Educational Administration: Theory and Practice
2024, 30(2), 1230-1244
ISSN: 2148-2403
https://kuey.net/

Research Article

Internet of Things (IoT) Current Research Challenges and Opportunities and Blockchain As A Potential Solution: A Review

Dinesh S.Tundalwar [1]*, Rashmi A. Pandhare[1], Mayuri A. Digalwar[2]

[1]*Department of Electronics & Communication Engineering, Indian Institute of Information Technology Nagpur,
Email: dineshtundalwar@yahoo.com, Email: rpandhare@iiitn.ac.in
[2]Department of Computer Science and Engineering, Indian Institute of Information Technology Nagpur, Email: mayuri@iiitn.ac.in

***Corresponding Author:** Dinesh S.Tundalwar
*Department of Electronics & Communication Engineering, Indian Institute of Information Technology Nagpur,
Email: dineshtundalwar@yahoo.com, Email: rpandhare@iiitn.ac.in

***Citation**:* Dinesh S.Tundalwar et al (2024), Internet of Things (IoT) Current Research Challenges and Opportunities and Blockchain As A Potential Solution: A Review, *Educational Administration: Theory and Practice*, *30*(2), 1230-1244
Doi: 10.53555/kuey.v30i2.4885

ARTICLE INFO	ABSTRACT

The Internet of Things (IoT) is transforming the physical and digital worlds. Our everyday objects are transformed into smart devices, from dustbins to toothbrushes. In spite of the IoT being relatively young, its growth is brisk. By 2025, it is expected that 80 billion IoT devices will be used in practice. This would not be possible without addressing the challenges associated with the IoT. By using a state-of-the-art survey, this paper explores recent research topics related to IoT, such as scalability, energy efficiency, M2M communications, communication protocols, interoperability, heterogeneity, security, and privacy. Survey results reveal that security and privacy are identified by the majority of researchers as major research challenges. Subsequently, this paper explores the recent security trends such as AES, DES, RSA, BLOWFISH, DH, SHA-1/SHA-256, NTRU, hybrid security techniques, fog computing, edge computing, software-defined networking, lightweight cryptography, homomorphic and searchable encryption, machine learning-based solutions, blockchain-based solutions, and IOTA. Blockchains are unique in their properties such as immutability, trust, privacy, integrity, and resiliency, which isolate the technology from other existing security solutions and place it among the potential security solutions among existing trends. In addition to this overview of blockchain technology, applications of blockchain in IoT and the architecture of IoT with blockchain are also presented. Finally, the challenges of integrating Blockchain technology with IoT such as scalability, security, the privacy of information, smart contracts, legal issues, throughput, latency, computational requirements, and storage with solutions were discussed, along with future directions of research while designing Blockchain-based IoT applications with low power consumption and high scalability.

Keywords: IoT, Scalability, Security, Privacy, Blockchain, IOTA, Smart Contracts, throughput, latency.

1. INTRODUCTION

The Internet of Things (IoT) is a network of devices that can sense, accumulate, and transfer data without human intervention. The Internet is a nucleus of IoT as it is a bridge between applications and IoT-based devices. Moreover, it's a platform that is not immune to security threats. All the applications exchange information through this platform, sometimes consisting of privacy-sensitive information. So, it is very important to provide rugged security to IoT-based devices to protect privacy-sensitive information from getting stolen by hackers and intruders. Security of IoT devices is indispensable as most of the subset of data involved in communication is sensitive to security and privacy, so it must be handled very carefully and need to protect from unauthorized body [1], [2]. Nowadays, data is of utmost importance in any field it belongs to since data is the new oil and needs to be protected from intruders and hackers, whether internal or external. A number of researchers have been experimenting with various security techniques like Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), BLOWFISH, Diffie–Hellman key exchange (DH), SHA-1/SHA-256, NTRU (Nth Degree Truncated Polynomial Ring Units), hybrid techniques for security in IoT, fog computing, edge computing, software-defined networking, lightweight cryptography, homomorphic and searchable encryption, machine learning-based solutions, to get rid of various security and privacy threats experienced by IoT devices, but they haven't been able to remove these threats completely[3][4]. As of late, researchers have looked into integrating distributed ledger technology like Blockchain and IOTA with IoT in order to combat privacy and security threats [1], [5], [6]. A blockchain is an immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later. Blockchain technology can be broken down into four main components, first is Consensus which ensures the genuine participants are included in the network, and the second is a ledger that stores the data flow within the network. Third, Cryptography ensures all data in the ledger or network is encrypted, and only authorized individuals can decrypt it. Fourth is a smart contract, Data flow in a network is regulated by this, as one should receive what data and how much of it [7]. Blockchain technology is characterized by features like peer-to-peer networks, decentralized, immutable, cryptographically secure, logs of data with a digital signature, transparency, traceability, and no third-party interference [8]. Researchers are exploring how to incorporate blockchain features into the IoT ecosystem in order to ensure better security and privacy for sensitive data. It is challenging for blockchain to integrate with IoT as IoT devices have resource constraints, i.e., they run on a battery and have limited storage, and processing power. An analysis of the recent challenges of IoT and the benefits of Blockchain as a potential solution to these challenges will be presented in this paper. Besides reviewing the challenges related to integrating blockchain and IoT, possible solutions are also discussed [8]–[11]. The main contributions of the paper are the survey on recent IoT challenges and the identification of the most addressed challenges through survey analysis. Also, an overview of recent security trends is provided, along with their strengths and weaknesses. Further, the blockchain's advantages over existing security techniques are discussed and then the complete overview of blockchain technology and its applications in IoT, along with a blockchain-based IoT architecture is presented. Finally, the open challenges of blockchain and IoT integration as well as their solutions are proposed. In this paper, section two discovers recent challenges in IoT and existing security trends using a state-of-the-art survey. Section three highlights the benefits of blockchain technology over existing security techniques. Further in section four, the overview of blockchain technology is discussed. The challenges of Integration of IoT and Blockchain technology with their solutions is communicated in section five. In section six, research directions are outlined that will be necessary in order to develop Blockchain-based IoT applications that consume low power and have high scalability. Finally, recapitulate the main points of the paper in section seven.

2. RELATED SURVEY

Research studies that address IoT technology challenges from recent years are presented in this section, and a summary of a few major research challenges is addressed in Table 1. Stankovic [1] outlined key areas of research in the internet of things as well as research problems within those areas. Additionally, eight thematic areas are identified for further research: massive scaling, architecture and dependencies, making knowledge and big data, robustness, openness, security, and privacy, and having humans in the loop. Sisinni et al. [2] pointed out that consumer applications, as well as industrial applications, can benefit from the internet of things. In addition, the challenges posed by energy efficiency, real-time performance, coexistence, interoperability, security, and privacy are discussed, and an overview of current research efforts and possible future research directions is provided. Hussein [12] uses IoT technology as a case study to highlight potential research applications and challenges in IoT research. A number of potential research areas were identified based on the case studies conducted, including Privacy and Security, Processing, Analysis, and Management of Data, Monitoring and Sensing, M2M (Machine to Machine) Communication and Communication Protocols, Blockchain of Things (BCoT): Fusion of Blockchain with the Internet of Things, and Interoperability. Goswami et al. [13] describe the history of the Internet of Things (IoT), its applications, challenges, and important issues in the present. Besides comparing various IoT communication protocols with their strengths and weaknesses, some other issues and challenges that the IoT architecture faces, such as standardization, architecture, scalability, and security, that must be addressed are also presented. Additional solutions are also provided to make the IoT architecture more stable, reliable, and secure. Zhang et al. [14] outline ten key areas for future research and examine the research problems and opportunities associated with these areas. In addition, Energy Harvesting, Data-driven IoT, IoT Search, Security, Privacy, Trust in IoT, Service Computing and IoT, Social IoT, IoT Recommendation, Edge Computing and, IoT, Conversational IoT, and Summarization in IoT are highlighted as potential research areas.

Dian et al. [15] highlighted the research conducted in the area of the wearable internet of things and its classification, and also outlined the advantages of cellular IoT and the usefulness it brings in the area of consumer application. Further, wearable sensors' resolution, power consumption, wearability, safety and security regulation, and privacy as IoT-enabled wearables are identified as challenges and future possibilities. Jayalaxmi et al. [16] discussed the role of the internet of things in the industrial revolution 4.0 to accelerate the industrial automation of internal and external working processes, including transport, manufacturing, and marketing units, with a number of connected devices. In addition, various security issues confronting the IIoT are provided with a comparative analysis of available solutions designed to enhance its protection system. Also, some open research problems are identified, including system integration, communication, energy factor, preventive and detective measures authorization, and architectural design for experts from different industries. Bhatt et al. [17] reviewed discrete IoT security challenges related to currently deployed IoT standards and protocols and presented a comprehensive review that examined how IoT security is emerging, including the identification of threats pertaining to the current IoT system, novel security protocols, and security projects presented in recent years that provide insight into the latest security trends and, therefore, are beneficial in developing IoT security. Additionally, recent research issues in IoT-(1) heterogeneity (2) inter-connectivity (3) ubiquitous nature (4) security standards are discussed. Also, provide information on the latest security trends that will be helpful in the development of IoT security. Furthermore, protocol-based attacks as well as data-based attacks were discussed as classifications of attacks.

Research challenges in IoT	Stankovic [1]	Sisinni et al. [2]	Hussein [12]	Goswami et al. [13]	Zhang et al. [14]	Dian et al. [15]	Jayalaxmi et al. [16]	Bhatt et al. [17]	Mao et al. [18]
Scalability	✓	-	-	✓	-	-	-	-	-
Architecture and Dependencies	✓	-	-	-	-	-	-	-	-
Creating Knowledge and Big Data	✓	-	-	-	-	-	-	-	-
Robustness	✓	-	-	-	-	-	-	-	-
Openness	✓	-	-	-	-	-	-	-	-
Security	✓	✓	✓	✓	✓	✓	-	✓	✓
Privacy	✓	✓	✓		✓		-		✓
Humans in The Loop	✓	-	-	-	-	-	-	-	-
Energy Efficiency/Power Consumption	-	✓	-	-	-	✓	✓	-	-
Real-Time Performance	-	✓	-	-	-	-	-	-	-
Coexistence	-	✓	-	-	-	-	-	-	-
Interoperability	-	✓	✓	-	-	-	-	-	-
Processing, Analysis, and Management of Data	-	-	✓	-	-	-	-	-	-
Monitoring and Sensing	-	-	✓	-	-	-	-	-	-
M2M Communication and Communication Protocols	-	-	✓	-	-	-	✓	-	-
Fusion of Blockchain And Internet of Things	-	-	✓	-	-	-	-	-	-
Standardization	-	-	-	✓	-	-	-	-	-
Architecture	-	-	-	✓	-	-	✓	-	-
Energy Harvesting	-	-	-	-	✓	-	-	-	-
Data-Driven IoT	-	-	-	-	✓	-	-	-	-
IoT Search	-	-	-	-	✓	-	-	-	-
Service Computing and IoT	-	-	-	-	✓	-	-	-	-
Social IoT	-	-	-	-	✓	-	-	-	-
IoT Recommendation	-	-	-	-	✓	-	-	-	-
Edge Computing and IoT	-	-	-	-	✓	-	-	-	-
Conversational IoT	-	-	-	-	✓	-	-	-	-
Summarization in IoT	-	-	-	-	✓	-	-	-	-
Data Resolution of Wearable Sensors	-	-	-	-	-	✓	-	-	-
Safety	-	-	-	-	-	✓	-	-	-
System Integration	-	-	-	-	-	-	-	-	-
Preventive and Detective Measures	-	-	-	-	-	-	✓	-	-
Authorization	-	-	-	-	-	-	✓	-	-
Heterogeneity Issue	-	-	-	-	-	-	-	✓	✓
Inter-Connectivity	-	-	-	-	-	-	-	✓	-
Ubiquitous Nature	-	-	-	-	-	-	-	✓	-

Table 1-Research challenges in IoT

Moreover, security models based on security requirements are proposed. Data encryption, fuzzy logic algorithms, multi-level data encryption, mathematical evaluation, blockchain-based authentication, cryptographic-based data encryption, and socket programming are all used in developing these models. Mao et al. [18] pointed out the significance of energy efficiency in the context of green IIoT and also highlighted that limited Energy efficiency is one of the most important research topics in green IIoT, as 1) limited resources can significantly affect the lifetime of IIoT systems and 2) massive sensors, devices, and machines keep consuming a considerable amount of energy, thus increasing the carbon footprint. Open issues and challenges like the coexistence of heterogeneous IIoT devices, handling of mobility in IIoT, 5G enabled IIoT, lightweight security, and privacy assurance, and edge intelligence for energy-efficient IIoT to make IIoT energy efficient are also addressed.

Based on the state-of-the-art survey data, Table 1 presents an overview of the challenges, opportunities, and directions that come along with the Internet of Things. From table 1, it is apparent that security and privacy are two challenges that have largely been addressed by researchers working in the field.

Real-time IoT applications generate a lot of data continuously, some of which contain confidential information, and so security and privacy represent two of the major challenges associated with IoT. Therefore, while implementing IoT applications that contain confidential information, the issues related to security and privacy need to be addressed. Thus, in this section, the survey extended to the resolution of privacy and security issues, as well as the exploration of recent security trends and techniques in IoT, as summarized in Table 2.

Srivastava et al. [3] provide a brief introduction to IoT Security and discuss various IoT Security Techniques such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), Rivest-Shamir-Adleman (RSA), BLOWFISH, Diffie–Hellman key exchange (DH), SHA-1/SHA-256, and also explain Hybrid Techniques used in IoT Security. Additionally, various IoT security techniques and hybrid IoT security techniques are compared. Harbi et al. [4] discussed current security risks at the perception, network, and application layers of the IoT architecture as well as a number of emerging security solutions like fog computing-based solutions, edge computing-based solutions, software-defined networking-based solutions, blockchain-based solutions, lightweight cryptography-based solutions, homomorphic and searchable encryption-based solutions, and machine learning-based solutions in brief. Moreover, the security challenges presented by the studied emerging technologies are also explored. Zhao et al. [5] and Bhandary et al. [6] propose an innovative way of enhancing the security and privacy of IoT devices using IOTA. By using the proposed solutions, this technology can solve problems with existing blockchain platforms. Uprety et al. [19] review a comprehensive survey of the different types of cyber-attacks on different IoT systems and also demonstrate how to combat these types of attacks using reinforcement learning and deep reinforcement learning. Furthermore, it provides a solid understanding of IoT security attacks and countermeasures using reinforcement learning. Moreover, the advantages and disadvantages of some research work relating to the security of IoT involving learning reinforcement are also addressed.

Table 2 below summarizes recent trends and techniques to address the security and privacy issues in the IoT. Security trends summarized in table 2 suggest that blockchain-based solutions for security and privacy have grown in popularity as they offer unique advantages over traditional data security technologies.

Recent security trends in IoT	Bhatt et al. [17]	Srivastava et al. [3]	Harbi et al. [4]	Singh et al. [7]	Strength	weakness
Fuzzy-Logic-Based Algorithmic Method	✓	-	-	-	Confidentiality, Trust	Integrity availability and Authenticity, Centralized
A Multi-Level Data Encryption Method	✓	-	-	-	Confidentiality, Integrity	Availability, Trust, Authenticity, Centralized
Mathematical Evaluation Method	✓	-	-	-	Availability, Trust	Confidentiality, Integrity, Authenticity, Centralized
Cryptographic-Based Data Encryption Method	✓	-	-	-	Integrity Authenticity	Confidentiality, Trust, Availability, Centralized
Socket Programming	✓	-	-	-	Confidentiality, Integrity, Authenticity	Availability, Trust, and Centralized
Advanced Encryption Standard	-	✓	-	-	Robust Security	Costly, Computation Complexity

(AES) Algorithm						
Data Encryption Standard (DES) Algorithm	✓	✓	-	-	Security	Computation Complexity, Centralized
Rivest-Shamir-Adleman (RSA) Algorithm	-	✓	-	-	Security	Slow, Computation Complexity, Centralized, Vulnerable to various attacks
Blowfish Algorithm	-	✓	-	-	Open-source, Fast, low memory usage	Authenticity, non-repudiation, Centralized
Diffie–Hellman Key Exchange (DH) Algorithm	-	✓	-	-	Robust Security	Authenticity, Vulnerable to various attacks, Centralized
Sha-1/Sha-256 Algorithm	-	✓	-	-	Security	Computation Complexity, Centralized
Fog Computing-Based Solutions	-	✓	✓	-	Authenticity, Confidentiality	Trust management, Centralized
Edge Computing-Based Solutions	-	-	✓	-	Access control, Authenticity, Privacy-preserving	Attack and fault resilience, Centralized
Software-Defined Networking-Based Solutions	-	-	✓	-	Security, Key management, Identity management	Scalability, Not Immune to all types of security threats, Centralized
Blockchain-Based Solutions	✓	-	✓	-	Access control, Authenticity, Trust Management, Decentralized	Computation Complexity, Privacy
Lightweight Cryptography-Based Solutions	-	-	✓	-	Authenticity, Confidentiality, Integrity	Key management
Homomorphic and Searchable Encryption-Based Solutions	-	-	✓	-	Privacy-preserving	Computation Complexity
Machine Learning-Based Solutions	-	-	✓	-	Anomaly detection, attack detection	Computation Complexity, Privacy
IOTA	-	-	-	✓	Trust Management, Scalability	Lack of Smart Contract system
Reinforcement Learning	-	-	-	-	Maximizes Performance	Efficiently learning with limited samples

Table 2- Recent Security trends in IoT

The following are some of the distinct advantages that blockchain-based security and privacy solutions have over traditional data security technologies:

a) Trust Management: Blockchain technology's major features such as decentralization, transparency, and traceability make trust management simpler. A consensus algorithm is one of the pillars of blockchain technology, which ensures trust management between the network's nodes. Managing trust in other existing technologies is very difficult, except for IOTA as it also belongs to a distributed ledger technology like blockchain.

b) Privacy through smart contracts: A blockchain network is a network in which every node has access to data. In such a model, privacy becomes an increasingly important issue, as privacy is an inherent right and should be protected. Blockchain technology assures privacy by means of smart contracts, which help to regulate how much and what data is received on the network. This exclusive feature only found in blockchain makes it unique from other technologies.

c) Data integrity: Because blockchain is immutable, the integrity of data stored on the network is guaranteed. Blockchain data is tamper-proof and accessing and modifying the data on the chain requires the consensus of the entire network. Immutability is a distinctive feature of distributed ledger technologies like blockchain and IOTA, and it is not available with other security techniques.

d) Resiliency of data: Data storage and security techniques applied to today's data have some direct or indirect relationship with centralization; there is always a concern of data loss because of various security threats, such as a DDoS attack or a DoS attack, which can lead to a single-point failure. It is possible for hackers and intruders to gain external access to a server and steal or alter data. This loss of data can have devastating consequences for applications that use real-time data, such as health wearables. Unlike centralized systems, the blockchain is decentralized, which means that all nodes have the same copies of data, limiting hacking and other types of external attacks. There is little or no risk of data loss since data remains the same across all nodes. As a result, blockchain-based data storage and security are ideal for storing critical information such as customer identities and real-time application data.

e) Reduced costs: Due to the decentralized nature of blockchain and the lack of involvement of a third party, the cost of the infrastructure is reduced. The benefits of blockchain technologies over other existing security techniques and technologies are summarized in Table 3 below.

Recent security trends in IoT	Trust Management	Privacy through a smart contract	The integrity of stored data	Resiliency of data	Reduced cost
Fuzzy-Logic-Based Algorithmic Method	x	x	x	x	x
A Multi-Level Data Encryption Method	x	x	x	x	x
Mathematical Evaluation Method	x	x	x	x	x
Cryptographic Based Data Encryption Method	x	x	x	x	x
Socket Programming	x	x	x	x	x
Advanced Encryption Standard (AES) Algorithm	x	x	x	x	x
Data Encryption Standard (DES) Algorithm	x	x	x	x	x
Rivest-Shamir-Adleman (RSA) Algorithm	x	x	x	x	x
Blowfish Algorithm	x	x	x	x	x
Diffie–Hellman Key Exchange (DH) Algorithm	x	x	x	x	x
Sha-1/Sha-256 Algorithm	x	x	x	x	x
Fog Computing-Based Solutions	x	x	x	x	x
Edge Computing-Based Solutions	x	x	x	x	x
Software-Defined Networking-Based Solutions	x	x	x	x	x
Blockchain-Based Solutions	✓	✓	✓	✓	✓
Lightweight Cryptography-Based Solutions	x	x	x	x	x
Homomorphic and Searchable Encryption-Based Solutions	x	x	x	x	x
Machine Learning-Based Solutions	x	x	x	x	x
IOTA	✓	x	✓	✓	✓
Reinforcement Learning	x	x	x	x	x

Table 3: Benefits of blockchain technologies over other existing security techniques and technologies

This benefit encourages IoT developers to integrate blockchain technology with the IoT to ensure security and privacy. An in-depth analysis is essential before integrating blockchain with IoT. The next section provides an overview of blockchain technology and its applications in IoT.

3. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Since technology such as IoT is rapidly evolving and growing, there are more chances of security threats of different kinds, which can potentially hinder its progress. Therefore, it needs to be addressed carefully. Currently, available security solutions are not adequate to address the underlying security issues of technology that is evolving so quickly. Blockchain technology has emerged as a potential solution for meeting the security needs of evolving technologies like the Internet of Things and can be a game-changer for securing IoT data [7]. There are many different types of players in a network, like commercial establishments, government or private bodies, or even individuals. Each has its own goals and does not trust one other. Cooperation between these actors benefits the overall society. When decentralized trustless networks exist, blockchain technology is an ideal solution. A blockchain is an immutable chain of data that can only be added to and can never be deleted or modified. Data cannot be deleted or modified after it has been added, and because there is no central database to keep track of them, everyone keeps a copy and processes the data locally. The blockchain ensures that every party has the same view of the chain at all times. Information is transparent to all, so everyone can check and verify it. In simple terms, a blockchain is a decentralized, immutable, append-only ledger.

3.1. Types of blockchain

Blockchain is classified into a public blockchain, private blockchain, consortium or federated blockchain, and consortium or federated blockchain based on properties such as consensus determination, read permission, immutability, efficiency, centralized, and consensus process [7], [20], [21].

3.1.1. Public blockchain: It is also known as a permissionless blockchain because anyone in the network can join or leave the network at any time. Bitcoin and Litecoin are popular examples of permissionless blockchains. Any node in the network is able to mine if it meets all computational requirements. Data on such a blockchain is nearly impossible to alter.

3.1.2. Private Blockchain: They are also known as permissioned blockchain. It belongs to one organization or enterprise. Depending on the requirements, the reading of the transaction may be public or limited to a few nodes. In a private blockchain, transactions are swifter because the network is centrally controlled. However, centralization also raises issues of trust, which are addressed in a public blockchain. Ripple is an example of a private blockchain.

3.1.3. Consortium or federated blockchain: Consortium or federated Blockchains only permit defined nodes to participate in the consensus process. Access to read and send may be public or restricted to a few verified nodes. It has very high efficiency compared to the public blockchain. Quorum, Hyper Ledger, and Corda are examples of consortiums or federated blockchains.

3.1.4. Pillars of blockchain technology

A blockchain is composed mainly of four components: consensus, ledger, cryptography, and smart contracts, which together form its infrastructure [7]. Fig.1 depicts the pillars of blockchain technology, which are considered to be the components of this technology.

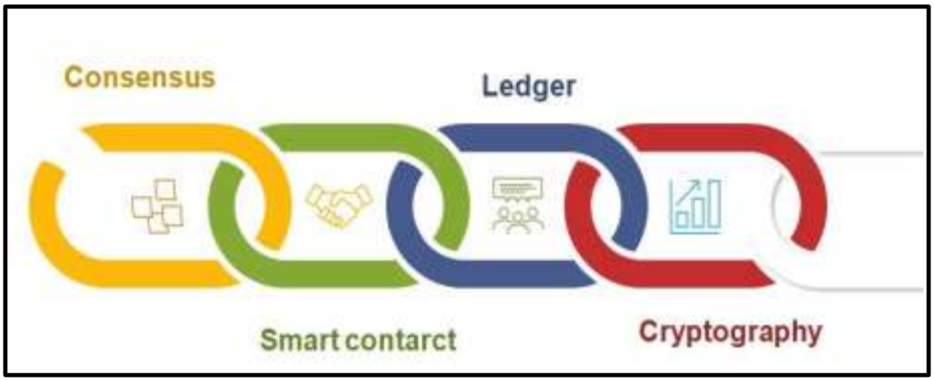

Figure 1: Pillars of blockchain technology

a) Consensus: In a trustless decentralization network like blockchain, where there is no central authority, any node wishing to add a block of data must have it first validated by the participating nodes, which is achieved through consensus. Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Burn (PoB), Proof of Capacity (PoC), Proof of Elapsed Time (PoET), etc. is some of the popular examples of the consensus algorithm.

b) Ledger: The technology uses an append-only ledger to provide a full transactional history. Unlike traditional databases, transactions and values in the ledger cannot be modified after they have been committed.

c) Cryptography: By utilizing cryptography, ensure that all transactions logged on the ledger are digitally signed, encrypted, and can only be decrypted by a verified node.

d) Smart contract: A blockchain network is a network in which every node has access to data. In such a model, privacy becomes an increasingly important issue, as privacy is an inherent right and should be protected. Blockchain technology assures privacy by means of smart contracts, which help to regulate how much and what data is received in the network. A smart contract is a program stored on the blockchain that runs when certain conditions are met. Privacy-sensitive data is not accessible to all nodes. Only nodes that are part of a smart contract can access this information. Smart contracts can be developed using Solidity language and viper.
These pillars of blockchain technology provide features like privacy, Security, transparency, traceability, decentralization, and immutability. These characteristics of blockchain technology can be combined with other technologies like IoT to alleviate the problems that arise due to its centralized nature.

4. APPLICATION OF BLOCKCHAIN IN IoT

As shown in Fig. 2, IoT has revolutionized the world by providing numerous applications such as smart cities, home automation, energy management, healthcare, and supply chain. Incorporating blockchain with IoT makes the technology even more secure, powerful, and attractive and attracts more investors to invest [22], [23]. The numerous applications have been exemplified as below.

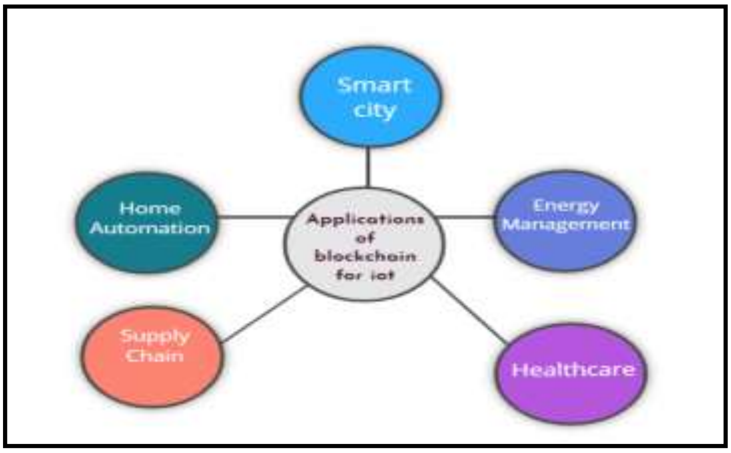

Figure 2: Application of blockchain in the Internet of Things (IoT)

4.1. Smart cities: Cities can become smart if they have a sensible, well-planned, and intelligent model to address all of the issues faced by residents, such as mobility of vehicles, energy management, waste disposal, and public administration. Using IoT and Blockchain, such a model is possible. The intelligent part is handled by IoT, whereas blockchain contributes to increased transparency, connectivity, security, data integrity, efficient management, and direct and secure communication between state agencies and the public [24].

4.2. Energy management: The blockchain records transactions between energy generators and consumers in a tamper-proof manner. As blockchain technology is decentralized, electricity can be traded between peers without a middleman, if any peers have excess energy, it can be sold to other peers using smart contracts [25].

4.3. Supply chain management: The main players in the supply chain are suppliers, manufacturers, carriers, retailers, and customers. The sharing of information and cooperation between these parties is always a major concern. These players can harness the Internet of Things to get real-time data and use it to share information and reduce costs in the supply chain. Nonetheless, the supply chain not only needs to gather the data but also ensure that the data is not leaked. The immutability, transparency, and traceability of the blockchain make it a perfect solution to these problems. In addition to this, a fine-grained data-sharing scheme for the supply chain is proposed [26].

4.4. Home automation: In recent years demand for home automation is on high. IoT is one of the reasons behind it. Home automation processing boards and related sensors are connected to each other, and these connections are gateway-centered. The gateway act as a bridge between the IoT cloud and devices, in smart homes, various IoT devices are connected to each other, and these connections are centered on gateways. Although gateways play a crucial role in smart homes, their centralized structure posed multiple security risks, including availability, certification, and integrity. Blockchain is a potential solution for such security vulnerabilities. Blockchain technology is implemented at the gateway layer to support decentralization and overcome the problems associated with traditional centralized architecture. Blockchain provides availability by authenticating network members and enabling efficient communication among them, ensuring the integrity of both internal and external data of the smart home. A blockchain-based smart home gateway network that prevents possible attacks on smart home gateways is proposed by [27].

4.5. Healthcare: Healthcare is the largest industry worldwide in terms of revenue and employment. Total healthcare expenditures account for about 9% of the world's GDP, which makes this an obvious target for hackers and intruders. Health wearables have evolved greatly since the introduction of IoT in healthcare, and that means healthcare data is being digitized at a rapid rate, just like data volumes in most other industries. Wearable IoT devices use cloud-based storage to store data gathered by sensors. For instance, a patient heart rate is read by a heartbeat sensor and sent to a server for diagnosis and tracking. Patients' health data stored on the cloud may be referred for paper assistance by different players in the healthcare industry, including doctors, nurses, administrative staff, Life/Health Insurance, Medical Researchers, lab pathologists, and Drug suppliers. If patient data is privacy sensitive, then one of these stakeholders has the potential to leak such information, these issues need to address carefully. Since the healthcare industry is decentralized and trustless, blockchain is a potential solution for preserving the privacy and security of sensitive health data. Blockchain technology can be used to store patient health data or records in a tamper-proof manner so that no one can alter them since blockchain is immutable. Smart contracts based on blockchain technology ensure the privacy of patient data by regulating how much and what data is received in the network [28].

Because of IoT's centralized nature, applications like Smart Cities, Energy Management, Supply Chain Management, Home automation, and Healthcare are facing issues such as privacy, security, integrity, and transparency. Therefore, blockchain is needed to integrate with IoT whose features can help to overcome these issues and make it more mainstream.

5. ARCHITECTURE OF IoT WITH BLOCKCHAIN

By leveraging the features offered by blockchain technology, integration of blockchain with IoT will help overcome some of the security vulnerabilities introduced by the centralized architecture of IoT [29], [30]. By introducing Blockchain technology as a fourth layer between the network layer and the application layer to the three-layer IoT architecture, the security issues can be addressed as shown in Fig.3.

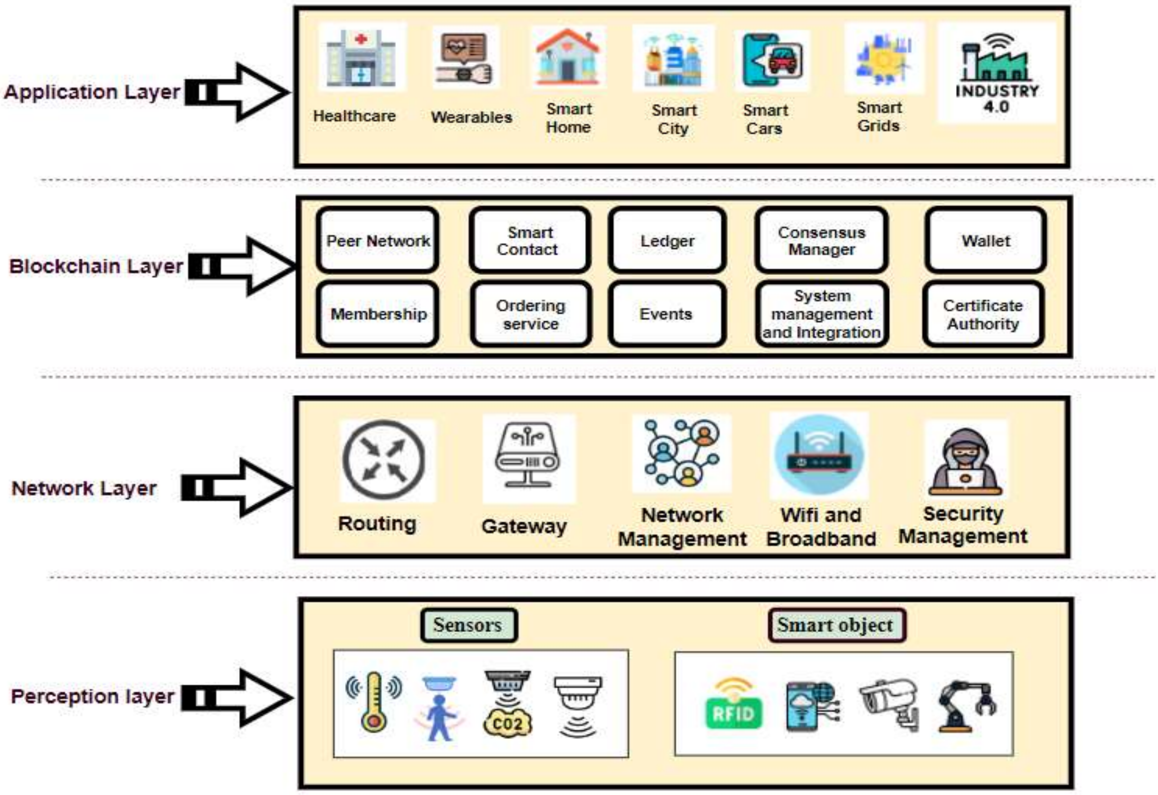

Figure 3: Architecture of IoT with blockchain

A basic 3-layer IoT architecture is comprised of a perception layer, network layer, and application layer. IoT primarily operates on these three layers.

5.1. Perception Layer: The perception layer, also referred to as the physical layer, is the first layer of three layers of the IoT architecture. In this layer, sensors, actuators, and smart objects are used to collect data such as temperature readings, motion detections, presence of gases, smoke and intruder's detections, etc. from the surrounding atmosphere and to pass this important data to higher layers for further processing and decision making.

5.2. Network Layer: An important role of the network layer is to connect the perception layer with the application layer. By using wired and wireless technology, the network layer transmits the sensory data collected from the perception layer to the application layer. This layer is primarily responsible for forwarding packets of data, routing them, as well as establishing logical connections, and reporting delivery errors.

5.3. Application layer: User interfaces or applications are the means by which a user is able to interact with a system. This layer contains all the necessary software to support user interaction and client applications. All the real-time IoT applications like healthcare, Wearable, Smart home, smart city, smart cars, smart grids, etc. will fetch the data from this layer.

In the IoT ecosystem, there are large chances of introducing security vulnerabilities during the communication between the network and application layers. The network layer delivers processed data to the application layer, where applications and consumers communicate and interact. To prevent security vulnerabilities from entering the application layer from the network layer, an additional layer needs to be placed between the network layer and the application layer. This shield prevents security vulnerabilities from entering the application layer from the network layer. In this case, the additional layer is referred to as a blockchain layer, since the various features of blockchain technology could serve as a shield to prevent security vulnerabilities from entering the IoT system. These features include peer network, ledger, smart contract, Consensus manager, wallet, membership, ordering service, events, system management, and integration and certificate authority. A peer network allows decentralized communication between IoT nodes, which eliminates the security threats that arise from centralized IoT systems. A blockchain ledger is one of the key features of the technology since it allows the record of transactions carried out between interconnected nodes and every node will have a copy of each transaction, so every node now has the same view of the data, making IoT nodes more transparent and traceable.

Furthermore, the immutable nature of the ledger also strengthens the integrity of the data by preventing it from being altered. Smart contracts are also among the most important components of blockchain technology that help to regulate how much and what data is received in the IoT network. A smart contract is a program stored on the blockchain that runs when certain conditions are met. Privacy-sensitive data is not accessible to all nodes. Only nodes that are part of a smart contract can access this information. A newly formed node can become part of an IoT network if it is validated by a consensus manager, which establishes trust between communicating nodes and thus prevents the entry of malicious nodes. Additionally, wallets, membership, ordering services, events, system management, integration, and certificate authorities all play roles in meeting security requirements. Thus, the integration of Blockchain with IoT is a potential solution to enhance the security and privacy of IoT systems.

6. CHALLENGES AND SOLUTIONS OF INTEGRATING TWO TECHNOLOGIES

As blockchain technology and the internet of things are two totally different technologies, integrating the two technologies will pose certain challenges that need to be addressed before the technology can be applied in practice. As shown in Fig.4, Among the major challenges were Scalability, Security, Privacy of Information, Smart contracts, Legal issues, throughput, latency, computational requirements, and storage[8]–[11], [31].

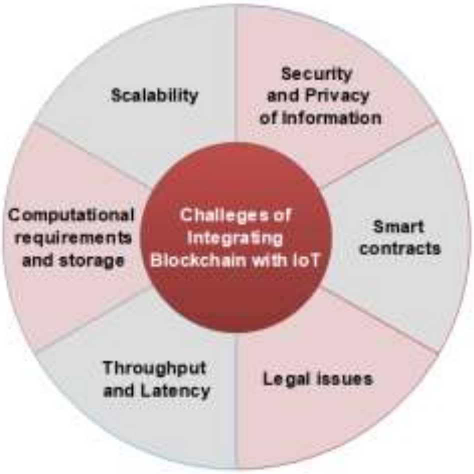
Scalability
Security and Privacy of Information
Computational requirements and storage
Challenges of Integrating Blockchain with IoT
Smart contracts
Throughput and Latency
Legal issues

Figure 4: Challenges of integrating Blockchain with IoT

Subsections focus on major challenges that arise from the integration of blockchain technology with the internet of things.

6.1. Scalability: In spite of the fact that IoT is a young technology and growing rapidly, it is predicted that 80 billion IoT devices will be deployed by 2025. Maintaining performance for such a continuously growing number of nodes is a challenge for blockchain technology. The scalability of the blockchain is limited by limitations related to hardware, transaction fees, block sizes, and response times. These factors inhibit the adoption of blockchain in IoT [32].

Solution: The selection of an IoT-friendly consensus algorithm is a potential way to address the issue of the scalability of the blockchain. The blockchain technology that powers Bitcoin is based on the Proof of Work (PoW) consensus algorithm, which is resource-intensive and has a low throughput that does not work well with IoT due to resource constraints. Therefore, it is important to look for IoT-friendly consensus algorithms**.** Salimitari et al. [33] Conducts a survey on various consensus protocols in IoT blockchain technology and presents their comparative analysis, which concludes that proof of elapsed time (PoET), Practical Byzantine Fault Tolerance (PBFT), and tangle are fully sustainable for the IoT environment. While PBFT has proved sustainable for IoT environments. Hao et al. [34] identified the disadvantages of PBFT along with the advantages, pointing out that PBFT does well in a static environment but doesn't keep up in a dynamic environment, and he proposes Dynamic PBFT as a solution**.** As explained in Feng et al. [35] work, in an asynchronous environment PBFT waiting time substantially increases and the communication level reaches O(n2) which has severe ramifications on the performance of permission blockchains. Furthermore, proposes a scalable dynamic multi-agent hierarchical PBFT algorithm (SDMA-PBFT) as a way to address the issue of PBFT in an asynchronous setting. Gao et al. [36] pointed out that PBFT, Honey Badger BFT, did not meet the scalability requirement in a large-scale network, and proposed a novel practical Byzantine fault tolerance consensus algorithm based on Eigen Trust, named T-PBFT, and compared it with PBFT and demonstrated that T-PBFT can optimize the Byzantine fault-tolerant rates. In addition to PoET, PBFT, and Tangle, Oyinloye et al. [37] discuss alternative protocols that are compared on the basis of Throughput, Scalability, Security, Energy consumption, and Finality that will be helpful for assessing which consensus algorithm would be suitable for IoT environments. Puthal et al. [38], and Maitra et al. [39] Present a novel consensus algorithm called Proof-of-Authentication (PoAH) to replace Proof-of-Work and implements this system to assess its applicability and sustainability for IoT and edge computing. Evaluations are carried out in simulation as well as on real-time testbeds.

6.2. Security and Privacy of Information: Although blockchain technology is immutable, several blockchain security issues can threaten its very existence. 51% attacks, Sybil attacks, Double-Spending attacks, Routing attacks, Security attacks, Selfish Mining attacks, and Vulnerable Smart Contacts are all threats to the blockchain that need to be addressed before using it in practice[8].

Solution: The 51% attack occurs when a group of malicious nodes obtains control over 51 % or more of the IoT network. In order to protect permissionless blockchains and open networks from 51% attacks, network sizes should be large enough so that it is difficult for attackers to take control of the network. When there are only a limited number of participating nodes in the IoT application, a permissioned blockchain is an ideal solution to prevent a 51% attack [7]. Many cryptocurrencies use a proof of work algorithm to prevent Sybil attacks. To combat double-spending attacks the mining pools of your blockchain must be monitored. Make sure that any pool exceeding 40% gets some of its miners diverted to other pools. The use of a secure routing protocol, especially one that has certificates, can help prevent blockchain routing attacks. It is imperative that smart contacts are rigorously tested for bugs by experts before they are implemented. Make your blockchain users aware of safe private key storage practices through emails, newsletters, etc. The privacy of information can be preserved in blockchain-based IoT systems by using strategies such as encryption, anonymization, Private Contract, Differential Privacy, and mixing [8]**.**

6.3. Smart contracts: A smart contract is a program stored on the blockchain that runs when certain conditions are met. Zou et al. [40] examine the biggest challenges developers face in developing smart contracts such as No effective method exists to guarantee smart contract code security, the development tools currently available are rudimentary, and There are still a number of limitations in programming languages and virtual machines, in resource-constrained environments, performance issues are difficult to solve, and a limited number of online resources are available.

Solution: It would be helpful for smart contract development if researchers and practitioners focused on conclusive and actionable topics such as automated smart contract patching, Solidity compiler testing, source code level gas optimization, automated Solidity library construction, etc. To further boost the development of smart contracts.

6.4. Legal issues: This new technology, called blockchain, has the potential to connect people from different parts of the globe without the necessity of following compliance laws, Manufacturers and service providers are both affected by this problem. Many businesses and applications will have difficulty adopting blockchain because of this challenge [41]**.**

Solution: The creation of regulatory laws by authorities and local administrative agencies is key to ensuring the best practices of blockchain in the IoT globally.

6.5. Throughput and Latency: Throughput and latency go hand in hand. Typically, throughput is measured by the number of successful transactions per second, while latency is the period of time between when a transaction is initiated and when it is ultimately completed. When the throughput is low, there are fewer transactions completed per second, which increases latency and may affect the performance of the application. For instance, Bitcoin, a proof of work (PoW) based currency, has only 3-7 transactions per second and the average transaction confirmation time is 60 minutes [32], it is far too low for IoT applications, especially real-time applications like healthcare, where an emergency is constantly looming around the corner. Low throughput and high latency can be caused by a large number of nodes waiting for verification and their energy demands as well as faulty nodes.

Solution: A possible solution could be the choice of a consensus algorithm that doesn't require complex computations, unlike Pow. According to Puthal et al. [38], a comparative study has been undertaken to evaluate the efficiency of Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Activity (PoA), and Proof-of-Authentication (PoAh) with regards to energy consumption, computation requirements, latency, and search space. The comparative analysis indicates that Proof-of-Authentication (PoAh) has the lowest energy consumption, computation requirement, and latency. Görkey et al. [42] present a comparative study of Byzantine Fault Tolerant Consensus Algorithms on Permissioned Blockchains implemented on different platforms to investigate the performance based on the number of validating nodes and throughput of the transactions block validation Time as shown in table 4.
By looking at table 4, it appears that anyone intending to develop IoT applications based on permissioned blockchains can choose Stellar-FBA or Ripple-FBA (RPCA) due to their high throughput and short block verification time. In the context of healthcare, Arul et al. [43] review the parallels of the blockchain-based consensus algorithm for IoT-based healthcare based on e-health, energy consumption, computation cost, throughput, application, scalability, latency, and leader selection as shown in table 5.

Implementation	Number of validating nodes	Transaction Throughput	Block Validation Time
Hyper ledger Fabricv1.0-PBFT	less than 200	200 TPS	4-26 sec
NEO-DBFT	7-1024	up to 1000 TPS	15-20 sec
Stellar-FBA	1000s of nodes	400 TPS	5-6 sec
RPCA	1000s of nodes	1500 TPS	3-5 sec
Parity-PoA	1000s of nodes	80 TPS	5-8 sec

Table 4- Comparative study of Byzantine Fault Tolerant Consensus Algorithms on Permissioned Blockchain implemented on different platforms.

Characteristics	PoW	PoS	DPoS	PoI	PBFT	PoET
e-health support	Medium	High	High	High	High	High
Energy Consumption	High	Medium	Medium	Medium	Low	High
Computation Cost	High	Low	Medium	Medium	Low	Low
Throughput	Low	Low	High	High	High	High
Application	Bitcoin	Ethereum	Bit share	NEM	Hyper ledger	Sawtooth
Scalability	High	High	High	High	Low	High
Latency	High	Medium	Medium	Medium	Low	Low
Leader Selection Based	Hash rate	Stake	Democratic method	Size of Transaction made	Voting Process	Random Timer System

Table 5- Characteristic based comparison of the consensus Algorithm

According to the table, if an IoT application requires low energy consumption and low latency, PBFT would be a good choice, while if the application demands scalability and low latency PoET may be the best choice.

6.6. Computational requirements and storage: Real-time IoT apps generate a massive volume of data, some of which are media, and to store such a large amount of information would require a lot of storage capacity. It is important to consider certain challenges while developing IoT applications that utilize blockchain as the storage mechanism. A blockchain block can only store up to 8MB of data, and even it charges for it, which inflates the implementation costs [44].

Solution: As an alternative to storing data on the chain, off-chain storage can be used, such as IPFS, which provides decentralized storage [28]. To ensure security and performance in off-chain storage, data should be stored in encrypted form and their hashes should be stored on the blockchain, which will consume less memory.

7. FUTURE DIRECTION

Although Blockchain technology can play a crucial role in the security and privacy preservation of confidential data in IoT applications, however, some future research directions should be taken into consideration before adopting blockchain in IoT applications. While designing a blockchain-based IoT application that demands Low energy consumption and high scalability at the same time both PBFT and PoET consensus algorithm alone could not serve this objective as PBFT has low energy consumption but has low scalability and PoET has high scalability but high energy consumption, hence a tradeoff between PBFT and PoET is required or a new consensus algorithm must be developed to meet this requirement. Blockchain and IoT-based real-time applications, such as health wearable and weather forecasting systems, in such applications, IoT devices need to continuously communicate with the blockchain to record and fetch the transaction for their desired execution, as most IoT devices are battery power and such continuous communication draws considerable battery power. In light of the fact that power consumption is a constraint of IoT devices, it needs to be monitored, and ways for limiting power usage during the communication of IoT and Blockchain must be found.

8. CONCLUSION

In this paper, the various research challenges in the internet of things in which security and privacy are mostly identified as researched challenges by the researcher are discussed. Furthermore, recent security trends to combat security and privacy threats are explored. In addition to this the advantages of blockchain over other emerging security trends, including trust management, privacy via smart contracts, the resiliency of data, and reduced costs, make it logical to choose blockchain as a security solution over other alternatives are communicated. Moreover, the integration of IoT with blockchain technologies and their challenges, such as scalability, security, privacy, smart contracts, legal issues, throughput, latency, computation requirements, and storage, along with their proposed solutions, were discussed. Finally, this paper concludes with future directions for aspiring researchers.

REFERENCES

[1] J. A. Stankovic, “Research directions for the internet of things,” *IEEE Internet Things J*, vol. 1, no. 1, pp. 3–9, 2014.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial internet of things: Challenges, opportunities, and directions,” *IEEE Trans Industr Inform*, vol. 14, no. 11, pp. 4724–4734, 2018.

[3] S. Srivastava and S. Prakash, “An Analysis of Various IoT Security Techniques: A Review,” in *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2020, pp. 355–362.

[4] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, “Recent Security Trends in Internet of Things: A Comprehensive Survey,” *IEEE Access*, 2021.

[5] L. Zhao and J. Yu, “Evaluating DAG-based blockchains for IoT,” in *2019 18th IEEE international conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science And Engineering (TrustCom/BigDataSE)*, 2019, pp. 507–513.

[6] M. Bhandary, M. Parmar, and D. Ambawade, “A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle,” in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 2020, pp. 827–832.

[7] M. Singh, A. Singh, and S. Kim, “Blockchain: A game changer for securing IoT data,” in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, 2018, pp. 51–55.

[8] M. U. Hassan, M. H. Rehmani, and J. Chen, “Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions,” *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[9] V. K. Aggarwal, N. Sharma, I. Kaushik, B. Bhushan, and others, “Integration of Blockchain and IoT (B-IoT): Architecture, Solutions, & Future Research Direction,” in *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1022, no. 1, p. 12103.

[10] T. Ahmed Teli, F. Masoodi, and R. Yousuf, “Security Concerns and Privacy Preservation in Blockchain based IoT Systems: Opportunities and Challenges,” 2020.

[11] A. Tandon, “Challenges of Integrating Blockchain with Internet of Things,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN*, pp. 2278–3075, 2019.

[12] A. R. H. Hussein, "Internet of things (IOT): Research challenges and future applications," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 6, pp. 77–82, 2019.

[13] S. A. Goswami, B. P. Padhya, and K. D. Patel, "Internet of Things: Applications, challenges and research issues," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, 2019, pp. 47–50.

[14] W. E. Zhang *et al.*, "The 10 research topics in the Internet of Things," in *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, 2020, pp. 34–43.

[15] F. J. Dian, R. Vahidnia, and A. Rahmati, "Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: A Survey," *IEEE Access*, vol. 8, pp. 69200–69211, 2020.

[16] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-H. Kim, "A taxonomy of security issues in Industrial Internet-of-Things: scoping review for existing solutions, future implications, and research challenges," *IEEE Access*, vol. 9, pp. 25344–25359, 2021.

[17] S. Bhatt, P. R. Ragiri, and others, "Security trends in Internet of Things: A survey," *SN Applied Sciences*, vol. 3, no. 1, pp. 1–14, 2021.

[18] W. Mao, Z. Zhao, Z. Chang, G. Min, and W. Gao, "Energy Efficient Industrial Internet of Things: Overview and Open issues," *IEEE Transactions on Industrial Informatics*, 2021.

[19] A. Uprety and D. B. Rawat, "Reinforcement learning for IoT security: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8693–8706, 2020.

[20] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (Big Data congress)*, 2017, pp. 557–564.

[21] H. Sheth and J. Dattani, "Overview of blockchain technology," *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146*, 2019.

[22] Z. Iftikhar *et al.*, "Privacy preservation in resource-constrained IoT devices using blockchain—A survey," *Electronics (Basel)*, vol. 10, no. 14, p. 1732, 2021.

[23] A. Abdelmaboud*et al.*, "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions," *Electronics (Basel)*, vol. 11, no. 4, p. 630, 2022.

[24] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *Journal of Network and Computer Applications*, vol. 181, p. 103007, 2021.

[25] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for Internet of Energy management: Review, solutions, and challenges," *Computer Communications*, vol. 151, pp. 395–418, 2020.

[26] Q. Wen, Y. Gao, Z. Chen, and D. Wu, "A blockchain-based data sharing scheme in the supply chain by IIoT," in *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*, 2019, pp. 695–700.

[27] Y. Lee, S. Rathore, J. H. Park, and J. H. Park, "A blockchain-based smart home gateway architecture for preventing data forgery," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1–14, 2020.

[28] S. Meisami, M. Beheshti-Atashgah, and M. R. Aref, "Using Blockchain to Achieve Decentralized Privacy In IoT Healthcare," *arXiv preprint arXiv:2109.14812*, 2021.

[29] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI," *Big Data and Cognitive Computing*, vol. 4, no. 4, p. 28, 2020.

[30] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–32, 2020.

[31] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021.

[32] S. Shahriar Hazari and Q. H. Mahmoud, "Improving transaction speed and scalability of blockchain systems via parallel proof of work," *Future Internet*, vol. 12, no. 8, p. 125, 2020.

[33] M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for iot networks," *arXiv preprint arXiv:1809.05613*, 2018.

[34] X. Hao, L. Yu, L. Zhiqiang, L. Zhen, and G. Dawu, "Dynamic practical byzantine fault tolerance," in *2018 IEEE Conference on Communications and Network Security (CNS)*, 2018, pp. 1–8.

[35] L. Feng, H. Zhang, Y. Chen, and L. Lou, "Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain," *Applied Sciences*, vol. 8, no. 10, p. 1919, 2018.

[36] S. Gao, T. Yu, J. Zhu, and W. Cai, "T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm," *China Communications*, vol. 16, no. 12, pp. 111–123, 2019.

[37] D. P. Oyinloye, J. senTeh, N. Jamil, and M. Alawida, "Blockchain Consensus: An Overview of Alternative Protocols," *Symmetry (Basel)*, vol. 13, no. 8, p. 1363, 2021.

[38] D. Puthal and S. P. Mohanty, "Proof of authentication: IoT-friendly blockchains," *IEEE Potentials*, vol. 38, no. 1, pp. 26–29, 2018.

[39] S. Maitra, V. P. Yanambaka, A. Abdelgawad, D. Puthal, and K. Yelamarthi, "Proof-of-Authentication Consensus Algorithm: Blockchain-based IoT Implementation," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, 2020, pp. 1–2.

[40] W. Zou *et al.*, “Smart contract development: Challenges and opportunities,” *IEEE Transactions on Software Engineering*, vol. 47, no. 10, pp. 2084–2106, 2019.

[41] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. B. Wills, “Blockchain with Internet of things: Benefits, challenges, and future directions.,” *International Journal of Intelligent Systems & Applications*, vol. 10, no. 6, 2018.

[42] I. Görkey, C. el Moussaoui, V. Wijdeveld, and E. Sennema, “Comparative Study of Byzantine Fault Tolerant Consensus Algorithms on Permissioned Blockchains,” 2020.

[43] P. Arul and S. Renuka, “Blockchain technology using consensus mechanism for IoT-based e-healthcare system,” in *IOP Conference Series: Materials Science and Engineering*, 2021, vol. 1055, no. 1, p. 12106.

[44] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, “Optimized blockchain model for internet of things based healthcare applications,” in *2019 42nd international conference on telecommunications and signal processing (TSP)*, 2019, pp. 135–139.