reeves, and M. Ugarte, "Proof-of-learning: A blockchain consensus mechanism based on machine learning competitions," in *Proc. IEEE Int. Conf. Decentralized Applications and Infrastructures (DAPPCON)*, 2019, pp. 119–124. https://doi.org/ 10.1109/DAPPCON.2019.00025.

[26] R. W. Ahmad et al., "The role of blockchain technology in telehealth and telemedicine," *Int. J. Med. Inf.*, vol. 148, 2021. https://doi.org/ 10.1016/j.ijmedinf.2021.104399.

[27] C. Wang et al., "A survey: Applications of blockchain in the Internet of Vehicles," *EURASIP J. Wirel. Commun. Netw.*, vol. 2021, no. 1, pp. 1–16, 2021. https://doi.org/ 10.1186/s13638-021-01935-5.

[28] G. Dimitrakopoulos and P. Demestichas, "Intelligent transportation systems," *IEEE Veh. Technol. Mag.*, vol. 5, no. 1, pp. 77–84, 2010. https://doi.org/ 10.1109/MVT.2010.936622.

[29] J. Ni, K. Zhang, X. Lin, and X. Shen, "Privacy-preserving real-time navigation system using vehicular crowdsourcing," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, 2016. https://doi.org/10.1109/VTCFall.2016.7881133.

[30] O. I. Abiodun et al., "A review on the security of the Internet of Things: Challenges and solutions," *Wireless Pers. Commun.*, vol. 119, no. 3, pp. 2603–2637, Aug. 2021. https://doi.org/ 10.1007/s11277-021-08239-0.

[31] Z. Ahmed et al., "Identifying Mirai-exploitable vulnerabilities in IoT firmware through static analysis," in *Proc.*, Oct. 2020, pp. 1–5. https://doi.org/ 10.1109/ICCCNT49239.2020.9225526.

[32] J. Ali et al., "Blockchain-based smart-IoT trust zone measurement architecture," in *Proc.*, 2019, pp. 152–157. https://doi.org/ 10.1109/ICCCNT45670.2019.8944662.

[33] D. R. dos Santos, M. Dagrada, and E. Costante, "Leveraging operational technology and the Internet of Things to attack smart buildings," *J. Comput. Virol. Hacking Tech.*, vol. 17, no. 1, pp. 1–20, Mar. 2021. https://doi.org/10.1007/s11416-020-00365-2.

[34] X. Jiang, M. Lora, and S. Chattopadhyay, "An experimental analysis of security vulnerabilities in industrial IoT devices," *ACM Trans. Internet Technol.*, vol. 20, no. 2, May 2020. https://doi.org/ 10.1145/3386361.

[35] Y. Zhang, M. Liu, and X. Chen, "Blockchain-enabled privacy preservation in edge-based federated learning for IoT applications," *IEEE Internet Things J.*, vol. 12, no. 4, pp. 2101–2115, 2025. https://doi.org/ 10.1109/JIOT.2024.3334567.

[36] A. Jurcut et al., "Security considerations for Internet of Things: A survey," *SN Comput. Sci.*, vol. 1, no. 4, p. 193, Jun. 2020. https://doi.org/ 10.1007/s42979-020-00201-6.

[37] F. Xiao et al., "Vulhunter: A discovery for unknown bugs based on analysis for known patches in industry Internet of Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 8, pp. 267–279, 2020. https://doi.org/ 10.1109/TETC.2018.2886936.

[38] Y. Harbi et al., "A review of security in Internet of Things," *Wireless Pers. Commun.*, vol. 108, pp. 325–344, 2019. https://doi.org/ 10.1007/s11277-019-06376-2.

[39] D. Li, W. Shen, and Z. Wang, "A novel method of security verification for JTAG protection function," in *Proc. IEEE 19th Int. Conf. Software Quality, Reliability and Security Companion (QRS-C)*, 2019, pp. 487–492. https://doi.org/10.1109/QRS-C.2019.00100.

[40] R. Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in Internet of Things: A survey," *SN Appl. Sci.*, vol. 3, no. 1, p. 121, Jan. 2021. https://doi.org/ 10.1007/s42452-020-04041-9.

[41] M. Zubair et al., "Exploiting Bluetooth vulnerabilities in e-health IoT devices," *Assoc. Comput. Mach.*, 2019. [Online]. Available: https://dl.acm.org/doi/10.1145/3319535.3354262

[42] G. Bere, J. J. Ochoa, T. Kim, and I. R. Aenugu, "Blockchain-based firmware security check and recovery for battery management systems," in *Proc. IEEE Transportation Electrification Conf. Expo (ITEC)*, 2020, pp. 262–266. https://doi.org/ 10.1109/ITEC48692.2020.9161632.

[43] D. He et al., "Toward hybrid static-dynamic detection of vulnerabilities in IoT firmware," *IEEE Netw.*, vol. 35, no. 2, pp. 202–207, 2021. https://doi.org/ 10.1109/MNET.011.2000290.

[44] P. Sun, L. Garcia, G. Salles-Loustau, and S. Zonouz, "Hybrid firmware analysis for known mobile and IoT security vulnerabilities," in *Proc.*, Jun. 2020, pp. 373–384. https://doi.org/ 10.1109/SPW50608.2020.00084.

[45] A. Benjaminsson, "Blockchain applicability in IoT systems," M.S. thesis, Faculty of Computing, Blekinge Inst. Technol., Sweden, 2021.

[46]Y. S. Mezaal, H. T. Eyyuboglu, and J. K. Ali, "New dual band dual-mode microstrip patch bandpass filter designs based on Sierpinski fractal geometry," in 2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT), 2013. https://doi.org/10.1109/ACCT.2013.55

[47]Y. S. Mezaal, H. T. Eyyuboglu, and J. K. Ali, "Wide bandpass and narrow bandstop microstrip filters based on Hilbert fractal geometry: Design and simulation results," PLoS ONE, vol. 9, no. 12, p. e115412, Dec. 2014. https://doi.org/10.1371/journal.pone.0115412.

[48]K. Al-Majdi and Y. S. Mezaal, “New miniature narrow band microstrip diplexer for recent wireless communications,” Electronics, vol. 12, no. 3, p. 716, 2023. https://doi.org/10.3390/electronics12030716

[49]J. A. Aldhaibaini, A. Yahya, R. B. Ahmad, A. S. Md Zain, and M. K. Salman, “PERFORMANCE ANALYSIS OF TWO-WAY MULTI-USER WITH BALANCE TRANSMITTED POWER OF RELAY IN LTE-A CELLULAR NETWORKS,” Journal of Theoretical & Applied Information Technology, no. 2, 2013.

[50]J. A. Aldhaibani , M. Q. Mohammed , A. A. Mahmood and M. Sellab Hamza, “Development of wearable textile patch antenna 2.43 GHz for biomedical applications,” Int. J. Adv. Technol. Eng. Explor., vol. 11, no. 111, pp. 2394–7454, 2024.https://doi.org/10.19101/IJATEE.2023.10102312