Computer Science Review 59 (2026) 100843

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

Intelligent IoT-Blockchain Ecosystem: A security perspective, applications, and challenges

Muralidhara Rao Patruni [a],*, Bhasker Bapuram [b], Saraswathi Pedada [c]

[a] Department of Computer Science and Engineering , and Cybersecurity, Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam, 530048, India
[b] School of Computing and Information Technology , REVA University, Bangalore, 560064, India
[c] Department of Computer Science and Engineering, GITAM School of Technology, GITAM Visakhapatnam, 530 045, India

ARTICLE INFO

Keywords:
Internet of Things
Industrial Internet of Things
Blockchain
Security and privacy
Authentication
Key management
Case study
And thematic analysis

ABSTRACT

Information and communications technologies (ICT) are vital in transforming the world with the advent of the intelligent information era. The lives of individuals in the 21st century are intertwined with smart living, encompassing smart cities, electronic health care, transportation, entertainment, and supply chain logistics that leverage service quality to provide a high-end user experience. The Internet of Things (IoT) and blockchain are potential solutions to contemporary problems, leveraging advancements in wireless communication technologies like 5G and 6G networks. Initially used for monitoring and controlling environmental changes, IoT has expanded to encompass every aspect of human life, enhancing our understanding of the world. This paper systematically studies state-of-the-art mechanisms, underlying technologies, research challenges, issues, and countermeasures to protect IoT environments using 6G technology. Also, we investigate possible security solutions with their performance measures to prove that the security solution is the best fit for the desired IoT environment. Lately, we emphasized future research views by considering 5G and 6G technologies that can help the sustainable development of the IoT-Blockchain ecosystem.

Contents

* Corresponding author.
E-mail addresses: patrunimuralidhar@gmail.com (M.R. Patruni), bhasker.b90@gmail.com (B. Bapuram), spedada@gitam.edu (S. Pedada).

https://doi.org/10.1016/j.cosrev.2025.100843
Received 17 January 2025; Received in revised form 25 September 2025; Accepted 12 October 2025
Available online 17 October 2025

1. Introduction

The Internet of Things (IoT) unexpectedly transforms business and consumer demands and drives toward a new industrial revolution. Nearly 20 billion IoT devices were connected to the Internet in late 2020. More than 30 billion IoT devices are predicted to be connected by the end of 2025 [1]. Today, IoT is a collection of huge network devices, including small sensors to large-scale visual sensors, smartphones, and drones connected to collect, process, and analyze the data to produce required solutions. The IoT global market is expanding its utilization everywhere globally, and it is predicted to reach ≈1855 billion US dollars in 2028 [2]. With the rapid development of telecommunication systems, the world has transformed from the Internet of Computers to the IoT. IoT can be a global network of interconnected devices uniquely identified and addressable based on standard protocols. On the other hand, the IoT is a network of physical devices with communication and computation capabilities to connect other devices. Of late, in today's

world, the creation of Internet applications is essential. It can be a difficult job, especially for researchers, to optimize Internet usage according to the level of application usage. In the past years, various definitions have been extracted from several organizations working in the IoT domain. Besides, IoT can be a collection of physical things embedded with sensors and actuators that have computational capabilities to communicate between the devices and systems [3,4].

The rapid growth of the IoT has led to the integration of billions of interconnected devices across critical sectors such as healthcare, energy, transportation, and smart cities. However, this exponential expansion has also introduced substantial security and privacy challenges due to the heterogeneous nature, constrained resources, and lack of unified security standards in IoT environments. IoT devices are particularly vulnerable to various cyber threats, including device impersonation, data tampering, unauthorized access, and large-scale Distributed Denial of Service (DDoS) attacks. For instance, the Mirai botnet exploited weak device credentials to launch high-impact DDoS attacks, disrupting major services globally. Moreover, insecure firmware updates and unencrypted communication make these devices susceptible to man-in-the-middle (MitM) and replay attacks. The dynamic and decentralized nature of IoT networks further complicates secure identity management and trust establishment among devices. Therefore, robust, scalable, and decentralized security frameworks are essential to address the multifaceted threats in modern IoT ecosystems.

With the rapid expansion of the IoT, secure integration is essential to enable seamless communication among smart devices. Wireless Sensor Networks (WSNs) play a crucial role within IoT, consisting of numerous nodes distributed across various locations that share similar functionalities and constraints. IoT sensor devices primarily focus on data collection, processing, and monitoring changes in the physical environment. As technology evolves swiftly, ensuring robust security for these devices becomes increasingly critical. Therefore, lightweight and secure authentication protocols are necessary to meet essential security goals such as confidentiality, integrity, availability, and authentication.

While 5G networks support a broad spectrum of Internet of Everything (IoE) services, they fall short of fulfilling the demands of emerging smart applications. This limitation has driven the exploration of 6G wireless communication technologies aimed at overcoming 5G's fundamental drawbacks. Incorporating artificial intelligence into 6G promises solutions to complex challenges in network optimization. Moreover, innovative technologies such as terahertz (THz) and quantum communications are being investigated to enhance future 6G capabilities. Ultimately, 6G networks will need to support the surge of data-intensive applications and an expanding user base.

Fig. 1 illustrates the evolutionary transition from traditional WSNs to the expansive IoT ecosystem. While WSNs primarily focus on localized sensing and data collection, IoT extends these capabilities by integrating diverse devices across heterogeneous networks, enabling complex applications such as smart homes, healthcare monitoring, and industrial automation. This figure highlights key technological advancements, including enhanced connectivity, scalability, and integration with cloud and blockchain technologies, which collectively underpin the modern IoT landscape.

Authentication mechanisms play a critical role in verifying the legitimacy of each node within an IoT system. This ensures that only authorized devices can participate in data exchange and access network resources, thereby enabling effective access control. By preventing unauthorized human intervention and malicious activities aimed at compromising devices or the network, these mechanisms help maintain the system's integrity. Consequently, robust security frameworks are essential to safeguard IoT networks against a wide range of threats and vulnerabilities, providing reliable protection without relying on manual oversight. Different cryptographic protocols are used to ensure system security. However, WSNs cannot support these traditional protocols due to limited computing power, memory, storage, and battery capacity. Thus, providing security because of the resource constraints of WSN is one most crucial research aspects in IoT environments. Therefore, various research studies have focused on efficient security protocols for WSNs. Indeed, the success of proposing the lightweight WSN depends on the clearness of sensor nodes.

Authentication techniques must meet common security and functional requirements, including mutual authentication, session secret key agreement, and user anonymity. Along with defenses against several well-known attacks, such as reply attacks, smart card fraud and loss attacks, password guessing and detection attacks, identity verification attacks, offline guessing attacks, sensor-node impersonation attacks, sensor capture attacks, man-in-the-middle attacks, and stolen verifier attacks. Therefore, as security becomes a challenging issue for WSN, the construction of security and efficient authentication schemes is highly demanded [5–8].

1.1. Communication standards

Since its inception in the late 1990s, IoT has brought remarkable services ranging from small-scale personal to large-scale industrial systems. For instance, while RFID supported the initial IoT system, contemporary IoT devices like smartphones and wearables can now connect to smart sensors installed in actual physical environments like smart homes, smart cities, and other related public and private environments. Of late, the emergence of sensing devices has become a key aspect in developing IoT environments [9]. It transforms from scalar sensing devices, including simple temperature, motion detection, and proximity sensors, to moderately computation-capable vector, gyroscope, and accelerometer sensors, to full, complicated multimedia sensors such as audio–visual, 3D-camera, and camera arrays. Besides, the advancement in networking capabilities has empowered the deployment of modern IoT systems comprised of multi-modal sensors for complex geographical monitoring for public safety, intelligent transportation, smart metering services, smart city projects, and smart industrial applications. The technological advancements in the application domains are yet challenging and enable numerous opportunities to tackle various issues related to sensing, networking, communication, storage, and analysis [10–17]. Table 1 depicts communication standards and protocols.

1.2. Blockchain enabled IoT

Cyber-Physical Systems (CPS) are essential for integrating networking, processing, and physical processes in IoT environments. Modern sensors can efficiently handle these systems, but become more susceptible to security issues. CPS aims to transition from traditional techniques to decentralized structures, implementing Industry 4.0 and Industrial Internet visions [18]. Deployment in industrial settings is crucial, and methods must be developed to ensure systems are ready for industrial use. Cyber attacks can target the CPS communication layer, leading to various attacks, such as replay, man-in-the-middle, impersonation, privileged insider, physical smart device capture, and ephemeral secret leakage. Blockchain (BC) is a novel technology that safeguards and executes transactions in a decentralized network without a centralized third-party system.

Blockchain technology, exemplified by platforms such as Bitcoin and Ethereum, has emerged as a robust solution for addressing security challenges in distributed systems by enabling secure communication, efficient processing, and reliable data storage. It maintains data on an immutable ledger that is accessible exclusively to authorized members within a permissioned network. When applied to IoT environments, blockchain enhances device security by ensuring controlled access, preventing data tampering, and reducing operational costs. By overcoming traditional technical limitations and eliminating centralized bottlenecks, blockchain enables autonomous device operation, reliable identity management, secure data preservation, and seamless peer-to-peer connectivity. This decentralized approach removes the need for

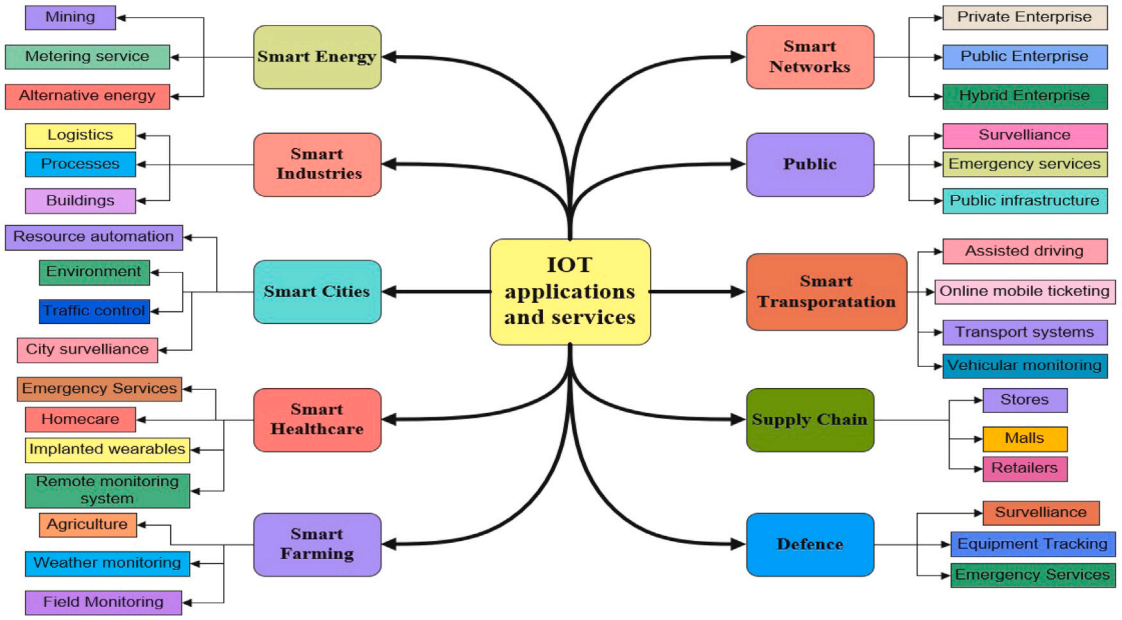

Fig. 1. IoT applications and services.

Table 1
Communication standards and associated protocols.

Standard body	Communication standard	Protocol	Frequency	Range	Data rate
IEEE	802.11n/ac/af	Wi-Fi	2.4 GHz/5 GHz/915 MHz	50–100 m	Up to 600 Mbps
	802.15.1	Bluetooth	2.4 GHz	10–100 m	1–3 Mbps
	802.15.4	ZigBee	2.4 GHz	10–100 m	250 kbps
		Thread	2.4 GHz	10–100 m	250 kbps
		MiWi	2.4 GHz	20–50 m	250 kbps
		6LoWPAN	2.4 GHz	Up to 100 m	250 kbps
ITU-T	G.9959	Z-Wave	868/908 MHz	30 m	100 kbps
Proprietary	LoRa alliance	LoRaWAN	433/868/915 MHz	2–15 km	0.3–50 kbps
	Sigfox SA	Sigfox	900 MHz	3–50 km	10–1000 bps
ISO/IEC	ISO/IEC 18 000 (LF)	RFID	120–150 kHz	10 cm	40 kbps
3GPP	5G NR (Release 16)	URLLC/mMTC/eMBB	sub-6 GHz, mmWave	Up to 1–10 km	Up to 10 Gbps

Abbreviations: URLLC: Ultra-Reliable Low-Latency Communication; mMTC: Massive Machine-Type Communication; eMBB: Enhanced Mobile Broadband; 5G NR: 5th Generation New Radio; 6LoWPAN: IPv6 over Low-Power Wireless Personal Area Networks; BLE: Bluetooth Low Energy; RFID: Radio Frequency Identification; LPWAN: Low Power Wide Area Network; SDO: Standards Development Organization.

intermediaries, thereby significantly lowering the cost and complexity of IoT deployment and maintenance. Overall, blockchain technology presents a promising framework for improving both the security and efficiency of IoT networks.

1.3. Blockchain layered approach

1.3.1. Network layer

Distributed ledger technology (DLT) is decentralized with different layers, including a network layer, protocol, and verification mechanism. It operates on a peer-to-peer (P2P) network, where users share resources without a central authority. Users can be classified into complete nodes and light/lightweight nodes. Full nodes carry out consensus rules, conduct mining, and store the entire ledger. Lightweight nodes support the network but cannot function as full ledgers. They act as transaction clients, keeping block headers current. DLT performance can be affected by block size, delay, speed, and propagation. Fig. 2 depicts the detailed layered architecture.

1.3.2. Consensus layer

The DLT stack includes consensus algorithms like PoW, PoS, DPoS, and PBST for validation and verification. PoW, also known as proof of work for Bitcoin, solves mathematical problems by competing between nodes to be the first. It generates a hash value and transmits it to another node, verifying its correctness. Ethereum also uses PoW, but its resource consumption is a drawback. Other proof-based algorithms include proof-of-stack and DPoS. Practical Byzantine Fault Tolerance (PBFT) was introduced to handle Byzantine replicas. It consists of three stages: prepare, prepare, and commit. PBFT partially trusts nodes, making it useful in Hyperledger Fabric, a popular example of this consensus algorithm. However, it has limitations in terms of computing resources.

1.3.3. Data layer

The physical layer of blockchain, or DLT, stores data in blocks connected in a chain form. It includes block data structure, digital signature, DAG data structure, Merkle root tree, time stamp, and cryptography. The Merkle tree structure records transactions and generates hash values. BC's decentralization prevents data tampering but consumes more energy and takes longer to process. This layer is accessible through full nodes.

1.3.4. Execution layer

It is a run-time environment. The compilers, Virtual Machines (VMs) and containers are installed on nodes. In this layer, the smart contracts are for trust. Smart contracts run at each node and VM in the network.

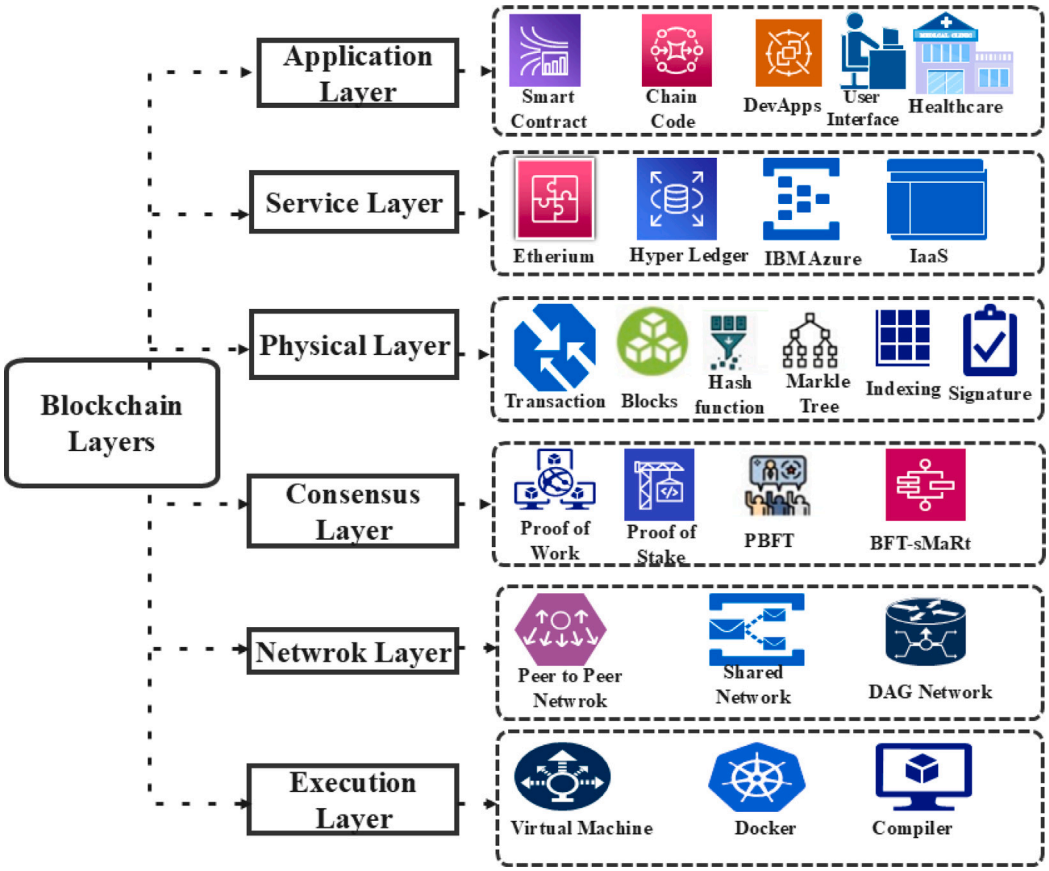

Fig. 2. Blockchain layered architecture.

The limitation of smart contracts is the wastage of computing resources and the abortion of transactions.

1.3.5. Service layer

The Service layer includes Ethereum, Hyperledger, and IBM Azure BaaS. The application allows users to access the information securely. It encompass blockchain platforms such as Ethereum, Hyperledger Fabric, and IBM Azure Blockchain-as-a-Service (BaaS), each offering essential tools and infrastructure for deploying decentralized applications (DApps) in IoT environments. Ethereum provides a public, Turing-complete platform for executing smart contracts, whereas Hyperledger Fabric offers a permissioned blockchain framework tailored for enterprise-grade, private transactions with modular architecture. IBM Azure BaaS further abstracts blockchain deployment complexities by providing scalable, managed services that integrate blockchain networks with cloud-based IoT infrastructure.

At the *Application Layer*, end-users interact with the system to securely access, retrieve, or share data collected by IoT devices. This layer ensures that data exchange remains encrypted, authenticated, and tamper-proof, leveraging underlying blockchain protocols to guarantee trust, traceability, and access control across diverse IoT services.

1.3.6. Application layer

The top layer of DLT connects decentralized applications to the underlying BC, with Bitcoin being the most popular application. The cryptocurrency ecosystem includes software like crypto wallets and smart contracts in turn offer, verify, and enforce contract execution. BC relevance extends beyond cryptocurrencies to IoT applications like intelligent automobiles, healthcare, agriculture, and cities. Smart contracts are self-executing programs with predefined rules encoded on the blockchain that automatically enforce and verify agreements without the need for intermediaries. They enable automated, transparent, and tamper-proof transactions, which are especially beneficial in IoT ecosystems for managing device interactions and access control. However, smart contracts also have limitations, including vulnerabilities to coding bugs, lack of flexibility once deployed, and challenges related to scalability and privacy. These constraints necessitate careful design, formal verification, and ongoing research to ensure their secure and efficient deployment in IoT applications [4,19].

1.4. Design issues and challenges

Many industries and applications are finding new uses for BC and Cyber Physical Systems (CPS). The complexity of Smart Contracts makes it hard to find reliable ones that last a long time for different smart applications. Gupta et al. [19] conducted a systematic review on smart contracts, BC and Artificial Intelligence(AI)-integrated platforms. Then, the security holes in SC code are looked into, along with possible fixes that can be made using well-known security systems like ZKP, TEE, and Secure Multi-Party Computation [20,21].

The transmission and processing costs of these methods are considerable. Then, we review how AI can be integrated into SC to address the difficulties outlined before. This systematic study addressed open difficulties and research challenges related to SC and AI integration issues. [22] proposes an attribute-based searchable encryption (ABSE) scheme. The computational cost of an ABSE scheme is handled by running the operations that require a lot of computing power on the BC network. The computational costs of the ABSE scheme are taken care of by running its operations, which require a lot of computing power on the BC network.

Mei et al. [23] devised a secure and effective authentication method that protects privacy and uses BC. This method allows for complete anonymity and checks the integrity of data batches while making key

management easier. Several authors [24–26] suggested an authentication method that protects privacy using lightweight cryptography to create a pairing-free ring cryptographic algorithm. This method uses fewer cloud–edge computing resources in the transportation of CPS. BC authentication provides more trustworthy service information for vehicular communication.

1.4.1. Security and privacy

Security and privacy are foundational concerns in the design of IoT-Blockchain systems, particularly due to the distributed nature of these networks and the sensitivity of data generated by IoT devices. As these systems operate over potentially untrusted environments, it is essential to address key challenges such as secure authentication, confidentiality, data integrity, resistance to tampering, and user anonymity. This section discusses how blockchain-based protocols can address these concerns while also highlighting their limitations and areas requiring further research.

Blockchain is a public, legitimate, and secure distributed processing system where all network users can access collected data. As IoT sensor-based devices grow, this creates some Security and privacy issues. Gupta et al. [19] proposed integrating BC with the IoT and artificial intelligence (AI). It gives researchers a lot to think about. It is hard to keep a user's private information private. Blockchain technology offers strong guarantees for data integrity and traceability, making it a valuable tool for enhancing security in IoT ecosystems. However, privacy remains a major challenge, especially in public blockchain systems where all transactions are visible to network participants. It is also evident that not all blockchain systems are public; permissioned and private blockchains exist, such as Hyperledger Fabric and Quorum, where access to data and participation in consensus are restricted to authorized entities. These models are more suitable for enterprise and IoT applications that require fine-grained access control and regulatory compliance. Security threats such as data leakage, device spoofing, and replay attacks must be countered using a combination of cryptographic methods, authentication protocols, and privacy-preserving blockchain mechanisms.

1.4.2. Scalability

BC platforms currently have significant latencies when dealing with many transactions. The Ethereum platform, for instance, can process 12 transactions per second, while the Bitcoin platform can only handle four. BC transactions can be made faster using sidechains. Few BC platforms, like Algorand and IoTA, improve how mining nodes reach a consensus to make them work better than existing ones. While transaction throughput (measured in transactions per second, or TPS) is one component of scalability, other factors such as latency, network size, and consensus efficiency also play critical roles. For instance, Bitcoin supports approximately 7 TPS and Ethereum about 30 TPS under default settings, which may be inadequate for large-scale IoT deployments. Permissioned blockchains like Hyperledger Fabric can offer significantly higher throughput and use more efficient consensus protocols [27].

In Proof-of-Work (PoW) based blockchain systems such as Bitcoin, security is closely tied to hashing power, as consensus relies on the computational difficulty of solving cryptographic puzzles. A critical vulnerability in PoW is the risk of a 51% attack, where an adversary controlling the majority of hashing power can manipulate the ledger, double-spend transactions, or exclude legitimate nodes. However, this vulnerability is specific to PoW; alternative consensus mechanisms such as Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Proof-of-Authority (PoA) mitigate this issue by replacing computational effort with stake, reputation, or identity-based validation [28].

1.4.3. Vulnerabilities

Secure SC-based apps are challenging to create without bugs, as source code and network data can be lost due to SC programming flaws. In 2016, hackers exploited a flaw in the Decentralized Autonomous Organization (DAO) code to steal 3.6 million ether. Testing SCs for defects or vulnerabilities is crucial, and methods have been developed to assess security states. However, the results of executing a smart contract are known in advance. This can pose a problem for decentralized AI, where mining nodes run SCs for machine learning and decision-making, resulting in random or unpredictable outcomes.

1.4.4. Cyber-attacks

Blockchain technology provides robust and secure IoT and AI architectures. These architectures are very prone to attacks. The main security algorithm in BC is the consensus algorithm, which any miner can break with more hashing power. The foundation of the decentralized system will be more mining power, with more miners farming at greater hash rates. The severity of this security issue is more pronounced in open blockchains like Bitcoin and Ethereum. Private BC platforms will be less affected by this problem because participants have already agreed on how to reach a consensus. The consequences of execution can be tampered with in a remote BC, similar to Hyperledger.

1.4.5. Overcharging

When there are dead codes, costly operations in loops, recursion, etc., the smart contract code is not well optimized. Given all the regulations that render sophisticated smart contracts ineffective, developers must exercise caution when creating them.

1.4.6. Correctness

A smart contract created and implemented on BC cannot be changed because it is kept on the BC network and possesses immutability. Before implementing a smart contract into the BC network, it is critical to assess its correctness. Verifying the accuracy of the rather long and sophisticated smart contracts is difficult for a smart contract development team.

1.4.7. Efficiency

In important applications like healthcare and financial systems, the speed at which a smart contract is carried out is very important. A smart contract can get information (shared information) from other smart contracts in the same way. Smart contracts must work well for this to work; otherwise, a deadlock could happen.

1.4.8. Standardization

The most difficult aspects of developing smart contracts are uniformity and social acceptance. Smart contracts can be standardized to boost their acceptability among BC-based systems worldwide. However, standardizing smart contracts is a time-consuming and complex procedure.

1.5. Recent works

The adoption of blockchain technologies in IoT application domains is covered in this subsection's discussion of recent surveys, mostly focused on security and privacy. The title of a survey article by Ratta et al. [29] "Applications of BC and IoT in the e-Health domain". In their research, the use of IoT and BC in the medical industry is assessed in connection with three crucial areas: remote patient monitoring, drug tracing, and medical record management. The difficulties of incorporating BC and IoT into healthcare systems are finally covered.

Rao et al. [30] and De Alwis et al. [31] examined the potential privacy and security threats of smart city IoT applications and industries in a comprehensive study. To evaluate the authentication and key management solutions put in place to protect Industrial IoT ecosystems, the authors relied on a thematic classification of security and privacy

problems. To illuminate the conceivable futures of smart cities/industries, they comprehensively review potential security threats, methods, countermeasures, and technology.

Zheng et al. [32] offered an in-depth review of prior research, a list of appropriate BC simulators, and a few untested simulators that might be able to simulate BC networks in an IoT setting. They also investigated a total of 18 BC simulators.

Rahman et al. [33] survey thoroughly investigates the new BC applications in healthcare. The authors provide an overview of the uses, research challenges, security risks, research possibilities, and future potential of BC technologies in an IoT-enabled healthcare system where BC protects the confidentiality and privacy of past and present medical data.

Adhere et al. [34] published a systematic review on BC in healthcare and IoT. This research analyses current market trends and focuses on the potential benefits of adopting BC in the Internet of Things and healthcare. According to the literature, BC is most frequently used in the IoT and healthcare sectors to ensure data security, including data integrity, access management, and privacy protection.

Recently, [35] published a comprehensive review article on BC in IIoT. This research systematically analyzed and discussed various advantages and disadvantages for future research.

Shahidine et al. [36] published a review article on BC in IoT to address security issues. The authors proposed a blockchain-based IoMT Authenticated Key Exchange (BIoMTAKE) protocol and used Hyperledger Fabric and cryptography libraries for performance analysis. Single trusted authority issues and vulnerability to security threats in wireless communication channels are open research problems for researchers.

To fully understand blockchain systems, this article by Xu et al. and Alghamdi et al. [27,37] reviews common blockchain systems at the macro level and examines a generic blockchain architecture and its fundamental components at the micro level. And discussed various security challenges in IoT.

This systematic review examines IoT BC-TMSs (blockchain-based trust management) by Liu et al. [38]. The authors defined good TMS criteria first. After developing a TMS taxonomy, the authors checked BC-TMSs in IoT using the criteria to compare past efforts. After the study, the authors identify outstanding issues and suggest future research subjects for decentralized, trustworthy IoT research.

Khan et al. [39] have systematically reviewed security and privacy issues in BC-IoT for healthcare applications. Discussed various possible attacks that are present but not addressed.

However, there are several surveys and review articles, most of which could not cover all the aspects of integrating IoT and BC environments. Besides, most existing survey articles focused on specific applications or generic views of adopting secure BC capabilities. Considering the surveys above and their potential for review, we thus organized our review paper with the scope and contributions listed below.

1.6. Motivation and contributions

Integrating IoT devices with blockchain technology is a promising solution to address security, privacy, data integrity, and interoperability issues in IoT ecosystems. This decentralized approach enhances trust, transparency, and efficiency across diverse IoT applications. This survey paper aims to provide insights into the current research, development, and deployment of IoT blockchain systems in industries like healthcare, supply chain, smart cities, and agriculture. Despite the growing interest, there is a need to understand key aspects of IoT blockchain systems. We intended to construct the review article with the following contributions:

(1) Presents a systematic review and global view of the most recent, relevant, and representative research progress in the IoT-BC ecosystem.

Fig. 3. Structure of the paper.

(2) Reviewed research works using a systematic case-study approach focusing on security and privacy in various IoT and industrial IoT application domains

(3) Designed a systematic case-study approach focusing on security and privacy in various IoT and industrial IoT application domains. A thorough discussion of the case-study model builds an intuitive and broad way of understanding security and privacy aspects in the IoT-BC ecosystem.

(4) Depicted a conceptual architecture to explore the components and layers of the IoT-BC ecosystem, including devices, services, key authentication, end-user applications, intermediate data processing units, storage units, and a few others.

(5) To understand and identify security issues, vulnerabilities, challenges, and possible countermeasures, this survey helps researchers to know existing security mechanisms, including authentication and key agreement, performance evaluations, simulation tools and environments, threat models, challenges, and future directions in advanced IoT-enabled blockchain environments.

1.7. Structure of the paper

Fig. 3 depicts the paper structure that intuitively depicts the entire article. We presented a background and rigorous review of related works in Section 2. We reviewed detailed security and privacy concerns and provided a thematic analysis of several existing schemes using a case-study model in Section 3. We proposed a conceptual architecture to explore the components and layers to emphasize the behavior of the IoT-BC ecosystem in Section 4. Then, we presented an analytical method to understand potential vulnerabilities and possible attacks and summarize existing security solutions in Section 5. Later, we systematically evaluated the performance analysis of the existing security solutions in Section 6. We then discussed the future scope for enabling 5G and 6G technologies to ensure the high-performance,

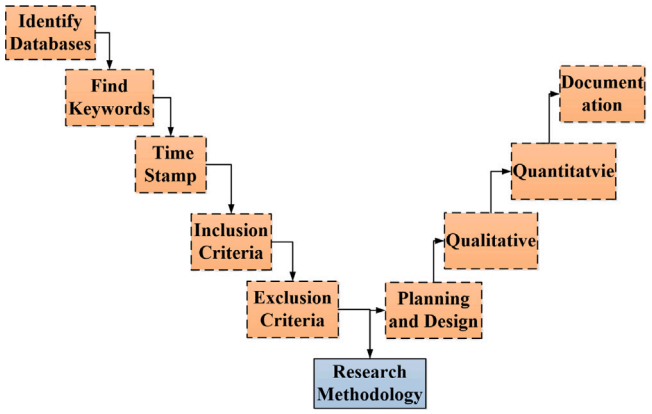

Fig. 4. Research method.

reliable, secure communication and data transmission for the IoT-BC ecosystem depicted in Section 7. Section 8 concludes with a research summary.

2. Background and related works

Industry and academia have paid little attention to research trends, but they are driving the IoT-led digital transformation. IoT establishes a wide range of global connectivity, AI manages decision-making, and Edge involves local processing and enhances processing capabilities. On the other hand, security issues and adversarial capabilities are increasing continuously. Technological connectivity drives the future by ensuring low latency, high data rates, reliability, and complete global coverage, coupled with advanced AI solutions like federated learning (ML/DL) and DL to make IoT environments. Besides, security and privacy are the two serious concerns that every IoT application domain should consider. And as IoT's worldwide connectivity continues to expand, security and privacy concerns may become even more important, requiring novel approaches.

2.1. Research methodology

The research study aimed to explore the potential of security solutions that can withstand potential attacks in the IoT-BC ecosystem. Four research methods were used based on the methodology adopted from [40], including planning and design, qualitative and quantitative research, and documentation. Data was collected from various scientific repositories, including IEEE Xplore, ScienceDirect, ACM Digital Library, PubMed Central, ResearchGate, and Web of Science databases. Over fifty articles were found addressing security problems in the existing system. The study focused on identifying articles that support BC as a solution factor. The inclusion criteria included articles matching the search keyword, being in English, having standard result analysis, comparing related works, proposing methods with conceptual architecture, and addressing real-time issues. The exclusion criteria excluded papers not in English, journal articles not indexed, book chapters, conference proceedings, and articles without quality metrics. Over twenty scholarly articles were found for the systematic survey (see Fig. 4).

2.1.1. Planning and design

This article explores the problem analysis of data privacy and security concerns arising from the interconnection of Internet of Things devices and BC networks. It focuses on potential solutions that can withstand node, user, and system-level attacks. The paper structure considers various aspects to meet future researchers' needs, ensuring a comprehensive understanding of the interconnectedness of IoT and BC networks.

2.1.2. Qualitative

The study analyzed over 200 scholarly articles on IoT and BC integration, focusing on security and privacy. The articles were analyzed across domains like smart agriculture, smart cities, intelligent transport systems, and eHealth. The study identified security aspects, requirements, properties, and solutions to withstand potential attacks. Most articles lack a clear conceptual architecture, leading to the proposal of a conceptual architecture for an effective, readable format.

2.1.3. Quantitative

The collected information from various scholarly databases can be used to present a systematic review article, focusing on essential elements of security solutions such as computation, communication, error rate, throughput, packet delivery ratio, and energy consumption. This helps narrow down research and ensures a standard review article presentation.

2.1.4. Documentation

This is the final phase of our review article. It highlights the findings of the literature review. All the information gathered from various sources was condensed and divided into sections. We also conducted a comparative analysis.

2.2. State-of-the-art solutions

Numerous research studies have recently been done on BC-based solutions that offer better security and more efficient metrics by looking at different aspects [41]. The integration of IoT and BC serves various areas, including securing the IoT ecosystem, threat intelligence, enabling trust in IoT, and secure banking management. Supply-chain Management, Healthcare, Lightweight BC for smart dust IoT, unmanned aerial vehicle applications, Smart City applications, BC Architectures for critical monitoring systems, complex underwater military services, etc.

Several research studies focus on enabling secure communication, ranging from conventional IoT to large-scale IIoT systems. Most articles produced numerous solutions aimed at providing security. Rao et al. [30] conducted a comprehensive literature search on privacy and security in smart IoT devices. To deal with challenges involving physical items, most IoT installations prioritize security measures, such as handling keys in an adaptable, dynamic, and lightweight way.

This study explores the security challenges and issues associated with distributed, cloud, fog, edge, and grid computing. Before implementing IoT technologies, it investigates spoofing, password guessing, denial-of-service, and Sybil attacks. The study also addresses privacy issues and regulatory challenges in IoT applications. It examines authentication and key agreement procedures to investigate security flaws in smart IoT systems. The study aims to build secure systems considering security needs, malicious attacks, smart cities and industries, and user interfaces. It examines theoretical reviews and countermeasures for security and privacy, revealing gaps in the literature, technical issues, privacy concerns, reliability, and risk evaluations. The study also covers formal verification methods, including accurate hardware and software behavior. Future research will focus on security and privacy issues in the growing IoT environment.

El et al. [42] conducted a comprehensive survey on IoT authentication schemes. This study provided a layer-by-layer overview of IoT security challenges and requirements. It then examines IoT authentication protocols. Using a multi-criteria categorization, it compares and evaluates existing authentication systems, highlighting their advantages and disadvantages.

Das et al. [43] studied Jiang et al.'s [44] scheme. It has several weaknesses, including the following: it does not protect against privileged insider attacks, inefficient sensor node registration, insufficient authentication during login and authentication, insufficient updating of a user's new password during password update, and after initial

node deployment in the WSN, it does not permit dynamic sensor node addition.

Das et al. [43] proposed a three-factor user authentication system for WSNs to avoid Jiang et al. [44]. The proposed approach is more secure than others. AVISPA replicates our formal security analysis methodology (Automated Validation of Internet Security Protocols and Applications). Simulation findings demonstrate the security of our approach.

Wazid et al. [45] proposed ASCP-IoMT as a lightweight, secure communication technique for IoMT environments using AI. They investigate its performance, security, and functionality compared to other schemes. The authors also investigate its impact on network speed. The results show that ASCP-IoMT has superior performance, security, and functionality compared to other schemes. The authors also compare the accuracy rates of decision trees, support vector machine (SVM), and logistic regression in AI-based big data analytics. The decision tree technique is quicker, but the SVM method is more accurate.

The study by Mall et al. [46] looks into the safety and security of authentication systems in the Smart Grid, the IoT, and WSNs. It shows weaknesses in AKA protocols with PUF and how performance changes as temperatures rise. Future PUF-based AKA protocols could address these issues, highlighting the potential of blockchain technology.

According to Adere et al. [34], BC is revolutionizing the Internet of Things (IoT) and the healthcare industry. BC improves data security by enhancing data integrity, access control, and privacy. Six data safety methods are used, including BC for metadata storage and IoT data exchanges. Blockchain is also used in smart cities for real-time data sharing. However, few authors propose integrating BC with data and drug supply chain management to prevent fraud and empower patients.

Javed et al. [47] analyzed network slicing applications and their potential integration with BC features. They discussed how BC can solve network slicing problems and how BC functions with network slicing. The research found that network slicing with DLT is still developing. The study demonstrated that BC has great promise in scenarios involving multiple parties, such as E2E network slicing, and as 6G networks become more complex, this is becoming increasingly important. The study provides a tutorial on BC and smart contracts.

Singh et al.'s [48] article explores the blockchain paradigm, transforming the IT industry due to its decentralized nature and peer-to-peer qualities. The authors examine real-world threats and security vulnerabilities in BC, examining challenges and attacks that hinder its widespread implementation. They also explore blockchain applications, benefits, and business opportunities and review existing security solutions and ongoing research work.

Latif et al.'s [49] study evaluates blockchain for the IIoT using a four-layer design and discusses potential challenges in each tier. They examine BC characteristics, various blockchain types, consensus processes, and implementation tools. They compare eight popular consensus algorithms, comparing their performance metrics like decentralization, energy efficiency, scalability, hardware reliance, and transaction speed. The study also discusses the most important blockchain implementation platforms, their basic operations, and potential applications in IoT and IIoT, including supply chain management, smart grids, transportation, healthcare, and agriculture.

Ratta et al.'s [29] study focuses on integrating IoT and blockchain in healthcare systems. They argue that IoT can improve doctor-patient communication and remote patient diagnosis but raise concerns about patient privacy. The authors propose a solution by combining IoT and blockchain, focusing on drug tracking, remote patient monitoring, and managing medical records. They also discuss the potential of IoT and blockchain in various IoT situations, making it a popular topic for further research.

Deebak et al. [50] developed a remote mutual authentication (B-RMA) system using blockchain for AI-empowered IoT sustainable computing systems. The proposed mechanism combines secure cloud networks and smart devices, meeting industrial requirements and IoT-based smart environments. The system was developed using Node.js and tested on throughput, overhead ratio, and execution time. The efficiency rate of concurrent requests was also considered. The findings demonstrate that the B-RMA creates a scalable environment that accommodates multiple needs.

Vangala et al. [51] proposed BCAS-VADN, a certificate-based authentication method for vehicles, to solve the issue of detecting accidents and warning others. The method allows vehicles to send secure messages to their cluster head, which then sends these transactions to an edge server, which analyzes and sends blocks to the BC cloud server. The cloud server converts incomplete blocks into complete ones and sends them to the BC. BCAS-VADN is compared to other state-of-the-art systems for lower communication and computation overhead, higher security, and more functionality.

Wazid et al.'s [52] study introduces a new method for verifying users and agreeing on keys using Crowd-Sourcing (CS) systems, BUAKA-CS. The study uses various algorithms to demonstrate its security capabilities, including resistance to replay and man-in-the-middle attacks. BUAKA-CS is faster to process and send, providing more security. A pragmatic analysis is also provided to assess its impact on the system's functionality.

Chen et al. [24] developed a blockchain-based key management technique for secure group channels in fog-based IoT devices. The method uses the DConBE and DPPOW PoW mechanisms and provides data recovery, non-repudiation, conditional anonymity, and resource authentication. It has also been shown in simulations.

Elkhodr et al. [53] introduces SIM, a semantic IoT middleware combining semantic annotation, blockchain security, and AI feedback modules. It enables interoperable, context-aware healthcare data management, ensuring encryption, service integration, and continual optimization.

Zaghouani et al. [54] DRDChain introduces a lightweight permissioned blockchain for decentralized IoT resource registration and discovery. Constrained devices act as clients, directory nodes serve as validators, and resource operations are managed by smart contracts. A Hyperledger Iroha prototype shows high reliability, low latency, scalable throughput, and modest storage overhead in realistic environments.

Panda et al. [55] propose a key management method based on BC for secure key handling in fog-based IoT devices. The method uses a one-way hash chain approach to provide public and private key pairs for mutual authentication. Experimental evidence supports the proposed scheme's superior performance over conventional techniques.

Khan et al. [56–58] study examines IoT security challenges across layered architectures, maps attacks to countermeasures, and assesses blockchain-based solutions. It highlights blockchain's potential in decentralizing trust, ensuring integrity, and enhancing authentication. The article concludes by identifying open issues like scalability, interoperability, and resource constraints.

Existing literature on IoT security issues has used secure authentication and key management schemes, which have limitations and are ineffective. BC offers better results due to its features. Some works address security issues specific to various applications, showing better energy efficiency, computation cost, and latency throughput performance. However, more enhancements are needed in BC consensus and smart contract-based algorithms, as depicted in Fig. 5.

3. Case studies and thematic analysis

This section reviewed several security issues associated with IoT that serve in various complex domains using IoT-BC case studies. Because of the new regulations, user and data privacy protection laws enable consumers and producers to understand the necessity of privacy preservation methods in areas where sensitive information is being processed. We then focused on privacy preservation schemes for integrating IoT with BC. We chose to review several application scenarios where BC adoption is mandatory. Tables 2 and 3 depict recent works published and address related issues in converging IoT and BC

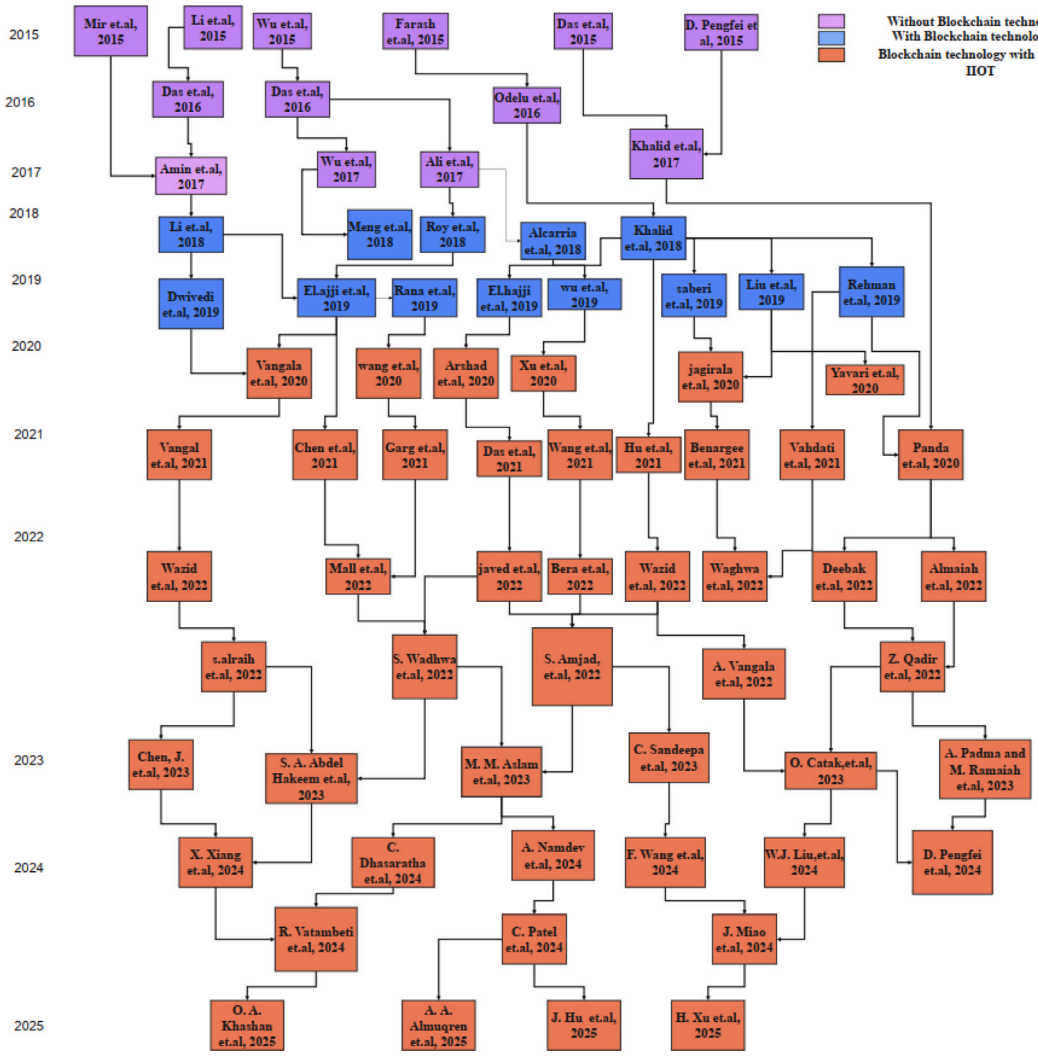

Fig. 5. The break-fix history of blockchain-based schemes.

environments. Thus, we reviewed existing security solutions to explore targeted fields, security challenges, future perspectives, and evaluation criteria as case study metrics. As a result, we chose five illustrated case studies. It is to highlight that the reviewed security issues and challenges are not depleted but can represent a high-level view of security in the IoT-BC ecosystem, combined with these five case studies. We structured each case study with the following parameters: overview, targeted field, case study, evaluation criteria, and future perspectives.

3.1. Case study: Smart agriculture

3.1.1. Overview

Agriculture is crucial for the economy in developing countries like India, and adopting intelligent and smart agriculture systems is essential for boosting GDP growth. Modern technologies like WSN and IoT maximize crop productivity, but security and privacy issues remain. IoT and Blockchain Technology (BCs) are commonly used to create secure application farming systems. Blockchain technology ensures safe communication, while decentralized systems like BC enable multiple systems to share data and maintain a local copy of the public ledger. Adopting these technologies in smart agriculture benefits the country's economy by reducing the risk of data loss and enhancing efficiency.

3.1.2. Targeted field

There are numerous applications in agriculture, including but not limited to precision farming, irrigation, monitoring animals, monitoring greenhouses, and other applications. Blockchain technology is being utilized to address concerns regarding network privacy and security in smart agriculture. To achieve security and privacy objectives, the authors offered a comprehensive assessment of how blockchain technology might be utilized for agricultural applications. The authors proposed a security-based generalized BCA after they had completed the process of finalizing the requirements for smart agriculture [61]. The British Columbia government has made it feasible for farmers and other users of smart farming technologies to gain access to agricultural data through a uniform platform (BC). In addition to providing openness, anonymity, and traceability, the persistent and auditable nature of the BC guarantees that the appropriate data will be utilized if required in the days and years to come. Singapore's Vangala 2021 Smart SCBAS-SF is a method of smart farming based on smart contracts and created by the authors. It is a BC-verified key agreement approach. Compared to the present mechanism, the suggested approach offers a higher level of security [62]. In this manner, the problems in smart agriculture in British Columbia are addressed to boost productivity.

3.1.3. Case study

Integrating blockchain technology in smart agriculture can improve security and privacy by enhancing data management. This is achieved through distributed ledger technology, ensuring data integrity, transparency, and security through an immutable and decentralized nature. Blockchain implementation involves IoT devices collecting data from

Table 2
Recently published works on IoT environments.

Article	Methodology	Contributions	Limitations	Evaluation metrics
Rao et al. [30]	Secure authentication approaches for smart IoT	-Analyze state-of-the-art techniques to address smart IoT applications' security issues. -Summarize how to design a secure IoT system for smart cities/industries. -Examine authentication and key agreement systems to detect smart IoT problems.	Blockchain technology has not been adopted.	-Done a Thematic analysis -Discussed various possible security attacks
El et al. [42]	Authentication schemes for the IoT environment	-Analyze various authentication schemes for the IoT environment. -Presented IoT layer architecture and discussed various possible security issues. -Presented how to develop a novel authentication scheme for IoT applications and networks.	Blockchain technology has not been adopted to address the security problems in IoT networks and Applications	-Done a security issues analysis for IoT architectures
Das et al. [43]	A three-factor user authentication scheme for WSNs	-Proposed a secure, temporal credential-based, three-factor user authentication mechanism in WSNs. The proposed method can withstand numerous known attacks through formal and informal analysis. -Simulate formal security analysis using the AVISPA tool. Results show the proposed system is secure.	-Blockchain technology is not included in this article. Required to adopt Blockchain for addressing security issues.	-Computation Overhead -Communication Overhead
Wazid et al. [45]	ASCP-IoMT is a novel AI-enabled, secure communication scheme	-ASCP-IoMT is a new AI-enabled, lightweight, secure IoMT communication system. It allows secure communications between IoT-enabled implantable medical devices, personal servers, and cloud servers. -The security research verifies ASCP-safety IoMTs against passive and active threats.	-Required to include blockchain technology to get a more secure environment.	-Throughput -End-to-End delay -Packet loss rate -Computation time -Accuracy
Mall et al. [46]	Physically unclonable function (PUF)-based AKA protocols for IoT	-This article outlines AKA and PUF protocols and their applications in IoT, WSNs, and smart grids. -Outline PUF-based AKA protocol deployment difficulties and research prospects. -Conducted analysis on security issues for IoT, WSN and Smart Grid.	Need to use BC to address security issues effectively.	-Communication cost -Computation cost -Security and functionality features
Adere et al. [34]	BC-based IoT framework	-Data management is BC's primary objective. -Data management requires data security. Data integrity, access control, and privacy are important. -This review found that numerous factors affect BC-based system architecture.	-The identity and authentication security issues still need to be addressed. -Required to develop an effective consensus mechanism.	-Throughput and latency requirements -File(Block) Size
Javed et al. [47]	The framework of BC with network slicing	-Presented a network slicing concept and DLT technologies and characteristics. -Presented the integration of DLT with Network slicing and discussed challenges.	-Need to discuss various issues like security, transparency, or trust among the stakeholders.	-Energy efficiency -Storage -BC Scalability -Complexity
Singh et al. [48]	BC for IoT systems	-Studied to analyze blockchain vulnerabilities in IoT networks and give countermeasures for such attacks. -Discussed Blockchain security attacks and flaws based on several studies	-Research issues still exist, requiring the enhancement of BC with IoT to improve security.	Communication and computation cost, and latency.
Latif et al. [49]	BC for IIoT	-Discussed a generic architecture and the challenges of IIoT. -Presented the integration of blockchain with the industrial IoT framework and its security issues and challenges.	Various issues and challenges need to be addressed in this integration framework.	The authors did a thematic analysis of various security issues.
Ratta et al. [29]	Blockchain-based IoT framework	-Presented a four-layer architecture of IoT. -Discussed the integration of blockchain with IoT for healthcare applications. -Presented various security attacks over healthcare applications of Blockchain IoT.	-Required to enhance the blockchain to address the security issues effectively.	-Computation cost and communication cost.

various farm operations, encrypting it, and sending it to a blockchain network. Smart contracts automatically execute when conditions are met, ensuring trustless transactions and data management.

AgriBlockIoT [63], a case study example, aims to enhance the security and privacy of agricultural data and improve the traceability of agricultural products. Farmers use IoT devices to collect data on crop health and environmental conditions, encrypted and stored on a permissioned blockchain to which only authorized stakeholders have access. Smart contracts are used for supply chain operations, including automatic payments upon delivery.

Enabling blockchain-based solutions enhances trust among consumers due to improved traceability of the products, reduced data

Table 3
Recently published works on blockchain environments.

Article	Methodology	New findings	Limitations	Evaluation metrics
Deebak et al. [50]	A blockchain-based remote mutual authentication (B-RMA)	-(B-RMA) to suit the standard constraints of Industry 4.0. -Integrated attribute-based signature (ABS) and BC to authenticate the gateways efficiently. -By using the smart contract technique, achieved the scalability and verification features.	-Required to include a formal model and verification technique to prove computer security.	-Execution time -Throughput ratio -Overhead ratio
Vangala et al. [51]	A novel BC-enabled certificate-based authentication scheme (BCAS-VADN)	-Designed a new authentication scheme for vehicle accident detection and notification in an ITS environment (BCAS-VADN). -Blockchain technology is used to store the transaction in a cloud server maintained by the Blockchain center, and the data is not tampered with by this technology.	-Expensive communication and computation costs. -Required to test throughput and latency.	-Computation cost -Communication cost -Security features
Banerjee et al. [59]	A new BC-envisioned-grained user access control mechanism	-CP-ABE-based scheme supports multiple attribute authorities having a constant-size key and ciphertext and supports policy hidden encryption. -The proof of the ABE scheme was provided. -The proposed scheme was evaluated by considering communication and computation parameters.	-Required to search the keyword-encrypted data stored in private BC.	-Computation cost -Communication cost -Security features
Wazid et al. [52]	A BC-based user authentication and key agreement scheme (BUAKA-CS)	-The proposed BUAKA-CS scheme uses a lightweight operation without extra overhead -BUAKA-CS did formal and informal security analysis using the Real-or-Random model (ROR) -The proposed technique was verified using the AVISPA tool.	-Required to focus on lowering the computing and communication expenses of BUAKA-CS.	-Computation cost -Communication cost -Security features
Chen et al. [24]	A BC-based key management method	-New encryption and decryption algorithms address security issues and operate in asymmetric groups to improve efficiency. -The DPPoW (Designated Prover Proof of Work) scheme. We can use DPPoW for resource authentication.	-Required to evaluate the proposed method with a real-time scenario and need to verify the scalability.	-Computational cost -Communication cost -Security features
Panda et al. [55]	A BC-based distributed IoT architecture with a secure key management scheme.	-A framework based on two BCAs has been designed. -The system is implemented on Ethereum, and a thorough evaluation confirms its ability to protect IoT.	-Required to enhance the proposed work for internetwork communication among devices. -Need to evaluate the scheme's effectiveness in terms of security.	-Scalability -Mutual authentication -Block size
Chen et al. [60]	Semantic-Enhanced Blockchain Platform	-Novel fusion of blockchain and semantic technologies: integrating descriptive ontologies with trust and immutability provided by blockchain. -Decentralized trust model: consensus-validated object registration and retrieval without central authority.	-The prototype explored only small-scale scenarios. -Requires a shared ontology; schema evolution and heterogeneity in real-world systems can be challenging.	-Computational cost -Communication cost -Accuracy

breaches and unauthorized access to sensitive information, and enhanced operational efficiency due to the automation of supply chain processes. Challenges and considerations include adoption, scalability, and legal and regulatory compliance.

Besides, the case study on smart agriculture focuses on food safety issues due to pesticide and fertilizer residue in agricultural products. A complete trace from manufacturing to wholesale, logistics, and retail is required to address these concerns. In 2018, an agriculture provenance system based on blockchain techniques was proposed, along with an intelligent architecture network security mechanism and a private blockchain system using dark web technology. Modern technology is needed to monitor all climatic conditions to increase crop yield. BC-based remote authentication for farm monitoring is proposed. A comparative analysis of existing schemes [60–62,64–67] was conducted based on communication cost, computation cost, security and functionality features, authentication and distribution period, and execution time.

3.1.4. Evaluation criteria

The study conducted a computation cost analysis using cryptography primitives to calculate the average execution time for transferring messages between different entities. The results showed that the cost of computation required to exchange messages across different entities for schemes varied between 22.37 ms for smart devices, 20.712 ms for smart devices, 4.733 ms for servers, and 4.5 ms for servers. The study also found that there is still a need to improve computation cost performance. The communication cost analysis showed that enhancements are required for various existing mechanisms. The study also highlighted the need to address security and privacy issues in data, focusing on asymmetric and symmetric cryptography algorithms. The study also conducted a comparative analysis of authentication and distribution time, private communication, BC authentication time, and average execution time for various existing schemes.

3.1.5. Future perspective

To encourage researchers to work in the field of BC-based smart sensing farm environments, this section outlines several issues and challenges that will need to be overcome shortly. The following problems and difficulties:

Scalability: The fundamental issue with BC is storage space. Blocks can only be added to the BC in this situation; they cannot be removed.

One of the suggestions is the quantity of transactions carried out per unit of time. Light clients, partitioned chunks, and the trade-off between big and small block sizes.

Privacy Leakage: Every block consists of BC transactions. All of these transactions have been made public. Blockchain cannot ensure transaction security and privacy. Various mechanisms have been developed to address security and privacy issues, but they need a strong BC-based security mechanism for agriculture applications. **AI-based Prediction system**: AI and ML can be utilized on the BC to analyze the IoT sensor data stored in the blocks. Various security measures have been developed in the AI, ML, and big data analytics sectors. AI and ML analyses have been added as extensions to the BC-based security solution for smart agriculture. AI/ML can be applied to data analysis and security measures. Big data and BC can be used to manage the expanding IoT data. In addition, ML can provide learning modes that help the system build its defenses and grow more resistant to various new types of attackers.

Error-Free Development of Smart Contracts: Smart contracts in BC can automate operations inside a BC. Incorrect data may be put in the BC due to a bug or mistake in a smart contract. Blockchain can be used as the foundation for many different applications, so mistakes in smart contracts could have serious implications.

Lack of Standardization: There are currently no standards to control the activities of a BC. It can lead to serious governance and interoperability incompatibilities among business organizations.

Lack of Professional Expertise: Only a few technologists have the essential skills to keep this field alive because BC is still relatively new.

High Cost of Development: In BC, adding a block is more expensive. Adding a work to the BC costs USD 550. It is critical to develop ways to lower this expense considerably.

Protection Against Selfish Mining: It is vital to ensure that no one mining node or small group of mining nodes uses excessive computing resources in a BC with few nodes. Such an event may result in successful BC manipulation or reversal. Although such an attack has not happened yet, current systems are not equipped to handle it if it does.

3.2. Case study: e-Health

3.2.1. Overview

Healthcare is a major priority as most patients and illnesses keep rising. Each patient's health-related data is necessary to maintain. It is essential to keep track of an individual's patient medical records to manage future health demands properly. The present infrastructure ensures that a patient's health record is maintained and shared systematically across diverse health-related organizations. Medical record integrity is a big issue, even when records are safely shared with other organizations. To satisfy the various security properties, such as confidentiality, integrity, and availability, for securing the patient's e-health record, introduce a BC. In health care, BC is being used to overcome security issues. Encrypted and shared cloud storage keeps the records safe from intruders. A BC is used to store the data. Each record is assigned to a block, logically linked to the previous block. As a result, there is a relationship between the records, and they are not collapsed. The timestamps of the blocks are present. A timestamp makes it simple to validate network transactions. Blockchain is a distributed and decentralized system, not controlled by a single authority. Therefore, BC plays a major role in securing patient e-health records.

3.2.2. Targeted field

In Blockchain, the e-health domain consists of various use cases to secure data, such as medical staff credential verification, IoT security for remote monitoring, supply chain transparency, and patient-centric e-health records. In the year 2021 authors proposed a Non-public network in the e-health domain to maintain the QoS and security needs among slices. The authors in [68] also proposed a BC mechanism for addressing security issues such as data integrity and reliability. Mallikarjuna et al. [69] proposed a BC 4.0-based IoT-cloud integrated framework (BEHR) to address the issues related to e-health record transmissions between various parties. The simulation results show that the proposed BEHR is better than conventional mechanisms. And conducted a comprehensive survey on BC-based emerging applications in the e-Health domain [33]. We studied various mechanisms and observed that security is a major concern in e-Health. Taloba et al. [70] presented a Blockchain-based security architecture using encryption and decentralization to safeguard the EHR and offer a secure means to access patient health data. The proposed mechanism balances access and security. Doctors, patients, caregivers, and outside authorities can securely store and access EHR medical records using the proposed system. Using BC in healthcare data management reduces breaches and fraudulent billing and improves privacy, security, and transparency. BC data exchange promotes safe and secure third-party sharing. This technique ensures secure healthcare management for patients, doctors, hospitals, insurers, pharmaceuticals, etc. Kim et al. [71] presented a BC-based PHR software and validated its user experience. The technology transmits patient data off-chain and stores encrypted data on-chain to avoid forgery and falsification. There are many ways in which patients can keep track of their opt-in and opt-out permission data on the BC. The testing was conducted for healthcare applications using BC. Others familiar with BC trusted the application, but those unfamiliar preferred another method. Harjul et al. [28] Various technologies such as BC, Edge, IoT and Cloud will be discussed in this article to connect patients, employees, hospital systems, EHRs and medical equipment. E-health and e-welfare services can be delivered effectively and securely via the edge-cloud continuum. We used a three-tier Edge-Cloud architecture as the foundational design, enabling the system components' best possible deployment. Integrating BC with Edge Computing for e-health and e-welfare privacy and trust. A comprehensive examination of the existing obstacles and hazards in adapting emerging technology to healthcare organizations' everyday procedures, including change management, transition costs, and regulatory requirements, is needed. Zarour et al. [72] BC models for protecting electronic health records are evaluated using Fuzzy-ANPTOPSIS in the research presented. There are a variety of variables and options to consider when using the hybrid fuzzy-ANP-TOPSIS technique to analyze MCDM problems, including an examination of BC. Various metrics are used to quantify the influence of BC models, their weights are calculated, and different rankings are produced. Healthcare BC services may be provided securely and effectively with a private BC. By safeguarding data through a decentralized peer-to-peer architecture, private BC offers more secure platforms for exchanging health data in the healthcare industry, revolutionizing how EHRs are marketed and maintained. Khan et al. [73] BC's rapid growth has produced new uses, especially in healthcare. Digital healthcare services need strong security methods that blend data security with management tactics. In this study, the writers used a numerical analysis and simulation to test and comprehend the purpose of Saudi Arabian security management. The authors used fuzzy AHP to evaluate effectiveness and fuzzy TOPSIS to simulate outcome validation. Alternative (A1) delivers the best protection among the six effective alternatives. Based on these evaluations, any designer can utilize the study's conclusions to build a time-saving and cost-effective method for using BC. Ejaz et al. [74] The authors of this paper focused on the latter scenario because it was intended to provide simple, dependable, and secure remote assistance and monitoring to elderly people living at home. The authors have developed a framework that combines edge computing and BC to meet some of the primary requirements of smart remote healthcare systems, including prolonged running times, low costs, dependability and safety, security, and trust under highly dynamic network scenarios. Regarding latency, power consumption, network utilization, and processing load, the performance of the proposed framework with BC was compared to that of a scenario in which no BC was used. Bittins et al. [75] a BC-based architecture to improve

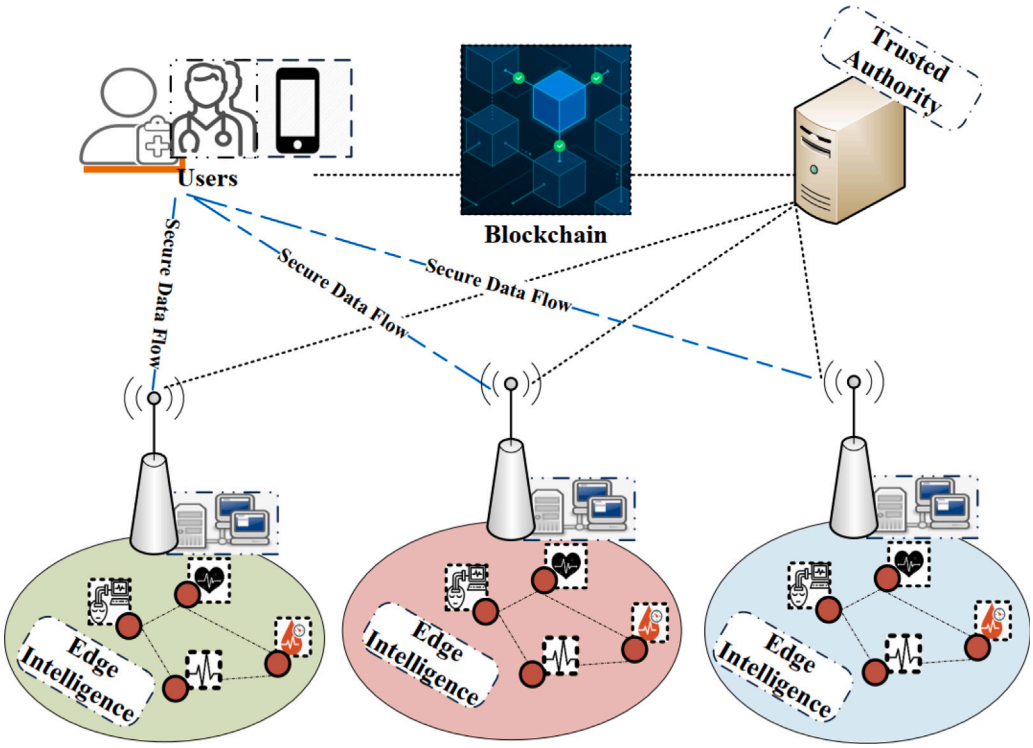

Fig. 6. Blockchain-based e-health environment.

the dependability of IHE-based data exchange solutions. This architecture (i) makes it easy to connect the EBSI infrastructure-based SSI credential verification to older healthcare systems, and (ii) it automatically adds provenance annotations to patient medical records based on the W3C PROV standard. This moral integration increases community trust in the data. Our design uses organ donation and transplant use cases to handle EFI transplant rules. It described the legal requirements that should be incorporated into subsequent-generation BC healthcare services by discussing patients' roles in expanding healthcare services like mobile healthcare and patient tracing. Ciampi et al. [76] analyze the problems and difficulties of integrating distributed ledger (BC) with HL7 FHIR. The health sector must certify and validate medical events to create health processes. The use of FHIR for dynamic care planning is provided after reviewing distributed ledger concepts, frameworks, and existing problems in the field of health. The permissioned BC platform, Hyperledger Fabric, is then integrated with several IHE DCP services in the real world to show how BCs may be used to secure FHIR resource authentication and process integrity. E.M. Adere [34] Blockchain technology's potential applications in IoT and healthcare were investigated thoroughly. BC's important goals are data integrity, privacy, and access control. Despite its potential benefits, BC is utilized in healthcare to manage data and the pharmaceutical supply chain to prevent fraud and empower patients. Vahdati et al. [77] presented a new IoT architecture for healthcare based on BC. The proposed architecture expands on a recently reported cognitive IoT system for healthcare monitoring that is built on BC. The designed architecture uses cognitive computing to organize management operations in IoT-based BC healthcare monitoring systems. Some COVID-19 case studies highlight the possibilities of the proposed architecture. Fig. 6 depicts the standard BCA in the e-Health domain

3.2.3. Case study

In this section, we are presenting a case study in the e-health domain. Introducing BC to various domains, like e-health, is associated with various risks. Most risks are standard, smart contracts, and value transfer risks. In BC, one of the major properties is no centralized authority, consisting of a decentralized framework. Data transmission is done between peers without a third party. A novel approach was proposed to address IoT healthcare's various issues and challenges using a BC-based integrated framework by Ikharo et al. [78]. But in their work, the cost and energy consumption are high. Required to develop the new framework to address these issues. IoT, BC, and AI (Artificial Intelligence) were all examined in the context of the e-Health domain. Integrating BC and AI technologies gives better results in terms of reliable efficiency and cost, and makes healthcare democratized. Blockchain provides storage space with security by using cryptography techniques [79]. However, this work did not consider security issues effectively. Due to the security issues leading to loss of integrity and confidentiality in patients' health records proposed a keyless signature infrastructure ensuring the authentication. Blockchain technology manages the integrity of data [80]. The transaction of health records is a major challenge between doctors and patients.

Almaiah et al. [81] Deep learning (DL) has been proposed as a lightweight authentication and data protection method for IoT-based CPS to facilitate decentralized authentication among Valid devices. Communication statistics are improved, and validation latency is decreased with decentralized authentication. The proposed model's importance was confirmed by comparing experimental results with traditional models. During evaluation, the proposed model shows huge improvements compared to traditional models. Garg et al. [82] This study offered access control and key management strategies that protect privacy for secure communication in IoT-enabled eHealth systems (SPCS-IoTEH). Informal security research is also conducted on the SPCS-IoTEH to show that it can withstand active and passive threats. SPCS-IoTEH outperforms other existing schemes.

3.2.4. Evaluation criteria

In this section, we conducted a comprehensive analysis by considering various metrics of existing mechanisms for the e-Health domain. Metrics like response time, transaction time, average cost, throughput, and network bandwidth serve to validate various BC-based mechanisms.

Response time: The response time metric is calculated based on the difference between the transaction received response time and submitted time. BHER mechanism improves the response time compared to conventional methods [69].

Transaction time: The transaction time is calculated by the time it takes for a transaction to be confirmed and available on the BC from the time it is submitted to the time it is confirmed and available.

Cost: The amount of computational resources and monetary costs that the BC consumes throughout its operation. Given the result, as the consumed energy of a transaction is predicted to be strongly associated with the resource cost required, the computing intensity would also affect the BC's operation costs. BHER mechanism reduces cost compared to existing mechanisms [69].

Throughput: The number of transactions completed successfully in a given period is what determines throughput. According to TCP and UDP transactions, the throughput value varied after 90 s in BC. It is required to enhance this by adopting new methodologies.

3.2.5. Future perspective

Interoperability and Traceability: The development of standards to promote interoperability among BC-based systems may pose a substantial problem for future researchers. Interoperability is necessary for the long-term survival and operation of BC-based healthcare systems. Even though a wide range of communication protocols is required for medical equipment, such as sensors and BC aids, interoperability can improve healthcare quality. The traditional method of achieving traceability has been to rely on a single authority to alter data without informing other parties. A lack of transparency could lead to a performance constraint and a single point of failure, though. [33].

Irreversibility: Security breaches in today's centralized healthcare systems make it impossible to guarantee the indestructibility of patient data. The inability to undo changes to data ensures the security of sensitive information. Combining regular cryptography with the BC hashing method achieves irreversibility. However, research into lowering BC's immutability to assure security is still in its beginning phases.

Tokenization: In recent years, the smart contract of real-world trade assets has aroused much attention. The audibility issue in BC is overcome by tokenizing resources as commodities. Reducing transaction costs, reducing transaction times and improving transparency are all benefits of tokenization in BC.

Integrating Blockchain with existing healthcare systems: In the e-health domain, BC provides secure transactions between peers and decentralized data sources. The behavior of data used in the e-Health domain can be modified, restructured, and rebuilt using BC. Data is collected from a variety of devices by healthcare systems, resulting in a vast number of data records. To maintain health data integrity, researchers must overcome considerable challenges in integrating BC into healthcare applications [33].

Fairness and security: Security and privacy issues are an open research problem in the BC-based e-health domain. Without a central control point, a BC-based e-health domain can store and transport e-health records in a transparent, safe, and decentralized manner. As the number of networked devices and online transactions increases, it has become increasingly difficult to process large transactions from various heterogeneous devices while guaranteeing data security and fairness.

Scalability: Scalability is a major barrier to the widespread adoption of BC in the e-health sector and many other application sectors. An increasing number of sectors and government agencies are placing increasing demands on their ability to scale.

Energy consumption: In the e-health domain, Energy consumption is crucial when considering BC-based IoT solutions. Because of the algorithms they use, BCs require a lot of energy. In blockchain, consensus mechanisms, for example, PoW, consume more energy than PoS.

Privacy leakage: Consumers can access their health record information using cryptography Techniques in the e-health domain. But in BC, everyone can have many addresses, and everything is available to the public. It is challenging to guarantee the anonymity of transactions on BC because the values of every transaction and the balances for every public key are exposed to the general public.

3.3. Case study: UAV communications

3.3.1. Overview

It is a robotic vehicle that may operate autonomously or under wireless remote control. The "drone" refers to an unmanned aerial vehicle (UAV). Sensors on unmanned aerial vehicles (UAVs) provide data on the vehicle's state and efficiently detect targets. UAVs were created for military applications but are now used in search and rescue, urban planning, environmental sensing, and precision agriculture. Since drones are connected to the Internet and communicate wirelessly, research has been focused on the security issues in the UAV communication network. It is possible to hack into and control a drone remotely using software like Sky Jack, turning it into a "zombie drone". Devices that connect wirelessly and directly to the Internet seriously jeopardize UAV network security. Sky Jack and other drone hijacking programs are made to break into drones and take remote control, transforming them into zombie drones under the attacker's control. Due to LOS connectivity, attackers utilizing a UAV may damage the cellular user equipment. As a result, the security of the UAV communication network must be addressed. Security issues might arise from unsecured WiFi, altered flight control settings, GPS intrusions, and unauthorized access to drone configuration files. Attacks against UAVs by Cyber-Physical Systems (CPS) can be mitigated using BC. Blockchain technology is a step toward making UAVs safer, more precise, and easier to control. Because it necessitates exchanging secure data between multiple UAVs, UAV communication is an excellent choice for blockchain implementation. With BC, transactions are recorded digitally in a network of connected blocks. The hash value of the preceding block is contained in each subsequent block, and so forth. Because of this aspect of BC, altering the data in a block is challenging because even a small change in the data affects the block's hash value. Decentralized distributed ledgers are transparent to all BC network nodes, faster to access, and immutable (participants). It is secure and trustworthy because of the distributed consensus method. The concept of BC is also used in a Smart Contract (SC). By using various mechanisms, BC provides strong, secure communication among UAVs.

3.3.2. Targeted field

We addressed BC for UAVs in this section, which is utilized to ensure secure communication between drones (UAVs). Drones (UAVs) communicated with one another, and while transmitting data between drones, different security risks from attackers were feasible. The Interplanetary File System and BC-based secure UAV communication mechanism over the 6G network were made by Gupta et al. to deal with problems like security, high data storage costs, network latency, reliability, and capacity. This proposed system protects data privacy and security while lowering data storage costs and improving network speed. Using unmanned aerial vehicles (UAVs) in catastrophe circumstances has great potential for creating adaptable and dependable emergency networks. The open-access UAV network and unreliable environment may pose security problems for UAVs when transmitting data. Wang et al. [83] developed RescueChain, a secure and reliable information-sharing tool for UAV-assisted disaster relief. To safeguard data sharing in the event of a disaster and to trace rogue entities in an immutable manner, the authors begin by creating a lightweight BCA. RescueChain's simulation results show that it can minimize delivery delay, boost user payoffs, and accelerate consensus compared to currently used solutions. Drones and UAVs are increasingly employed for spying and warfare. This UAV technology has security flaws like radio waves that rivals might use to cause data loss or destruction. Rana et al. [84] proposed a BC framework to secure UAVs and drones. Blockchain combines private key cryptography and peer-to-peer networks for security. With the help of BC, increase security and connectivity.

3.3.3. Case study

Blockchain-based UAV network communications will be the focus of this part, which includes a case study. Using unmanned aerial vehicles (UAVs) in catastrophe circumstances has great potential for creating adaptable and dependable emergency networks. The open-access UAV networking and unreliable environment may pose security problems for UAVs when transmitting data. Kumar et al. [85] Blockchain-based infrastructure for drone operation monitoring has been proposed to guarantee trust and security. By implementing GPS spoofing settings, we hope to learn more about how sensitive Unmanned Aerial Vehicles (UAVs) are to false GNSS signals. Using the Ethereum BC, a BC network has been built that is resistant to spoofing attacks. Blockchain is a popular technology for cryptocurrency. Blockchain affects UAV applications. The proposed solution employs the aerospace network's ledger for important data transfer in BC. Intruders that steal a single network block cannot affect the entire network because of the ledger's cryptographically imposed data integrity. Outliers in geolocation data are discovered and removed by the BC network regularly. Verified data is distributed for aviation and spacecraft operations. The proposed method outperforms previous methods in drift error in secrecy and integrity. Li et al. [86] proposed a Blockchain-enhanced data-collecting system for UAV-assisted WSNs. Large-scale monitoring will be possible with UAV-assisted WSNs that collect sensor node data. Spatial and temporal data aggregation based on compressed sensing and tailored for sparsity minimizes redundant WSN data. Merkle tree-based UAV identity authentication ensures data transmission safety. Semantic description of a recommended emergency plan. The DSB BC is supported by a data reconstruction-directed consensus mechanism. Disaster semantics is the analysis of a tragedy and the circumstances that surround it. According to tests, BC-enhanced spatiotemporal data aggregation improves the network life cycle and data reconstruction accuracy. DSB accurately describes disasters. Xu et al. [87] introduced a BC to the UAV-assisted IoT space and suggested a safe and efficient data collection solution. The swarm uses distributed ledgers built on the BC to protect itself from invading UAV swarms. The authors outline several security solutions based on Bitcoin and blockchain in the proposed framework. Passing data and documenting transactions allows UAVs to obtain charging coins. In exchange for the charging time, charging coins must be used to charge the device. To control UAV behavior, a stringent reward policy is proposed. Only excellent behavior will earn enough charging coins to charge your phone fully. The authors presented an adaptive linear prediction technique to reduce energy consumption. IoT devices use this approach to upload a prediction model rather than the raw data, dramatically reducing in-network transmissions. According to the simulation outcomes, the proposed solution can significantly improve data collection security and effectiveness.

3.3.4. Evaluation criteria

Offloading Latency: The offloading latency parameter is calculated based on successful resource transmission based on allocated tasks. Wang et al. [83] The proposed approach lowers the offloading latency for various job sizes. This is because the ground vehicle group is close to UAVs and is equipped with enough computational power. Kumar et al. [85] reduce the latency.

Energy Efficiency: The lower bound of battery capability for each UAV is defined by the total energy consumption of one cycle. It is possible to reduce the size and weight of the battery if the total energy consumption is reduced. This could have a huge impact on drones' energy consumption. One UAV's transmission, recording, and flight consumes an average amount of energy if a detected value is successfully rebuilt. Wang et al. [83] Using VFC, the energy efficiency of UAVs can be increased since the calculation missions can be effectively offloaded. Xu. et al. [87] With an increase in SR, the overall and average energy usage linearly drop. This is the result of the large number of Internet of Things sensors. Energy consumption decreased from 64 percent to 78 percent. With the SR increase from 80 percent to 99 percent, the average energy consumption decreases from 8.1 to 5 J.

Cost: The computation and communication cost is evaluated based number of transactions successfully done in the BC-based UAV framework. Xu et al. [87] mechanism reduces the cost.

Throughput: The throughput value is evaluated based on transmitted data size and time. Kumar et al. [85] Testing and optimization improve the send rate. When the Send Rate is increased, the query workload throughput grows synchronously. When throughput reaches a fixed level, the open workload will become a bottleneck and will not improve.

3.3.5. Future perspective

- Data handling: 6G uses a large frequency of 95 GHz- 3 THz, 1 Tbps (uplink and downlink), and a bandwidth of 1 THz compared to the present 5G communication technology. Massive volumes of data would be produced, requiring big data analytics, deep learning, and machine learning techniques.
- Data security: In UAV-to-Ground and UAV-to-U2U communication, data security is a critical challenge. Techniques for physical layer security and machine learning can be used to mitigate attacks such as denial of service (DoS), masquerade, spoofing, and eavesdropping. Data manipulation can lead to inaccurate results (via quantum assaults, for instance). The real-time deployment of the suggested BC-based solution is still in the early stages of development, even if it may alleviate data security challenges.
- Standardization: It is still early in the BC technology standardization and regulation process, even among well-known groups like IEEE and ITU. Because of this, the real-time deployment of BC over the UAV network requires appropriate norms, guidelines, and laws. Technological standards and suggestions must be developed to make the deployment of UAVs over 6G communication channels simple and efficient. Without the standardization of BC technology, getting BC into real-world 6G networks is problematic.
- Blockchain and 6G integration: 6G communication infrastructure is lacking, which may make it difficult to deploy UAVs with BC. Due to high spectrum efficiency, frequency, large data rates, and 1 Tbps throughput, network equipment and BC infrastructure may not be suited for 6G communication systems. UAV deployment is feasible upon restoring the current infrastructure with 6G-enabled devices. It would be a significant problem in terms of capital and operating expenses.
- Smart contract vulnerabilities: It is possible to write smart contracts in various programming languages such as Solidity, Kotlin and Java. With it, public participants can feel more confident about forming trusted agreements without needing a third party and worrying about eavesdropping or spoofing attempts. Smart contract vulnerabilities must be thoroughly tested and verified before being deployed to the public network.
- Energy efficiency: Unmanned aerial vehicles (UAVs) are severely hampered by their dependency on battery power in processing, storing, and responding. There is a bottleneck in computing power to execute SC and consensus procedures on UAVs using BC and 6G-based UAV networks. To remove the bottleneck, a UAV network and operational optimization are required.
- Handover delays: Surveillance is one of the few applications that require long-range communication and connectivity with intermediate infrastructure, necessitating handover mechanisms. All communication under the BC-based proposed system must go through the public, which can cause some delay while the consensus mechanism is in operation.

3.4. Case study: Supply-chain an industrial management

3.4.1. Overview

This emerging trend of supply chain quality management combines the highly respected disciplines of quality management (QM) with supply chain management (SCM) (SCQM). In contrast to traditional QM, SCM considers the performance of both upstream and downstream partners. Scholars examine supply chain management (SCM) from various perspectives. The need for modern information technology for efficient supply chain management is highlighted. In addition, erroneous information in the supply chain management (SCM) might lead to problems. Information technology software solutions have made it usual for networked industrial enterprises to communicate and engage with each other. Conventional manufacturing processes and data exchange methods in industries are losing ground to newer ICT technologies like the Internet of Things and BC. Blockchain has recently shown a bright future as the foundation for many Internet of Things (IoT) applications. The Internet of Things (IoT) allows certain BCAs to collect data directly from connected devices. Other IoT-related enterprises can use blockchain to create a secure and accessible data storage and sharing platform. Blockchain technology is the source of the word "BC", which was first used in the context of cryptocurrency in 2008. It is a distributed ledger that permanently and irrevocably records transactions between several parties. The preservation and validation of information is a topic on which all parties involved can agree. With distributed consensus methods and encrypted digital signatures, this BC-based solution eliminates the need for third intermediaries to facilitate direct transactions between peers. Regarding data storage and sharing, BC will have a greater impact on supply chain management for industries.

3.4.2. Targeted field

This section specifically discusses how BC is used for supply chains and industries using IoT. The authors presented a predictive delivery performance metric assessment methodology as well as DelivChain, a BCA optimized for industrial supply chain management. They discussed why DelivChain's architecture could improve supply chain management from many viewpoints by introducing the architecture details [88]. Jabbar et al. conducted a systematic survey on how BC works and addressed the various issues in supply chain management. Analyze the main technical and non-technical barriers to BC adoption in supply chain applications. The core concerns of scalability and interoperability are discussed, as are possible solutions [89]. Wan et al. [90] conducted a comprehensive review of BC's impact on supply chains with different databases. This research examines BC's impact on supply chain information sharing. The decentralized structure of BC offers high transparency, attracting interest from many areas. BC-enabled information exchange can improve collaboration in healthcare, construction, and smart city supply chains. From our findings, BC-enabled information exchange within a supply chain assures all members can get verified information, enhancing collaborative relationships.

3.4.3. Case study

This section discusses supply chain and industrial management applications developed using BC. The main focus is on the impact of BC on the supply chain. At the same time, we discussed new developments and their limitations. The limitations of this work are related to the respondents. Here, the results are biased. The transaction cost is huge, so we must address the issue [91]. Researchers from Li et al. [92] completed a comprehensive study of BC's possible applications in the industrial sector, including WSN, IoT, and traceability. A technical examination of BC's viability and approaches to transitioning from present methodologies to a BC-oriented platform was among his findings. There is also a discussion of a new use of BC for storing referral data. Authors Saberi et al. [93] proposed and discussed the use of BC in supply chain management. Data sharing, smart contracts, decentralized ledgers, and trustworthy, secure networks are all made possible by BC. This research is required to address various security and privacy issues. We know that no existing work exists to develop a taxonomy model to enhance supply chain activities. Shoaib et al. [94] proposed a BC-based supply chain through an integrated framework for successful deployment by identifying the priority of elements. This framework is used for the long-term supply chain. The authors did not include security and privacy issues in this work.

3.4.4. Evaluation criteria

In this section, we have comprehensively analyzed various mechanisms by considering various parameters such as accessibility, data management, overall cost, reliability and eco-reconciliation, sustainability, efficiency, communication cost, security, and privacy issues. All these factors will decide the best model for BC-based SCM.

Accessibility: This is one of the success factors of BC-based supply chain management. It consists of traceability, integrity, and trackability metrics.

Data Management: Data management is a factor in the supply chain, using BC to validate interoperability, data access control in SCM, authentic data, accounting, and auditability in SCM.

Overall Cost: This factor considers the cost, energy savings and administration cost reduction for the BC-based SCM.

Reliability and Eco-Reconciliation: This factor will verify reliability, no data loss, scalability in SCM, decentralization, environmental friendliness, human safety, and streamlinedness in BC-based SCM.

Sustainability: This factor verifies the permanence, high availability, and long-term growth of successful SCM.

Overall efficiency: This factor is verified based on effectiveness and efficiency, automation, problem-solving, simplification of the current paradigm, quality control, and the fairness of the product.

Computational Cost: The computational cost is calculated based on successful transactions within a specific period in BC-based SCM.

Security and Privacy issues: Most research articles related to BC-based SCM must address data sharing and storage security and privacy problems.

3.4.5. Future perspective

In this section, most of the challenges of BC-based SCM using IoT must be considered. All these challenges and limitations are extracted from the maintenance and deployment of BC in SCM.

Scalability: The devices continuously generate automated daily or hourly inspection data, which could cause the BC storage capacity to run out after a given operation time. One choice is to delete the captured data after a predetermined period. Today, the most common approach for BC consensus is proof of work (PoW), although this approach is slow and resource-heavy. A more appropriate consensus method, such as PoS or PoA, should be investigated as they gain traction.

Information confidentiality for suppliers: Companies will not share all of their data with third parties in the business world, so it is crucial to only store essential data on the BC and to put protections in place so that the data is only accessible to the parties (VCP) who need it.

IIoT Device Installation: IIoT software and hardware installation are the responsibility of humans. The IIoT's installation process and the way the data is gathered determine how reliable the data it produces.

High Learning Curve for customers: Customers must learn to appreciate the value of IIoT and BC in Open Manufacturing. Authors must understand how to comprehend the system and spot inconsistencies in the BC. In adjacent areas such as agriculture, the usage of IIoT and BC is currently primarily limited to simple activities such as traceability via RFID and other easy-to-learn applications.

Implementing Foundation is necessary: With blockchain technology, there are upfront and ongoing maintenance costs. Before making a choice, organizations using BC should assess if the benefits exceed

the disadvantages. Additionally, it can take some time until IoT devices fully automate data recognition and replace human input in every industry.

Incidental Cost: Blockchain technology is not a magic bullet; to be employed in various industries, it must be integrated with other technologies like machine learning, the Internet of Things (IIoT), edge computing, and others. It will not exist independently; it will be a part of a larger system. The financial strategy should immediately consider the required budget.

Smart Contract does not produce industrial standards: The fact that Smart Contracts execute established business procedures should not be overlooked. All required industry standards must be pre-set in the SCQM in this situation. All the data gathered will be meaningless for determining the level of product quality or the accuracy of human performance in upholding standards along value chains if they do not adhere to industrial standards. Several businesses, and even different manufacturers within the same industry, adhere to different standards depending on the consumer's expectations, the large variety of product categories, and the shortening of the product life cycle. One size does not fit all in terms of practical application for industries. Before machines can produce outcomes that are precise and reliable, organizations must comprehend this and be able to specify all pertinent criteria.

Universality: Several sectors can use the proposed methodology for choosing suppliers. Before investing in the BC framework, businesses must conduct a feasibility assessment. It is best suited for industrial organizations with significant requirements for quality control, a lengthy global supply chain, and insufficient managerial energy on-site due to fragile relationships with customers or suppliers.

3.5. Case study: Industrial IoT

3.5.1. Overview

The IoT is introducing new research advancements for industrial applications (IIoT). Over the past few years, IoT solutions have become increasingly popular across various industries, including healthcare, smart manufacturing, smart cities, energy, transportation, and many more. The use of IoT technology in industrial settings is referred to as IIoT. Robotics, artificial intelligence (AI), big data analytics, intelligent sensors, actuators, and improved communication protocols are just a few of the cutting-edge technologies combined in this system for application in traditional industrial settings. The IIoT is developing the next generation of intelligent systems by incorporating digital change in established sectors. IoT networks with billions of devices generate enormous amounts of data. IoT infrastructure flaws could be used to exploit this data's potential to include sensitive information. IIoT frameworks are typically centralized. Single-point failure in a centralized system can affect the IoT's acceptability and scalability. Decentralized techniques can increase IIoT security and trustworthiness. It enables IoT network development and prevents single-point failure. Existing centralized designs demand high-end computers for data management, security, and privacy. These are primarily third-party services. Users must trust these data services. In the worst case, this data can be exploited and disclosed to unauthorized persons. Blockchain technology is being used to solve the IIoT network's aforementioned problems. Using decentralized consensus processes, a BC is a distributed ledger that enables transaction processing and validation without the involvement of outside parties. All transactions in the BC are immutable since information about each transaction is available to every authorized node. Blocks on the BC are also protected from tampering by cryptography systems, including digital signatures, encryption algorithms, and hash functions. All authorized users can track transactions on BC, ensuring the IIoT systems' trustworthiness. Blockchain can be a brilliant decentralized option for improving IIoT security, privacy, scalability, and reliability.

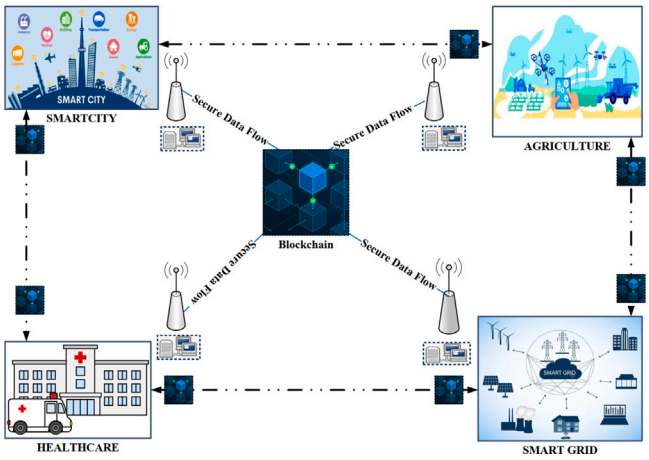

Fig. 7. Conceptual architecture of blockchain-enabled Industrial Internet of Things.

3.5.2. Targeted field

This section focuses on integrating BC with IIoT solutions for addressing various problems, such as security, privacy cost issues, etc. The new BC has shown immense potential for altering smart sectors and contributing significantly to economic growth. In the IIoT, BC plays a major role in overcoming interoperability challenges. The IIoT BC frameworks should be built with industrial requirements in mind. Including smart contracts, transaction data, network interaction, and other elements is required. Due to BC's decentralized nature, secure communication and data-sharing methods in IIoT networks have reached new heights. In industrial operations, BC dramatically decreases risks and expenses. Javaid et al. [95] proposed a BC framework using the dynamic consensus algorithm Proof of work (PoW) with a block checkpoint mechanism. The proposed mechanism addressed the issues of scalability and security. The performance results show that the proposed mechanism can attest that it can scale and offer better security with minimum block mining time. Kaur et al. [96] conducted a systematic survey on IIoT with BC using 5G or 6G technology. The authors first discussed Industry 4.0, Industry 5.0, and the promise of IIoT and BC. A literature review and recommendations for the future were provided to assist researchers in locating research gaps. The authors discussed the functioning, structure, and capacities of BC outlined IIoT's architecture, current issues, and difficulties. Lin et al. [97] studied a private BC-based IIoT system with UAV assistance and developed a non-convex optimization problem to reduce UAV energy usage. In this work, writers cooperatively optimized the block generation approach, bandwidth allocation, work allocation, and UAV trajectory design suggested a sub-optimal optimization technique based on SCA. Simulations demonstrated that the suggested approach can outperform existing methods. Fig. 7 depicts the standard BCA in the IIoT domain

3.5.3. Case study

This section discusses various case studies carried out on BC for Industrial IoT. Recent industrial Internet of Things (IIoT) developments have opened up many new possibilities for various industries. To address the vast IIoT data security and efficiency challenges, BC is widely regarded as a potential option for data storage, processing, and sharing safely and efficiently. An article by Liu et al. and Kebande et al. [98,99] suggested a new deep reinforcement learning (DRL)-based performance optimization framework for BC-enabled IIoT systems that would help with speed and security issues. The proposed system develops a methodology for evaluating the system in terms of scalability, decentralization, latency, and security. Improving the underlying BC's scalability without compromising the system's

decentralization, latency, or security. The authors first presented a quantifiable measurement for the performance of BC systems in our proposed framework. Then, using the DRL technique, the BC system's on-chain transactional throughput was maximized by selecting the block producers and consensus process and modifying the block size and interval. Rahman et al. [100] developed a BCA for end-user querying to address data privacy, integrity, and user reliability in IIoT systems. The framework uses BC to store IoT data as on-chain data and the cloud to store huge amounts of off-chain data (e.g., photos). It also provides search services by executing queries in both on-chain and off-chain data and generating an aggregated result. It offers a new query method that secures sensitive data during execution. A data owner encrypts on-chain and off-chain data using the privacy-preserving query technique before sending it to the BC and cloud. CSPs can search encrypted on-chain and off-chain data to protect sensitive data. BC is developing a multi-signature query verification mechanism. Each BC node can independently endorse a query result, and a user can double-check the endorsement before utilizing it. The authors plan to employ Ethereum-based smart contracts to construct a query verification technique.

3.5.4. Evaluation criteria

This section comprehensively analyzes various mechanisms by considering parameters such as time, energy consumption, throughput, and security and privacy issues. All these factors will decide the best model for BC-based IIoT.

Time: The Time required for making encryption query and results show an almost linear increment. The time varies based on several searchable keywords. In Blockchain, if the number of BC nodes increases, the required time also increases exponentially.

Energy Consumption: The Energy consumption considered mechanisms for different transaction data sizes [97]. We observed that Energy consumption increases if the transaction size of data increases. Energy consumption is evaluated based on data uploaded and transmitted during a specific period. In our observations, using BC-based IIoT reduces energy consumption.

Throughput: The throughput was evaluated based on BC size and the number of transactions stored in the block. BC system throughput for all schemes decreases with increasing transaction size. Adjusting the BC node size and transactions increases throughput. The proposed DRL technique [98]. By choosing the block producers and consensus method and modifying the block size and interval, the BC system's on-chain transactional throughput was maximized.

3.5.5. Future perspective

In this section, most of the challenges of BC-based IIoT frameworks must also be considered. All these challenges and limitations are extracted from maintaining and deploying BC in the IIoT. Latif et al. and Wang et al. and Fei et al. [49,101] and [102]conducted a comprehensive review on integrated BC with the IIoT framework and discussed various research directions, issues, and challenges.

Security and Privacy Issues: The security and privacy issues are open research problems for researchers using the BC-based IIoT framework. Most of the existing works addressed serious security problems, but still, various problems need to be addressed and enhanced.

Scalability: All consensus mechanisms in public and private BC networks require fully participating nodes to maintain a copy of all network transaction records. It offers security, decentralization, and fault tolerance at the expense of scalability. In traditional databases, extra storage is only necessary if the number of records grows. Additional computational capacity is necessary in BC-based systems to execute transactions faster. The scaling of BC has been a hot topic in academia. Here, we summarize some of the most important contributions to the scalability problem. As a result, BC scalability is still a work in progress. BC scalability is a hurdle to digital finance and IIoT applications because of high performance and networking costs. The vertical scaling of BC could be a scalability study. Conversely, horizontal scaling may be a more viable answer to this problem. As a result, semantically autonomous inter-BC communication could be a new research area.

Resource-constrained IoT devices: By combining IIoT and regular internet, smart devices can improve network automation. Most IoT devices have limited resources, making employing BC-based, decentralized designs difficult. IoT devices cannot engage in PoW due to limited processing power and battery life. IoT devices do not have enough storage for the BC. Combining IoT devices with BC-based networks may hinder decentralization. Future research could expand BC to the IoT edge. High speed and networking overhead hinder blockchain from being deployed on IoT devices. IoT gateways can be used with lightweight clients to push transactions into the BC network.

Security standards for smart contracts: Despite the smart contract's intrinsic security protections, the weak link has exploitable loopholes. Attackers took advantage of smart contract flaws in the DAO hack. Offering sophisticated security protocols for smart contract scripting is one route that might be taken in this area. By adhering to these security requirements, smart contracts will be made sure to be free of any vulnerabilities that can jeopardize the security of IoT devices in IIoT networks.

Trade-off between public and private Blockchains: The BC-based financial applications are still in the early stages of development and cannot yet compete with Visa and PayPal in IIoT networks. Applications must be able to manage a variety of usage scenarios and offer consumers anonymity in addition to Bitcoin. Different BCs are required in applications like IIoT, where BC is dispersed across numerous geographies and use cases. By properly connecting, these BCs can deliver various IoT services.

ML/DL for decentralized IoT frameworks: With the improvements in AI and machine learning over the last few years, we have seen revolutionary changes. These technologies are widely used in various fields, including IIoT, computer vision, and autonomous cars. Including machine learning in IoT networks is critical to fully realizing industrial automation's vision. In IIoT networks, ML and DL algorithms may make intelligent decisions. IIoT networks improve industrial and energy trading. Machine learning and deep learning can detect IIoT cyber threats. Intrusion detection systems recognize network hazards. AI and IoT maintain network and source trust. IIoT users can commercialize and crowdsource data after a BC-enabled system is constructed. Industrial automation training can benefit from open, BC-secured large data. BC can secure sensitive data repositories. AI can automate IIoT eyes and ears. ML and DL in a BC-based system improve IIoT security and performance.

4. IoT-Blockchain ecosystem

The IoT is critical to improving the sustainability, performance, and security of industrial systems and their infrastructure. The typical IoT architecture comprises four layers: a perceptron layer for data collection, a network layer for bidirectional communication, a service layer for data analysis and processing, and an application layer for providing a graphical user interface to users. Figs. 8 and 9 depicts the standard conceptual architecture for the IoT and BC ecosystems respectively.

Perceptron layer: This layer will establish a wireless communication link between several internet-connected devices, enabling them to observe, detect, and enhance data with other devices. Sensors, actuators, RFID tags, readers, and intelligent systems are only a few real-time examples of the perceptron layer. This layer is divided into two sections, as explained below. To understand the trustworthy nature of the device in the distributed network, each sensing device should have a unique ID. Data protection is crucial to prevent monitoring and tapping by intruders because data transmission between two points must occur in public places.

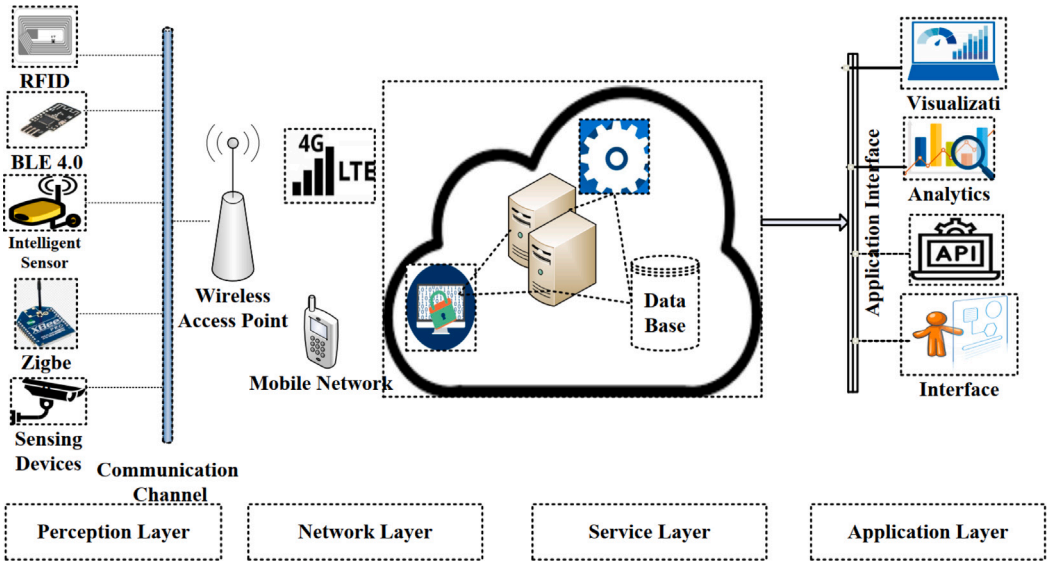

Fig. 8. Typical IoT four-layered architecture.

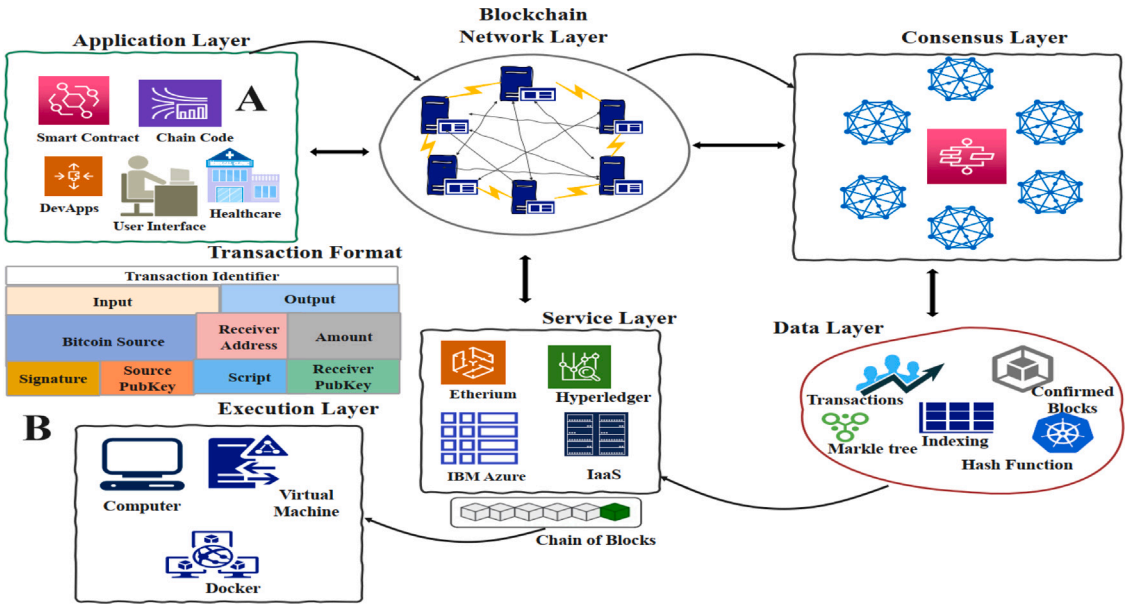

Fig. 9. Conceptual architecture for IoT-Blockchain ecosystem.

Network Layer: In IoT architecture, the network layer is an integral aspect of the infrastructure. This layer addresses and routes data packets supplied by IP addresses from one location to another. The standard protocols for the network layer are IPV4 and IPV6. IPV4 had reached its limit and could no longer process IoT application transmissions with scalability. The IPV6 standard provided ample address space for many IoT devices. Short-range and internet communication technologies have been combined for IoT device communication systems. Real-time examples include short-range communication technologies like Bluetooth and Zigbee, which only transmit data from detecting devices to the nearest gateway based on the available bandwidth. Wi-Fi, 4G, 5G, and PLC are internet communication technologies that can send data over vast distances (Power Line Communication).

Middleware/Service Layer: It is a crucial component in IoT infrastructure that authorizes and disables data services for user apps and device applications. It includes business logic, service division, integration, implementation, and repository. Cloud storage is essential for IoT devices, as they lack sufficient storage space for data. Cloud storage offers security features like availability, immutability, scalability, and verified access. It facilitates secure end-to-end data flow for authentication, authorization, identification, encryption, remote provisioning, buffering, synchronization, scheduling, group communication, and device management.

Application Layer: It involves data retrieval, processing, and visualization. Users can access reports and responses through data retrieval. Secured data stored in a database can be accessed for analytics, enabling real-time data searching. Data delivery models and principles ensure secure, legitimate, and protected data. Implementing a dispersed network in IoT eliminates the need for additional server components for accessing big databases for safe data storage from sensory devices.

Smart BC-based Industrial IoT (IIoT) This system aims to create a secure authentication scheme for IoT devices using Ethereum (distributed ledger technology) using pre-shared key distribution. The smart contract holds the keys to all devices, providing secure authentication between them. The system controls sensors, servers, network devices, machines, the cloud, and software applications. It also includes

Table 4
Analysis of various attacks.

Attacks	Das et al. [105]	Bera et al. [62]	Anu et al. [61]	Das et al. [43]	Deebak et al. [106]	David et al. [107]	Fadi et al. [108]
$\varphi UIA\varphi$	✓	✓	✓	✗	✗	✓	✗
$\varphi PIA\varphi$	✗	✓	✓	✓	✗	✓	✓
$\varphi PGA\varphi$	✓	✗	✓	✓	✗	✓	✗
$\varphi BFA\varphi$	✓	✗	✗	✗	✓	✗	✗
$\varphi DIA\varphi$	✗	✗	✓	✗	✗	✓	✗
$\varphi FDI\varphi$	✗	✓	✓	✗	✗	✗	✗
$\varphi SPA\varphi$	✗	✗	✗	✓	✓	✗	✗
$\varphi SNIA\varphi$	✓	✓	✓	✗	✗	✗	✗
$\varphi SKA\varphi$	✗	✗	✓	✗	✗	✓	✗
$\varphi MIMA\varphi$	✓	✓	✓	✓	✗	✓	✗
$\varphi SVA\varphi$	✓	✗	✓	✓	✓	✗	✗
$\varphi JMA\varphi$	✗	✗	✓	✗	✗	✓	✗
$\varphi DOS\varphi$	✓	✗	✓	✗	✓	✓	✓
$\varphi DDOS\varphi$	✓	✗	✗	✓	✓	✗	✗
$\varphi MNA\varphi$	✗	✗	✓	✗	✗	✗	✓
$\varphi DEA\varphi$	✗	✗	✓	✗	✗	✓	✗
$\varphi SCA\varphi$	✗	✓	✗	✓	✗	✗	✗
$\varphi HFA\varphi$	✗	✓	✗	✗	✗	✓	✗
$\varphi ROA\varphi$	✗	✗	✗	✗	✗	✓	✗
$\varphi WOA\varphi$	✗	✓	✗	✗	✗	✓	✗
$\varphi GHA\varphi$	✗	✗	✗	✗	✓	✗	✗
$\varphi BHA\varphi$	✓	✗	✗	✗	✗	✗	✗
$\varphi SHA\varphi$	✗	✗	✓	✗	✗	✓	✗
$\varphi FSNA\varphi$	✗	✗	✗	✓	✗	✓	✗
$\varphi NC\varphi$	✗	✓	✓	✓	✗	✗	✗
$\varphi DOA\varphi$	✗	✗	✓	✗	✗	✓	✗
$\varphi REA\varphi$	✓	✓	✓	✓	✗	✓	✓

application sensing, data processing, network communication, cloud storage, terminal access, and management to meet security requirements. The Smart BC-based IIoT system aims to meet security requirements by controlling sensors, servers, network devices, machines, the cloud, and software applications.

Sensing and Data processing: Secure IIoT management involves integrating sensors, actuators, radio frequency identification, and smart hardware components. Sensors collect data from the environment and transmit sensitive information for processing. The data is stored on cloud servers. Sensor devices have limitations in storage and energy. Son et al. 2020 [103] proposed a secure authentication protocol using BC, providing security and efficient data transmission between sensor devices.

Network communication and storage: These are crucial in integrating a centralized network to provide services for application users, virtual machine instances, and sensitive information. The data processing layer loads and runs various apps and virtual machines, ensuring user authentication, management, device monitoring, and data storage. However, various attacks can occur between the network and the storage data transmission. Bagga et al. [104] proposed a secure authentication protocol based on BC that considers two forms of authentication and is highly resistant to various security attacks.

Terminal Interface and Management: Intelligent applications and services are crucial for managing security risks. A secure connection between storage and services allows real-time data handling, categorizing systems' operational state, or scheduling activity. Industrial settings can be monitored securely through indexing. End users access information services from cloud storage through a user interface, but authentication issues occur. A BC-based user authentication and key agreement protocol is proposed to address these issues. Layer architectures have been proposed to improve security and efficiency, but each layer may face various security attacks. A BC-based Industrial IoT (IIoT) architecture is proposed to address these attacks, providing more security and efficiency while performing robustly against passive and active attacks.

5. Security and privacy

This section considers several security mechanisms to review their requirements, properties, vulnerabilities, issues, and possible attacks. For different IoT applications, security solutions are investigated. Rao et al. [30] and El et al. [42] conducted a systematic survey and thematic classification on security and privacy issues in emerging industrial IoT technologies. Their articles focused on authentication and key management protocols to secure IIoT environments. They addressed various security attacks, reviewing various security mechanisms and tools to address challenges in intelligent technological environments. Das et al. [109] carefully studied Rana et al. [110] work and found that it is insecure against significant attacks, including stolen smart cards, privileged insider, user impersonation, password change, and ESL attacks. We observed from the above-mentioned articles [30,42,109] that they mainly focused on security issues and challenges in BC-based frameworks. Various other research works [43,50,61,62,105–108] [82,111–113] Specifically focused on providing reliable and secure communication technologies to enhance the security requirements of blockchain-based IoT applications. Table 4 depicts various potential attacks in the IoT-BC ecosystem. Besides, Table 5 denotes the landscape of various security requirements, challenges, attacks, and possible security solutions.

5.1. Security requirements

Confidentiality: WSN security services ensure information integrity and restrict access to data. Public-key cryptography is a common method, but it requires more resources for computing and transmission. WSNs are resource-restricted, making it difficult to withstand known attacks. Multiple security protocols based on symmetric-key cryptography have been developed to address these issues, ensuring unauthorized users do not have access to sensitive information.

Integrity: It assures that data generated and received during transmission and storage is not tampered with.

Authentication and Authorization: The authentication process for IoT devices is crucial for secure communication. It requires a lightweight schema, as many devices have limited resources. Multi-factor authentication is recommended, combining encryption techniques like RSA, SHA, AES, and ECC. This approach is valuable as it supports multi-factor authentication, reducing additional demands on IoT devices. The authentication schema should be valuable and efficient, ensuring the integrity of other IoT devices.

Table 5
Security functionality [30].

Security requirements	Security challenges	Possible attacks	Security solutions
Mutual authenticity	Secure communication	φNCφ	Oneway hash function
Node level security	Frequency jamming	φDos/DDoSφ	Biometric authentication
Forward and backward secrecy	Profiling and localization of the tracking system	$\varphi HFA\varphi$	2FA,3FA,MFA
Access control	Vulnerable to DoS & Interference	φMNAφ	Behavioral factors
Secure session key agreement	CIA of sensor node	φDOAφ	Pairing based authentication
Privacy preservation	Identification and authorization	φROAφ	ECC
Application security	Insecure initialization and configuration	φMIMAφ	Symmetric cryptographic solutions
Data security	Insecure interface	φSCAφ	Smart-card authentication
Intrusion detection	Attack tolerance	φSVAφ	Fuzzy extractor
Seamless communication	Malicious node isolation	φSHAφ	Attribute-based authentication
Secure routing	Secure route establishment	φGHAφ	Seamless roaming
Attack detection	Access control and information security	φBHAφ	XOR
Secure message transmission	Data storage	φJMAφ	Physical proximity-based
Constrained resources	Insider resource blitz	φFDIφ	Gesture based
Data freshness	Resource-efficient counter steps	φSNIAφ	PUF authentication
Robust and resilient management	Cryptographic techniques	φFSNAφ	Secure session key agreement
Modern cryptographic primitives	Enormous data handling	φWOAφ	Chebyshev chaotic map

Access Control: It is a crucial aspect of IoT security, ensuring that devices do not access unreadable information. It is essential for monitoring resource access and preventing unwanted information flow efficiently. In IoT and blockchain contexts, data can be transmitted continuously and shared between people and devices, ensuring security.

Availability: It ensures that IoT services are available when needed, even with resource limits such as power outages or DoS attacks.

Data freshness: It ensures that the data sent by sensory devices is as fresh as possible. The freshness feature ensures that every message received is current. It necessitates using recent data sets and ensures no attacker responds with an old message.

Non-repudiation: It ensures that communication parties data transmission cannot be disputed even though the message has already been transmitted. This might be considered when the communication parties have agreed to the contract.

Resilient to device security: The interconnected nature of IoT devices makes them vulnerable to hacked devices, allowing attackers to access secret credentials and session keys. To maintain device security, secure authentication and key agreement processes must be implemented, as compromised nodes may affect other network sections. Implementing security methods to protect non-compromised devices is crucial to ensuring the security of all network sections.

5.2. Security issues and challenges

This subsection discusses various security challenges in the subsectors of IoT environments.

Scalability: A vast volume of data is generated and communicated in the IIoT environment for further processing. However, the dynamic node addition puts the current system in danger due to the growing number of devices used. Therefore, secure node authentication procedures are needed to facilitate the installation of sensing devices while maintaining security.

Energy: Many Internet of Things (IoT) devices have limited resources, particularly in battery life. By activating the power-saving mode, these devices can automatically conserve energy when no activity is detected. However, the vast majority of the devices are used for ongoing surveillance. This flaw makes imposing high-level security on these IoT systems incredibly difficult.

Heterogeneity: We were discovered to employ a range of IoT sensors, RFID systems, mobiles, and other devices for our convenience. The compute, communication, and storage capacities of these devices may vary. As a result of these IoT devices, designing secure authentication becomes difficult.

Trajectory: It is a particular form of data regularly acquired by sensors in IoT setups. Multiple trajectory data sets are now available for tracing and profiling human activity. The trajectory can generate large amounts of data because data is collected from many sensors and other IoT devices. Furthermore, the trajectory is designed to perform mobility tracking, which is widely used in various applications such as urban planning, market analysis, and route selection. People can get real-time trajectory information and analyze trip trends using trajectory services. As a result, adversaries can exploit trajectory as a key potential tool to gather user activity and carry out nefarious acts. Author [107] first proposed a variable-length n-gram architecture for producing sequential data with differential privacy. They also established several strategies to ensure system efficiency, such as determining a threshold value, assigning a privacy budget, and enforcing consistency limits.

Dynamic Security Update: It is vital to upgrade the security schemes to provide continuing security features and to withstand security flaws in the present system. The trusted authority in the other network entities must issue this. So that they can keep their memories up to date. As a result, developing a new security mechanism capable of handling ongoing security updates in the IoT context remains difficult.

Security against physical capturing: Most devices in the IoT environment are deployed in hostile environments so that enemies can physically capture them. As a result, they can extract information from the device memory using a power analysis attack and then proceed to do malicious operations such as password and session key computation. Furthermore, an attacker can clone the device and put it on a real network to cause widespread damage. To overcome this problem, tamper-resistant packaging services are required. However, a secure authentication must be required to identify the hacked device while causing no harm to the rest of the network's components.

Potential Attacks Most devices in the IoT environment are openly exposed to several vulnerabilities and various potential attacks, including DoS, DDoS, Denial of Sleep, Injection, Side channel, to name a few. Fig. 10 depicts various attacks possible with the integration of IoT environments (see Table 6).

5.3. Threat model

Adversary capabilities and primary implications are determined based on the widely used Dolev-Yao threat model [118], "Canetti and Krawzyk (CK) adversary model" [119], and "Honest but Curious" [120].

The "Dolev-Yao model" is crucial in computer security, particularly cryptographic protocols. It provides a formal framework for analyzing and designing secure communication protocols in the presence of active adversaries. This model accounts for active adversaries, allowing for a more accurate representation of real-world security threats. It also aids in protocol verification, enabling the early identification of vulnerabilities and weaknesses. The model is often used as a teaching tool in computer security courses, providing a theoretical foundation for understanding modern security challenges.

Table 6
Cryptographic countermeasures for IoT–blockchain attacks.

Attack	Acronym	Cryptographic countermeasures [12,13,27,30,31,62,91,100,106,114–117]
User impersonation attack	ϕUIAϕ	Mutual authentication using ECC-based ECDSA; zero-knowledge proofs
Mass node authentication	ϕMNAϕ	Smart contract-based registration; hash chain-based scalable authentication
Privileged insider attack	ϕPIAϕ	Role-based access control via smart contracts; secure multi-party computation (SMPC)
Desynchronization attack	ϕDEAϕ	Timestamp + HMAC counters; state validation using blockchain ledger
Side-channel attack	ϕSCAϕ	Constant-time cryptographic operations; masking and threshold cryptography
Replay attack	ϕREAϕ	Nonce + timestamp checks; ephemeral session keys
Hello flood attack	ϕHFAϕ	Distance bounding; authenticated neighbor tables via blockchain
Eavesdropping/Sniffing	ϕEDSϕ	End-to-end encryption (AES-GCM, ECC); lattice-based post-quantum crypto
Password guessing attack	ϕPGAϕ	Argon2id hashing; PAKE protocols
Routing attacks	ϕROAϕ	Blockchain-based trust routing; cryptographic route authentication
Brute-force attack	ϕBFAϕ	Key strengthening (PBKDF2, Argon2); request rate-limiting on-chain
Wormhole attack	ϕWOAϕ	Time-of-flight validation; physical anomaly detection with on-chain timestamping
Dictionary attack	ϕDIAϕ	Salted hashes; biometric or multi-factor authentication
Gray hole/Black hole attacks	ϕGHAϕ/ϕBHAϕ	Blockchain-enforced peer reputation; trust score computation
False data injection	ϕFDIϕ	Data signing using ECDSA; Merkle proofs for integrity validation
Spoofing attack	ϕSPAϕ	Public key infrastructure (PKI); location-based authentication
Sinkhole attack	ϕSHAϕ	Token-based route validation; consensus on routing trust
Sensor node impersonation attack	ϕSNIAϕ	Identity-based encryption (IBE); certificate verification on-chain
Fake/Sybil node attack	ϕFSNAϕ	Blockchain-based ID verification; proof-of-location schemes
Session key disclosure attack	ϕSKAϕ	ECDHE with forward secrecy; periodic session key renewal
Node capture	ϕNCϕ	Tamper-resistant modules; threshold secret sharing with smart contract rekeying
Man-in-the-Middle attack	ϕMIMAϕ	Mutual TLS; blockchain-based key handshake and ZKP
Denial of sleep attack	ϕDOAϕ	Energy-efficient MAC protocols; beacon authentication
Stolen verifier attack	ϕSVAϕ	HMAC challenge-response; salted verifier chains stored on-chain
Jamming attack	ϕJMAϕ	FHSS (frequency hopping); blockchain-assisted route reconfiguration
Ephemeral secret leakage attack	ϕESLAϕ	Secure PRNG-based ephemeral keys; PQC key encapsulation
Denial of service attack	ϕDOSϕ	On-chain rate limiting; PoA or PoAc consensus mechanisms
Distributed DoS attack	ϕDDOSϕ	IP filtering via decentralized firewall; blockchain-maintained reputation

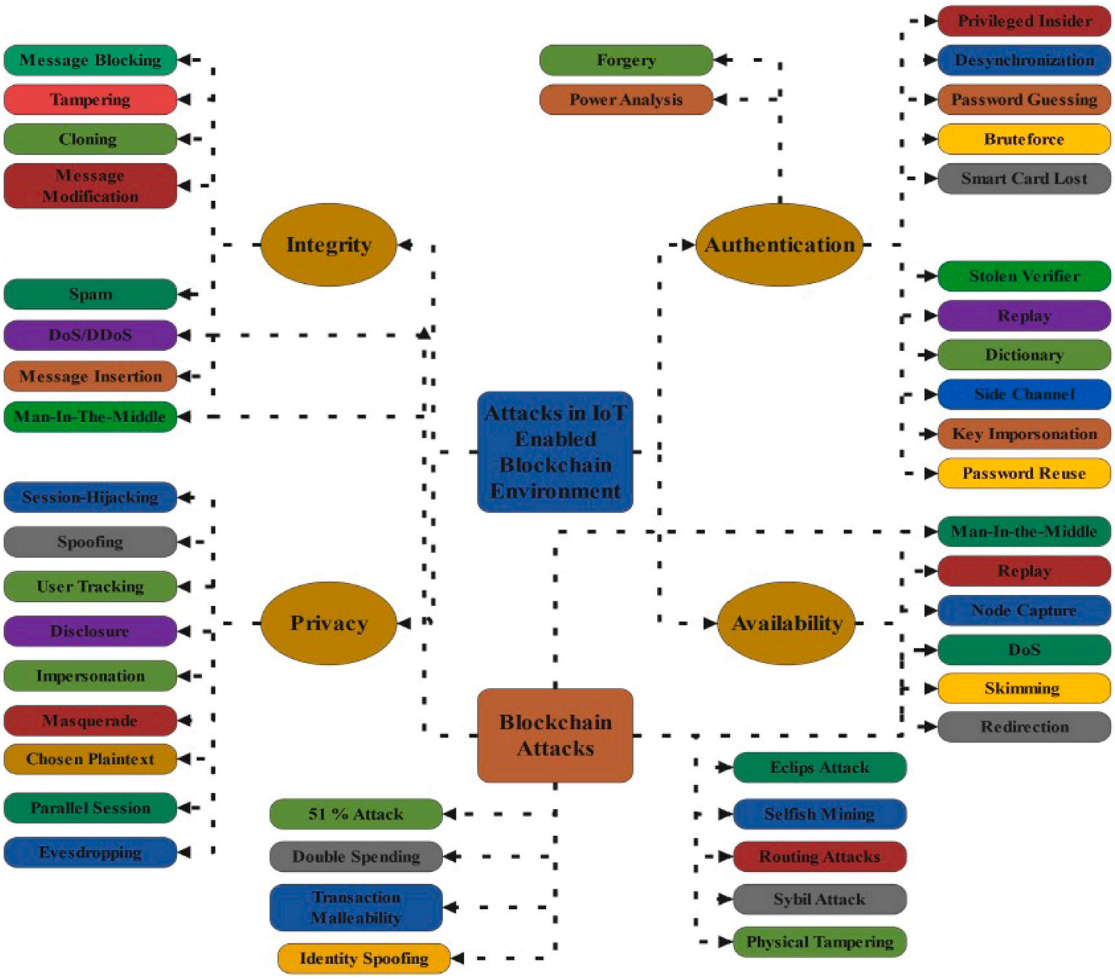

Fig. 10. Potential security and privacy issues.

Table 7
Cryptographic security solutions for IoT-blockchain attack mitigation.

Framework	Attacks mitigated	Security solutions
SBBDA-IoD: Secure blockchain-based authentication and key management for IoT drones [121]	ϕUIAϕ, ϕPIAϕ, ϕREAϕ, ϕMIMAϕ, ϕSVAϕ, ϕESLAϕ, ϕNCϕ	Blockchain-backed timestamp validation; ECC-based key exchange; on-chain identity verification
PIA: A secure and efficient identity authentication scheme in IoT [122]	ϕUIAϕ, ϕREAϕ, ϕSCAϕ, ϕDOSϕ	Pseudonym-based identity masking; hash-chain authentication; DoS-throttling via request control
Blockchain-machine learning fusion for enhanced malicious node detection in IoT [123]	ϕFSNAϕ, ϕSPAϕ, ϕBHAϕ, ϕGHAϕ, ϕWOAϕ, ϕHFAϕ	Blockchain ledger validation + ML classifier to flag routing anomalies; trust scores updated on-chain
Classification of security issues and cyber attacks in IoT [124]	ϕBHAϕ, ϕWOAϕ, ϕGHAϕ, ϕFSNAϕ, ϕHFAϕ, ϕDOSϕ	Taxonomy-driven threat modeling; lightweight consensus protocols; blockchain-based integrity checks
False data injection attack and its countermeasures in WSN [125]	ϕFDIϕ, ϕFSNAϕ, ϕWOAϕ, ϕHFAϕ	Signature-based data validation; ECC-based authentication; secure beaconing protocols
Securing IoT devices against emerging security threats [126]	ϕFSNAϕ, ϕSPAϕ, ϕREAϕ, ϕMIMAϕ, ϕDOSϕ, ϕPIAϕ	Hybrid blockchain-PKI scheme; session tokens; secure smart contract logging; anomaly detection

Table 8
Notations used.

Notation	Definition
U_i	IoT user node
G_w	Gateway node
BC	Blockchain network
TS	Timestamp
N_i	Nonce generated by U_i
SK_i, PK_i	ECC key pair of U_i
SK_w, PK_w	ECC key pair of G_w
$H(\cdot)$	Secure hash function
$E_{PK}(\cdot)$	ECC Encryption with public key
$D_{SK}(\cdot)$	ECC Decryption with secret key
$Sig_{SK}(\cdot)$	ECC-based Digital Signature
$V_{PK}(\cdot)$	Signature verification
K_{sess}	Session key

The CK adversary model is a formal framework used to analyze the security of cryptographic protocols, particularly those based on symmetric-key cryptography. It extends the traditional "active adversary" model by introducing a more realistic and powerful adversary capable of mounting various attacks against the protocol. Key features of the CK model include an active adversary, which can intercept, modify, and inject messages exchanged between protocol participants; a stateful adversary that can maintain state information across multiple executions; and a corruption ability that allows the adversary to corrupt honest participants in the protocol. The CK adversary also exhibits adaptive behavior, adapting its strategy based on the information it gathers during protocol execution. The model considers security concepts like being unable to distinguish between encryption schemes by a chosen plaintext attack (IND-CPA) and not being able to change digital signature schemes by a message attack (UF-CMA). This model captures more realistic threats that cryptographic protocols face, allowing for a more accurate protocol security analysis.

The "Honest but Curious" threat model is a widely used tool in cryptographic protocol analysis. It assumes that participants are honest, follow protocol specifications, and are curious about the execution. Participants are limited to passive attacks, observing and analyzing information exchanged during protocol execution but not actively tampering with or altering messages. They act independently, not collaborating to launch coordinated attacks. Participants have limited capabilities compared to more malicious adversaries, unable to exploit vulnerabilities beyond passive observation and analysis. Participants in the Honest but Curious model do not have malicious intent, in contrast to those who participate in more adversarial threat models, as their motivation is a curiosity rather than a desire to compromise the security or integrity of the system. This model strikes a balance between assuming that people will be honest and recognizing that some might be curious. It lets us study cryptographic protocols based on realistic assumptions while protecting us from passive attacks.

Researchers use the Threat model to develop sophisticated security frameworks and analysis techniques. The popular assumptions are as follows:

(1) Since the communication between two entities is in an insecure wireless communication channel, an Adv can then impersonate and eavesdrop on the original messages transmitted on public networks.
(2) An Adv can physically capture multiple sensors set up or implanted in a patient's body and then collect all the sensitive information stored in the captured sensors using side-channel or differential power attack scenarios [140].
(3) An Adv may try to hear a legitimate user's activities to gain access, as long as public networks are highly influenced by security threats.
(4) An Adv can hijack the established session states between the truthful parties. This enables A to get any secret credentials and keys utilized throughout the communication session between the parties.
(5) An Adv can be available internally or externally to determine communication access, whereby they can extrapolate public communication parameters, including encryption, public keys, random generators, etc.
(6) The Adv has total control over the channels used to transfer communications, allowing him or her to intercept, remove, and modify messages already present in the channel.
(7) The Adv can create fresh messages and spread them through the channels.
(8) A potential Adv can impersonate a trustworthy party to prevent other trustworthy parties from discovering its genuine identity.
(9) The identical destination party may also receive a message already delivered in the network by Adv.
(10) The Adv can be Honest But Curious (HBC) is one of the participating entities. It will compile all information conceivable from the messages it receives while strictly adhering to the stated protocol.
(11) The Adv may capture the information of communicating entities to infer the patient's sensitive information over the power analysis attack, i.e., from the medical device memory.

6. Counteractions and performance evaluation

In this section, we explore various security solutions provided for the sub-sectors of the IoT-BC ecosystem. Table 4 depicts various cryptographic solutions that could withstand potential attacks. It emphasizes the attack analysis of existing security solutions. Primarily, we discuss various authentication schemes using cryptographic primitives, including one-way hashing, identity-based, ECC, pairing-based, Chebyshev chaotic map-based, and XORing. Later, we evaluate performance

Table 9
Performance evaluation.

Reference	Technique used	PE1	PE2	PE3
Vangala et al. [66]	SC-based BC envisioned authentication scheme	$9T_H + 4T_{ECM}$	2272	11.93 ms
Mishra et al. [127]	Mutual authentication and key agreement scheme	$1T_B + 3T_M + 4T_H + 1T_S$	4606	0.0931 s
Odelu et al. [128]	Secure authenticated key agreement scheme	$4T_{MUL} + 2T_{PAR}$	1504	9.8 ms
Wu et al. [129]	New 2FA scheme for health-care	$2T_S + 10T_H$	3968	0.264 ms
Wu et al [130]	Three factor user authentication scheme	$2T_M + T_{REP} + 11T_H$	2204	22.0631 ms
Sidorov et al. [131]	Ultralightweight mutual authentication RFID scheme	$15T_{HW} + 14T_{ROT} + 12T_{XOR}$	1760	0.00048 s
Khalid et al. [132]	ECC based lightweight authentication protocol	$5T_{SM} + 5T_H + 1T_{PA}$	576	11.1703 ms
Srinivas et al. [133]	Lightweight blockchain-enabled RFID-based authentication	$12T_H + 15T_{ROT} + 25T_{XOR}$	2240	0.00384 s
Mujahid et al. [134]	Ultralightweight RFID authentication for passive low cost tags	$T_{HW} + 29T_{ROT} + 29T_{XOR}$	962	0.00032 s
Wazid et al. [135]	LDAKM-EIoT: Lightweight device authentication scheme	$32T_H$	864	10.24 ms
Garg et al. [136]	BAKMP-IoMT: Blockchain-based authentication scheme	$19T_H + T_{FE}$	1376	23.18 ms
Shariq et al. [137]	RFID authentication protocol using digital Schnorr cryptosystem	$3T_H + 1T_{ME} + 1TSM + 1M$	–	1.8624 ms
Vivek et al. [138]	BC based IoT-D2D authentication protocol	$7T_H + 1T_P$	1984	40.99 ms
Bera et al. [62]	Private BC-envisioned drones-assisted authentication protocol	$2T_{ECA} + 1T_{POLY}$	2016	4.733 ms
Anusha et al. [139]	BC-Based Robust Data Security Scheme	$11T_H + 5T_{ECM} + 2T_{EC}$	1984	14.871 ms

Note: PE1: Computation cost; PE2: Communication cost; PE3: Execution time;
Note: T_{EM} : "time for performing a scale multiplication in an elliptic curve"; T_{EA} : "time for performing a point addition in an elliptic curve"; T_H : "time for performing a cryptographic hash operation"; T_X : "time for performing an XOR operation"; T_{AES} : "time for performing a symmetric encryption operation using Advanced Encryption Standard (AES)".

by considering various metrics, including computation, communication, and execution time, as depicted in Table 9. In addition, we dig into a thorough review of various security solutions to evaluate their performance in other measures, including energy efficiency, privacy preservation, and authentication and authorization depicted in 10, and 11, respectively.

6.1. Attack mitigation techniques and security solutions

In the integration of blockchain with IoT environments, various security challenges arise due to the decentralized architecture and resource-constrained nature of these devices. Various potential attacks were possible due to the integration of IoT environments. However, researchers provides extensive solutions to safeguard IoT environments (see Table 7).

- **Sybil Attack:** Use of permissioned blockchain with Membership Service Providers (MSPs) and decentralized identity frameworks to verify and restrict node identities.
- **Replay Attack:** Employ nonce-based challenge-response protocols and timestamps to ensure message freshness and prevent reuse of old data.
- **Man-in-the-Middle (MitM) Attack:** Implement mutual authentication using TLS/DTLS and utilize blockchain for immutable communication logs.
- **Denial-of-Service (DoS) and Distributed DoS (DDoS) Attacks:** Apply rate limiting, anomaly-based intrusion detection systems (IDS), and adopt consensus protocols like PBFT or DPoS to handle load efficiently.
- **Data Tampering and Forgery:** Utilize cryptographic hashing and Merkle tree structures to validate data integrity; enforce input verification using smart contracts.
- **51% Attack (Consensus Manipulation):** Restrict validator access using permissioned blockchains and implement hybrid consensus mechanisms to prevent centralization.
- **Side-Channel Attack:** Deploy secure hardware components (e.g., TPMs) and obfuscate execution paths through noise injection and randomization.
- **Firmware and Software Hijacking:** Maintain blockchain-based firmware audit trails and verify updates using digital signatures and secure boot mechanisms.
- **Privacy Breach and Tracking:** Apply zero-knowledge proofs (ZKPs), homomorphic encryption, and mix networks to preserve identity and transaction privacy.
- **Blackhole and Sinkhole Routing Attacks:** Use blockchain for decentralized trust scoring and adopt multi-path routing strategies to ensure resilient data forwarding (see Table 8).

6.1.1. Preliminary assumptions

- The blockchain maintains a verified ledger of registered public keys and identities.
- All identities and keys are issued by a smart contract SC_{auth} on BC.
- Communication is over an insecure channel.

6.1.2. Protocol design phases

Phase 1: Registration (One-time)

(1) U_i generates (SK_i, PK_i).
(2) $U_i \rightarrow SC_{auth} : \{ID_i, PK_i, Sig_{SK_i}(ID_i \parallel PK_i)\}$
(3) SC_{auth} verifies the signature and stores (ID_i, PK_i) on-chain.

Table 10
Energy efficiency.

Reference	Methodology	Metrics	New findings
Wang et al. [83]	RescueChain, a secure and efficient information sharing scheme	-Offloading latency -Energy efficiency	-Developed a lightweight BC-based framework for secure data sharing and detecting malware function. -A reputation-based consensus protocol has been developed to improve consensus efficiency. -VFC-based off-chain system offloads UAVs' heavy data computing and storage tasks to ground vehicles.
Amjad et al. [141]	A BC-based node authentication model, DDR-LEACH protocol	-Energy consumption -Throughput	-The node authentication was done to eliminate unauthorized nodes. -Optimal CH selection is done by using the DDR-LEACH protocol. -Data integrity validation was done by AES algorithm, and a formal security analysis was conducted.
Sylla et al. [142]	A BC-enabled decentralized context-aware authorization management architecture	-Energy consumption -Execution time -Token generation time	-A novel BC-based authorization management system was proposed. -Enhance security by using smart contracts. -To enable dynamic and flexible authorization management, integration as a service within any situational security service in the IoT is available.
Hu et al. [143]	A hybrid BC, namely H-chain	-Energy consumption -Computational capability	-Introduced the H-Chain consensus mechanism, which consists of permissioned PoW and PBFT. -By considering various BC factors, an analysis of the energy consumption of permissioned PoW and PBFT consensus mechanisms.
Wadhwa et al. [144]	Consensus approach based on PoW	-Number of blocks -Memory utilization -Energy consumption	-The data transmitted by IoT devices to BC is for security concerns. -Edge networks are used to satisfy the goals of the consensus mechanism for data offloading.
Bakkiam et al. [106]	A lightweight privacy-aware secure authentication (LPASA) scheme	-Energy consumption -Packet delivery ratio -Latency	-Devised authentication protocol (LPASA) presented. -Secure session keys are generated to establish mutual authentication and successful communication. -Proposed protocol evaluated by considering the various parameters presented.

Phase 2: Mutual Authentication

(1) $U_i \rightarrow G_w : ID_i, N_i, TS_1, Sig_{SK_i}(N_i \parallel TS_1)$
(2) G_w queries BC to verify PK_i and signature.
(3) G_w generates N_w, computes $K_{sess} = H(N_i \parallel N_w \parallel TS_1 \parallel TS_2)$
(4) $G_w \rightarrow U_i$: $N_w, TS_2, E_{PK_i}(K_{sess}), Sig_{SK_w}(N_w \parallel TS_2)$
(5) U_i verifies signature, decrypts K_{sess}.

6.1.3. Security goals achieved

- Resistance to φUIAφ, φPIAφ: Smart contract-verified identity + ECC digital signatures.
- Resistance to φREAφ, φMIMAφ: Nonce + timestamp prevents replay; ECC ensures integrity.
- Resistance to φSKAφ, φSVAφ: Ephemeral session keys never reused; verifiers not stored.
- Resistance to φFSNAφ: Blockchain enforces Sybil-proof identity registration.

Attack mitigation strategies follow preliminary assumptions that the blockchain maintains a tamper-resistant ledger of registered identities and public keys, and that all identity credentials are issued and verified by a dedicated smart contract (SC_{auth}), the proposed protocol effectively mitigates a wide spectrum of attacks within the IoT-Blockchain ecosystem. Operating over insecure communication channels, the registration and mutual authentication phases employ strong cryptographic primitives such as ECC-based digital signatures, timestamped nonces, and ephemeral session keys. These mechanisms collectively defend against Sybil identities, replay attacks, man-in-the-middle intrusions, session key compromise, and verifier-based leaks. By leveraging blockchain's immutable infrastructure and decentralized trust enforcement, the protocol ensures secure onboarding, robust mutual authentication, and privacy-preserving session key negotiation. Consequently, the design upholds key security properties such as forward secrecy, mutual trust, identity assurance, and desynchronization resistance, making it well-suited for deployment in resource-constrained and adversarial IoT environments.

6.2. Energy efficiency

This section examines various research works related to BC-based energy-efficient techniques. Wang et al. [83] proposed A secure and efficient scheme to improve consensus efficiency and address security issues. Amjad et al. [141] proposed a BC-based LEACH protocol to improve efficiency and security. Sylla et al. [142] proposed a novel authorization scheme and BC-based framework. Hu et al. [143] proposed a hybrid BC framework and introduced an H-chain consensus mechanism. Wadhwa et al. [144] proposed a Consensus approach to improve the data offloading. Bakkiam et al. [106] proposed the LPASA scheme. As mentioned, all mechanisms improve security and energy efficiency, but energy efficiency and security issues are still open research problems. Required enhanced mechanisms to address these issues. Figure

6.3. Privacy preserving

Privacy preservation is one of the key challenges in BC and IIoT technologies. We analyzed various privacy-preserving mechanisms based on BC and IIoT. Cha. et al. [145] proposed a privacy-aware BC-based gateway. Daghmehchi et al. [146] proposed a Hy-Bridge mechanism to address privacy issues. Chen et al. [117] proposed a BC-based secure data-sharing mechanism using Hyperledger Fabric. Bakkiam et al. [106] proposed a privacy and authentication-based mechanism (LPASA) to withstand various attacks. Dwivedi et al. [147]

Table 11
Privacy preserving.

Reference	Methodology	Metrics	New findings
Cha et al. [145]	A privacy-aware blockchain-connected gateway (BC gateway)	-Computation cost -Security and privacy analysis	-Developed blockchain-connected Gateway. -Improve the user privacy and trust among IoT applications and Devices.
Daghmehchi et al. [146]	A hybrid Blockchain-based billing and charging framework (Hy-Bridge)	-Analysis of Privacy-preserving -Block validation -Power consumption -Anonymity -Information loss	-The proposed framework, Hy-Bridge introduced to link the Blockchain with subnets. -The transactions done between the blocks provide user privacy and anonymization. -Introduced the credit sharing features for IoT.
Chen et al. [117]	An enterprise privacy protection and data sharing scheme based on the Hyperledger Fabric Blockchain	-Throughput -Latency -Computation cost -Communication cost	-Developed a secure data sharing and privacy protection Infrastructure. -Devised a key-chain table for log data. -The proposed scheme achieves the mutual authentication and data integrity.
Bakkiam et al. [106]	A lightweight privacy-aware secure authentication (LPASA) scheme	-Computation cost -Communication cost -Storage cost	-Devised authentication protocol (LPASA) presented. -LPASA withstands various active and passive attacks. -Formal and informal security analysis was done to present the effectiveness of the LPASA protocol.
Dwivedi et al. [147]	A novel hybrid framework of modified BC models	-Confidentiality -Integrity -Availability	-Presented a privacy-preserving ring signature scheme and BC model authentic users and ensuring security. -The proposed model withstands DoS, Mining, Storage and dropping attacks.
Zhang et al. [148]	A BC-based secure and privacy-preserving PHI sharing (BSPP) scheme	-Data security -Privacy preservation -Secure search -Time control	-Presented a BC-based PHI sharing platform for e-health diagnosis improvements. -Developed BC components, including the data structure and consensus mechanism. -BSPP protocol presented for E-Health BC.
Ma et al. [149]	A novel mechanism, namely NOInfer and a new protocol for the Alternating Direction Method of Multipliers (ADMM)	-Privacy (inference attack) -Efficiency	-Developed a single-server architecture of MTL. -Presented the Alternating Direction Method of Multipliers (ADMM) to achieve a training model. -The proposed system resists the inference attack efficiently.
Alcarria et al. [150]	A Blockchain-based authorization system	-Block period -Timestamp -Resource Utilization	-Authorization model used for collecting sensing information from sensor networks -Trustworthy-based token model developed for cryptocurrency
Yavari et al. [151]	An improved BC-based authentication protocol (IBCbAP)	-Security analysis -Resist the Replay attack -Secret discloser attack	-Addressed the issues of Cha et al. [145] BC-based authentication and privacy scheme has security flaws. -IBCbAP security analysis, both formal and informal. The Scyther tool is used for formal proofing. -The proposed IBCbAP method validates the correctness by using Ethereum BC.
Jangirala et al. [133]	A novel lightweight BC-enabled RFID-based authentication protocol (LBRAPS).	-Computation cost -Communication cost	-Designed LBRAPS protocol based on XOR and one-way cryptographic hash. - Analyzed the security of the LBRAPS protocol against various attacks. -Formal security analysis done for LBRAPS using AVISPA tool.

proposed a novel framework to satisfy the security properties. Zhang et al. [148] proposed a BC-based secure and privacy-preserving scheme (BSPP). Ma et al. [149] proposed a novel ADMM mechanism for privacy issues. Besides, various other researchers devised [152–161] novel blockchain enabled privacy-preserving algorithms to withstand potential attacks. The aforementioned works particularly focus on privacy-preserving issues. All these works achieve better results than existing works and effectively withstand various passive and active attacks. We examined all mechanisms that still require enhanced and novel mechanisms to address security and privacy issues and withstand more attacks.

6.4. Authentication and authorization

In this section, we examine various authentication and authorization schemes using BC. Alcarria et al. [150] proposed an authorization scheme using BC. Yavari et al. [151] developed the IBCbAP protocol to withstand reply and secret discovery attacks. Amjad et al. [141] introduced a node authentication protocol to reduce the computational cost. Sylla et al. [142] developed an authorization scheme using a smart contract. Vivekanandan et al. [138] device authentication protocol using BC to reduce the computation cost. Jangirala et al. [133] proposed the LBRAPS protocol and proved their security analysis could withstand potential attacks. The above-mentioned schemes are intended to improve security and performance by considering communication cost, throughput and energy efficiency. But still, authentication and authorization open doors to expanding adversarial capabilities. Thus, it demands novel mechanisms to enhance the security and efficiency of advanced IoT environments.

6.5. Testbed implementation

To validate the proposed Intelligent IoT-Blockchain Ecosystem in the context of smart city integration, a comprehensive application testbed was designed and deployed. The prototype encompasses multiple critical services including decentralized healthcare, real-time traffic management, smart waste collection, and air quality monitoring. Each service module leverages blockchain technology to ensure secure data provenance, trusted interactions, and transparent audit trails.

The decentralized healthcare module consists of three subcomponents: (i) medicine booking, (ii) emergency appointment scheduling, and (iii) blood donor discovery. The user interface was developed using React.js, while backend smart contracts were implemented in Solidity and deployed locally using Ganache. Interaction with the blockchain was facilitated via Web3.js, with MetaMask handling user-side transaction signing. Users were able to book medicines, schedule appointments, and search for verified blood donors based on location, availability, and donation history. All actions were immutably recorded on the blockchain, ensuring traceability and tamper resistance. Figs. 11 and 12 depicts various application integrations associated with smart city using blockchain solutions.

The traffic management module employed sensor-based vehicle density data and edge devices to generate real-time congestion alerts. These were recorded on-chain to avoid tampering and to allow decentralized decision-making by traffic control nodes. Similarly, the smart waste collection system integrated fill-level sensors on municipal bins, with waste data periodically broadcast to a blockchain network. Smart contracts were triggered when thresholds were breached, automatically dispatching collection services and ensuring accountability in waste logistics.

For environmental monitoring, air quality sensors collected PM2.5, PM10, CO_2, and temperature metrics, which were periodically committed to the blockchain. This immutable data store provides trusted public access and supports analytics for pollution mitigation and urban planning. The integrated testbed was hosted in a simulated local environment combining Ethereum blockchain. The results show that the system performs within acceptable latency thresholds, with smart contract execution and transaction confirmation occurring reliably across services. Gas usage varies depending on payload and contract complexity. All modules maintained responsiveness and were resilient to injected faults and simulated attacks, demonstrating robustness and scalability of the architecture. Figs. 13 depicted the performance of the block transactions used within the application.

7. Challenges and future vision

The integration of IoT and blockchain technology presents numerous opportunities but also presents challenges. Scalability is a primary challenge, as both technologies generate vast data. Current blockchain platforms struggle with throughput and latency issues, hindering the real-time processing of IoT data. Interoperability is essential for seamless data exchange and communication, and standards must be established to ensure devices from different manufacturers can work together efficiently. Security is a significant concern in IoT deployments, and blockchain can enhance security by providing a decentralized and immutable ledger. Privacy is another critical aspect, and blockchain's transparency can pose challenges for privacy protection. Cost is another challenge, especially for small and medium-sized enterprises. Regulatory compliance is a significant consideration, especially in industries like healthcare and finance, where strict regulations govern data handling and privacy. Energy efficiency is another concern, and future research may focus on developing energy-efficient consensus mechanisms for blockchain networks and low-power communication protocols for IoT devices. Edge computing can address scalability and latency issues by processing data closer to the source, while AI integration can enhance the capabilities of both IoT and blockchain systems. Supply chain management is a promising application area for IoT and blockchain technology, and collaboration between industry stakeholders, researchers, and policymakers is essential to overcome technical, regulatory, and economic barriers to adoption.

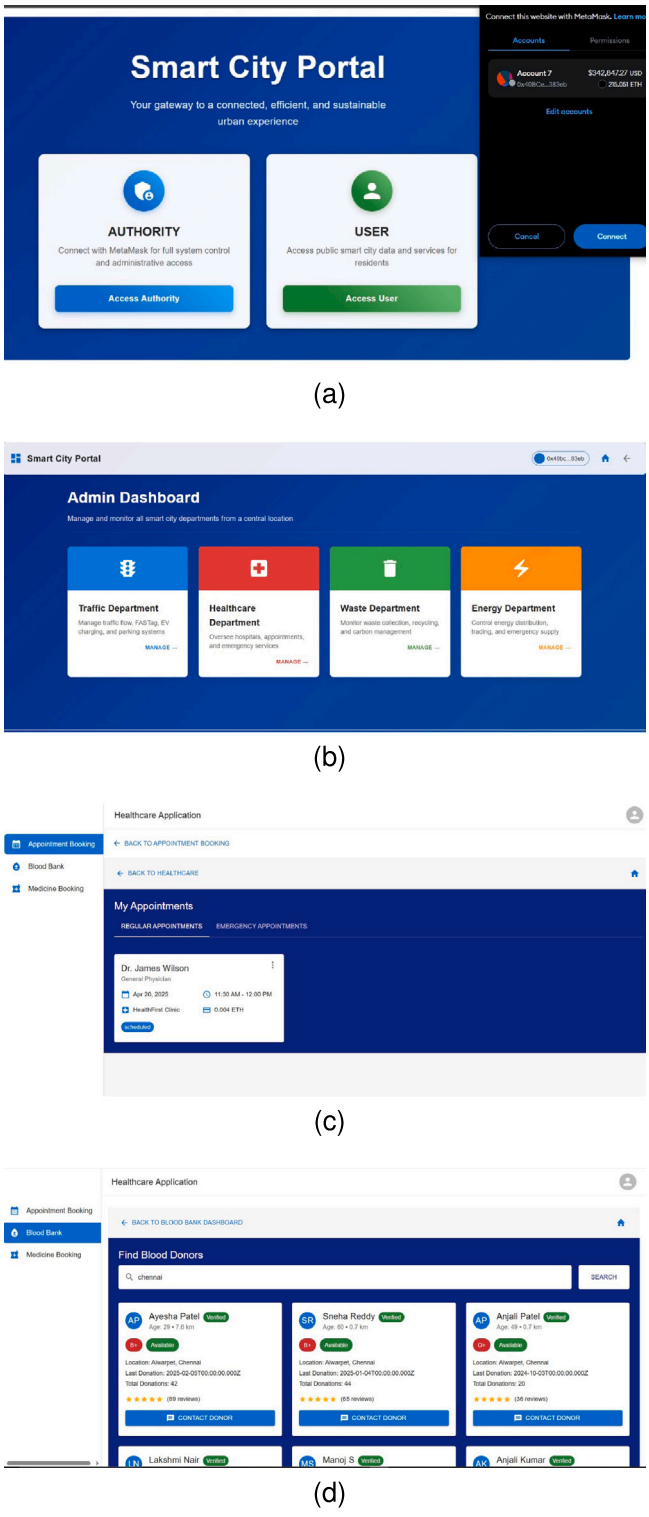

Fig. 11. Testbed results for smart city dashboard.

7.1. Future vision

The mobile telecommunications industry has been debated since the fifth-generation (5G) mobile communications launch. With 5G commercially available, research has shifted to the sixth generation (6G) to improve speed and reliability. However, current networks struggle to handle the increased wireless data traffic from smart technologies,

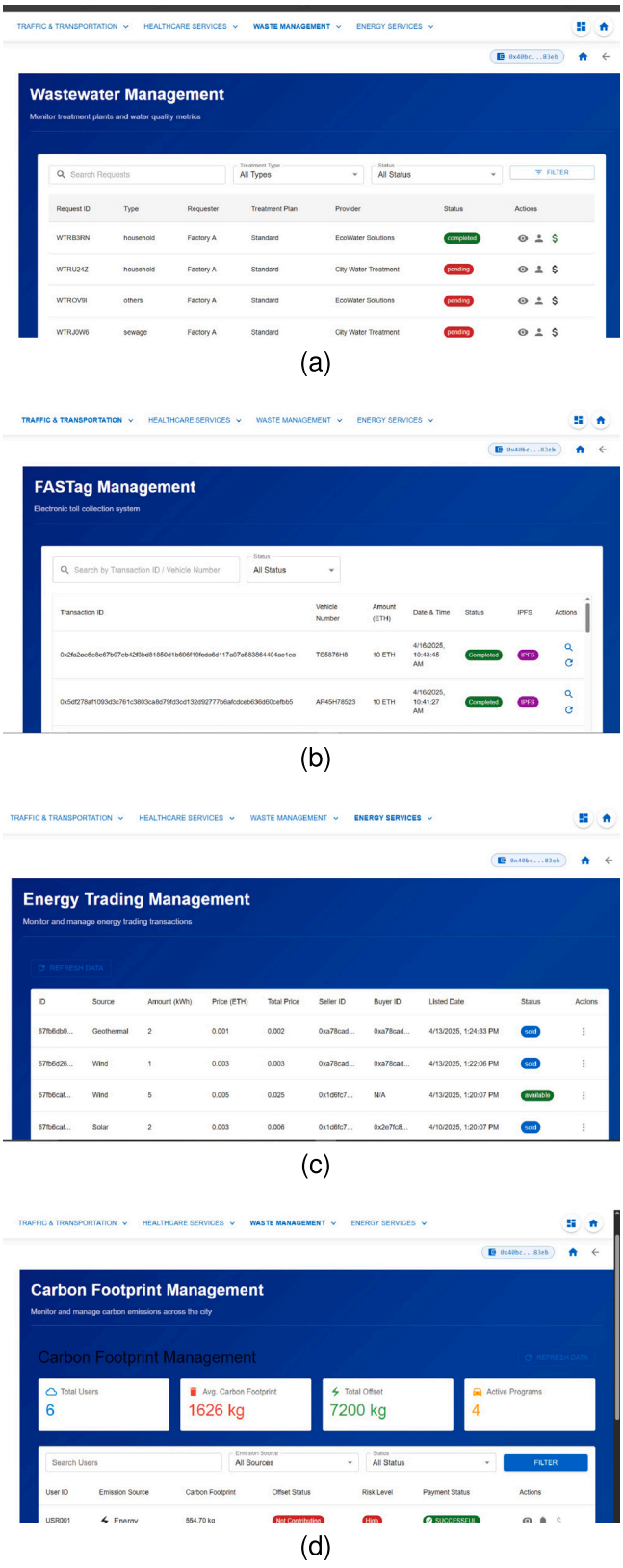

Fig. 12. Testbed results for smart city service integrations.

which include real-time, interactive services. 6G technology was introduced to meet energy-efficient standards, addressing the limitations of current systems. The 6G represents a significant advancement in communication networks. Fig. 14 depicts various trends that must be addressed in future research. With a single platform, 6G offers a variety of applications, such as enhanced mobile broadband communications, automated driving, virtual reality, and the IoT.

The rapid technological advancements of the decade have led to a growing demand for advanced wireless technologies, as depicted in Table 12. The first commercialization system for 6G is expected to be introduced in 2030, aiming for a highly connected, instantaneous global digital civilization. 6G will integrate wireless connectivity with technological capabilities like caching, communication, processing, control, image, and navigation, supporting full-vertical applications like positioning, radar, and sensing.

By skillfully utilizing the benefits that blockchain technology, IPFS, machine learning, and decentralized communication offer, the system emerges as a strong and statistically reliable solution for managing automobile communications. Its potential influence extends across a wide range of sectors, including smart cities, logistics, and transportation, and it provides a statistically robust foundation for improving the efficacy, security, and trustworthiness of communication systems.

Machine learning (ML) algorithms are widely used in various communication technologies to improve system performance regarding security, efficiency, latency, and throughput. However, addressing security issues using ML and deep learning (DL) algorithms is challenging. Using adversarial training to protect 6G ML models for predicting millimeter-wave (mmWave) beams from attacks was suggested by Catak et al. [116]. This would make ML and AI models safer. If DL model security risks increase, further research is needed in the 6G field.

Several authors have systematically reviewed 5G and 6G technology, their features, and future directions. Alraih et al. [163]compared 5G and 6G technology, providing use cases, vision, applications, technical requirements, and frequency. Sandeepa et al. [162] conducted a comprehensive study on B5G/6G network privacy-related issues, discussing the security and privacy goals of 5G and 6G networks. Aslam et al. [164] highlighted the importance of 6G technology in addressing security and privacy issues, as it will not be able to keep up with wireless communication network expansion by 2030. Abdel et al. [114] discussed enhancements over 5G and 6G security architectures, security concerns, and difficulties associated with the 6G physical layer.

The following are some of the future research directions and ideas we plan to pursue to solidify this research:

- Transitioning from simulation to a tangible prototype will provide insights into practical challenges and feasibility.
- Initial trials will help validate the system's functionality and gather user feedback for refinement.
- Assessing the system's efficiency and ability to handle increased loads or data volumes is crucial for its broader adoption.
- Strengthening the security measures to safeguard data integrity and protect against potential threats.
- Continuously refining the ML algorithms to improve accuracy and efficiency in classification, prioritization, and spam detection tasks.
- Ensuring the system's compatibility with existing infrastructures and advocating for industry standards to facilitate integration.

By concentrating on these areas of improvement, we want to improve the system's reliability and general effectiveness. We anticipate a future in which the system establishes new performance standards and serves as a foundation for developing connected car solutions. This will be accomplished by performing extensive pilot tests, refining security measures, and investigating ethical aspects. Table 13 depicts the acronyms used.

7.2. Lessons learned

From our exploration of intelligent IoT-Blockchain ecosystems, several key insights have emerged that are critical for future research and deployment:

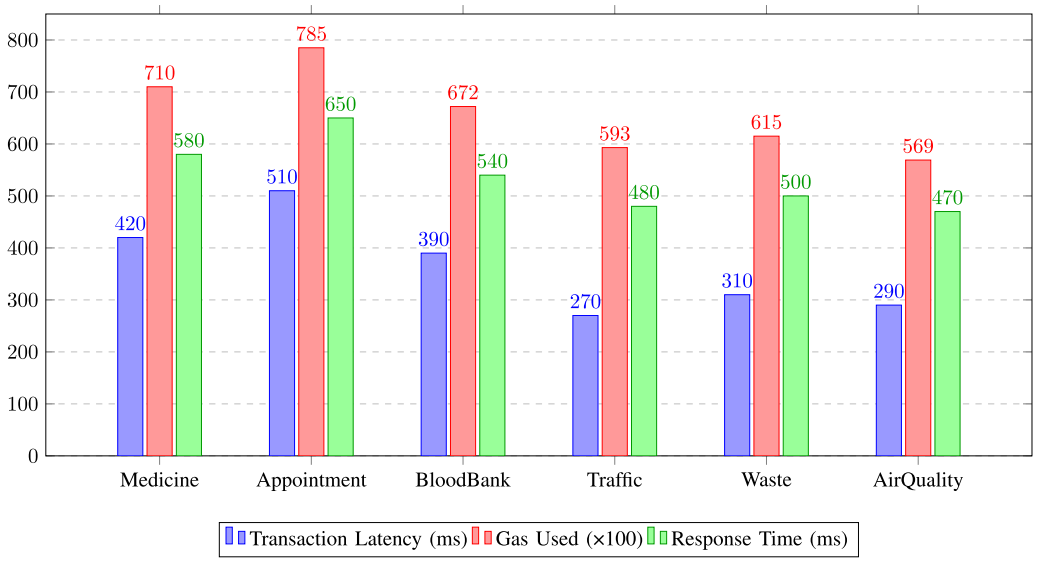

Fig. 13. Performance evaluation of smart city modules.

Table 12
Comparison between 5G and 6G [162].

Performance requirement	5G KPIs	6G KPIs
Peak data rate	20 Gb/s	1 Tb/s
User experienced data rate	100 Mb/s	1 Gb/s
Control plane latency	10 ms	<1 ms
User plane latency	eMBB < 4 ms URLLC < 0.5 ms	< 0.1 ms
Reliability	99.999%	>99.99999%
Mobility	500 km/h	1000 km/h
Connection density	1 million devices per km^2	10–100 million devices per km^2
Area traffic capacity	10 $Mb/s/m^2$	1 $Gb/s/m^2$
Spectral efficiency	DL: 30 bps/Hz UL: 15 bps/Hz	2–3 times compared to 5G
Network energy efficiency	10–100 × that of 4G	10–100 × that of 5G
Network energy efficiency	–	10–1000 times compared to 5G
Positioning accuracy	Outdoor: 10 m Indoor: 3 m	Outdoor: sub-meter level

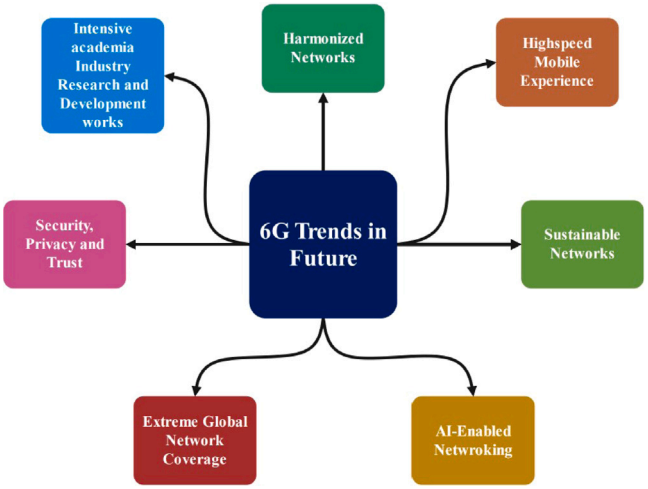

Fig. 14. Future trends in 6G technology.

- **Security is multifaceted and context-dependent.** Integrating blockchain with IoT addresses many traditional security challenges, such as data integrity, access control, and trust management. However, it introduces new threats, particularly at the consensus and smart contract layers, which must be carefully addressed using context-aware protocols.
- **Privacy cannot be an afterthought.** While blockchain ensures transparency and immutability, it can inadvertently expose sensitive information. Balancing transparency with user and device privacy requires advanced techniques such as zero-knowledge proofs, off-chain storage, and permissioned ledger configurations.
- **Scalability requires more than just throughput optimization.** Our study highlights that scalability in IoT-Blockchain systems encompasses node management, latency control, energy efficiency, and data synchronization. Relying solely on increasing transactions per second is insufficient for large-scale IoT integration.
- **Consensus mechanisms must be tailored to IoT constraints.** Lightweight, low-latency consensus algorithms like PBFT, PoA, or DAG-based models are more suitable for resource-constrained IoT devices than traditional Proof-of-Work schemes.
- **Smart contracts need formal verification.** Vulnerabilities in smart contract code can severely impact system integrity. Rigorous testing and formal methods are essential to prevent exploits and ensure secure automation.
- **Cross-layer collaboration is essential.** Security and performance improvements cannot rely solely on a single layer (e.g., blockchain or IoT protocols). Effective protection requires coordinated mechanisms across hardware, network, consensus, and application layers.

These lessons emphasize the need for interdisciplinary approaches, combining insights from distributed systems, cryptography, embedded computing, and AI to build scalable and secure IoT-Blockchain ecosystems.

Table 13
Acronym and Definition.

Acronym	Definition
IoT	– Internet of Things
WSN	– Wireless sensor Networks
M2M	– Machine to Machine
H2M	– Human to Machine
BCA	– Blockchain Architecture
BC	– Blockchain
N-IoT	– Network Internet of Things
RFID	– Radio Frequency Identification
PLC	– Power Line Communication
CPS	– Cyber-physical Systems
ICPS	– Industrial Cyber-Physical Systems
MiTM	– Man in the middle
ESL	– Ephemeral Secret Leaking
BC	– Blockchain
DLT	– Distributed Ledger Technology
P2P	– Peer to Peer
PoW	– Proof of Work
PoS	– Proof of Stake
DPoS	– Delegated Proof of Stake
PBST	– Practical Byzantine Fault Tolerance
DAG	– Directed Acyclic Graph
VM	– Virtual Machine
TEE	– Trusted Execution Environment
SMPC	– Secure Multi-Party Computation
ZKP	– Zero-Knowledge Proof
ABSE	– Attribute-based Searchable Encryption
SVM	– Support Vector Machine
E2E	– End to End
IIoT	– Industrial Internet of Things
RSU	– Road Side Units
CS	– Crowd Sourcing
EHR	– Electronic Health Record
PHR	– Personal Health Record
DConBE	– Dynamic contributory broadcast encryption
DPPoW	– Designated Prover Proof of Work
IHE	– Integrating the Healthcare Enterprise
FHIR	– Fast Healthcare Interoperability Resources
BHER	– Blockchain-based E-Health Record
TCP	– Transmission Control Protocol
UDP	– User Datagram Protocol
UAV	– Unmanned Arial Vehicle
GNSS	– Global Navigation Satellite System
DSB	– Disaster Semantic Blockchain
VFC	– Vehicular Fog Computing
U2U	– UAV to UAV
ICT	– Information and Communication Technology
CSP	– Cloud Service Provider
DAO	– Decentralized autonomous organization
RSA	– Rivest, Shamir, Adleman
SHA	– Secure Hash Algorithm
AES	– Advanced Encryption Standard
ML/DL	– Machine Learning/Deep Learning
DoS	– Denial of Service
LEACH	– Low Energy Adaptive Clustering Hierarchy
KPI	– Key Performance Indicators

8. Conclusion

With the growing use of IoT devices in everyday life, security and privacy have become major concerns specifically in environments that are dynamic, diverse, and often resource-limited. Integrating blockchain into IoT systems offers a strong foundation to solve problems like data tampering, unauthorized access, and trust management. However, building secure systems in such complex networks requires flexible, smart solutions that can adapt to different devices, users, and threat situations.

In this paper, we provided a detailed and structured overview of the intelligent IoT-Blockchain (IoT-BC) ecosystem, focusing on both security and privacy challenges. We reviewed various authentication techniques such as identity-based, two-factor, and multi-factor methods, which can help protect devices and user data. Our analysis shows that traditional security methods are not enough for modern IoT systems. Instead, decentralized and privacy-preserving methods are needed to support safe and secure communication.

We also highlighted the importance of trusted device interactions and secure information sharing between machines. Blockchain helps by offering tamper-proof data storage, smart contract automation, and secure access control. Still, there are challenges like smart contract bugs, limited scalability, and data privacy that must be addressed.

Finally, we discussed future directions such as using 5G and 6G networks, building strong consensus methods, and combining edge computing with blockchain. These ideas aim to make IoT systems more intelligent, secure, and efficient. Overall, this paper lays the groundwork for designing secure and reliable IoT-Blockchain solutions and points out future areas of research to make these systems even better.

CRediT authorship contribution statement

Muralidhara Rao Patruni: Conception and design, Analysis and interpretation of the data, Drafting the article or revising it critically for important intellectual content, Approval of the final version. **Bhasker Bapuram:** Conception and design, Analysis and interpretation of the data, Drafting the article or revising it critically for important intellectual content, Approval of the final version. **Saraswathi Pedada:** Conception and design, Analysis and interpretation of the data, Drafting the article or revising it critically for important intellectual content, Approval of the final version.

Code availability

No code is used

Declaration of competing interest

All the authors do not have any conflict of Interest

Data availability

No data was used for the research described in the article.

References

[1] M. Vaezi, A. Azari, S.R. Khosravirad, M. Shirvanimoghaddam, M.M. Azari, D. Chasaki, P. Popovski, Cellular, wide-area, and non-terrestrial IoT: A survey on 5G advances and the road towards 6G, IEEE Commun. Surv. Tutor. (2022).
[2] J. Chen, J. Patra, M. Pradel, Y. Xiong, H. Zhang, D. Hao, L. Zhang, A survey of compiler testing, ACM Comput. Surv. 53 (1) (2020) 1–36.
[3] R. Choudhary, Y. Shaik, P. Yadav, A. Rashid, Generational differences in technology behavior: A systematic literature review, J. Infrastruct. Policy Dev. 8 (9) (2024) 6755.
[4] D.H. An, Blockchain Applications in Agriculture, Vernon Art and Science Incorporated, 2024.
[5] V. Shah, V. Thakkar, A. Khang, Electronic health records security and privacy enhancement using blockchain technology, in: Data-Centric AI Solutions and Emerging Technologies in the Healthcare Ecosystem, CRC Press, 2023, pp. 1–13.
[6] S. Biswas, K. Sharif, F. Li, I. Alam, S.P. Mohanty, DAAC: Digital asset access control in a unified blockchain based e-health system, IEEE Trans. Big Data 8 (5) (2020) 1273–1287.
[7] S. Biswas, K. Sharif, F. Li, Z. Latif, S.S. Kanhere, S.P. Mohanty, Interoperability and synchronization management of blockchain-based decentralized e-health systems, IEEE Trans. Eng. Manage. 67 (4) (2020) 1363–1376.
[8] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, N. Kumar, Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications, IEEE Trans. Netw. Sci. Eng. 8 (2) (2019) 1242–1255.
[9] I.U. Din, M. Guizani, S. Hassan, B.-S. Kim, M.K. Khan, M. Atiquzzaman, S.H. Ahmed, The internet of things: A review of enabled technologies and future challenges, Ieee Access 7 (2018) 7606–7640.

[10] B.D. Deebak, F.H. Memon, S.A. Khowaja, K. Dev, W. Wang, N.M.F. Qureshi, In the digital age of 5G networks: Seamless privacy-preserving authentication for cognitive-inspired internet of medical things, IEEE Trans. Ind. Inform. 18 (12) (2022) 8916–8923.

[11] B.D. Deebak, S.O. Hwang, A cloud-assisted medical cyber-physical system using a privacy-preserving key agreement framework and a Chebyshev chaotic map, IEEE Syst. J. (2023).

[12] B. Deebak, S.O. Hwang, Healthcare applications using blockchain with a cloud-assisted decentralized privacy-preserving framework, IEEE Trans. Mob. Comput. (2023).

[13] P.M. Rao, B. Deebak, Lightweight two-factor authentication framework with privacy preserving for smart ehealth, Peer-To-Peer Netw. Appl. 17 (1) (2024) 373–396.

[14] B. Deebak, S.O. Hwang, Privacy preserving based on seamless authentication with provable key verification using mIoMT for B5G-enabled healthcare systems, IEEE Trans. Serv. Comput. (2024).

[15] B.D. Deebak, F. Al-Turjman, A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks, Ad Hoc Networks 97 (2020) 102022.

[16] P.M. Rao, B.D. Deebak, Security and privacy issues in smart cities/industries: Technologies, applications, and challenges, J. Ambient. Intell. Humaniz. Comput. 14 (8) (2023) 10517–10553.

[17] O. Gungor, T. Rosing, B. Aksanli, Adversarial-hd: Hyperdimensional computing adversarial attack design for secure industrial internet of things, in: Proceedings of Cyber-Physical Systems and Internet of Things Week 2023, 2023, pp. 1–6.

[18] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, Cyber-physical systems and their security issues, Comput. Ind. 100 (2018) 212–223.

[19] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, S.W. Kim, Smart contract privacy protection using AI in cyber-physical systems: Tools, techniques and challenges, IEEE Access 8 (2020) 24746–24772.

[20] J. Dispan, Confidential computing via multiparty computation and trusted computing, 2023.

[21] H. Zhong, Y. Sang, Y. Zhang, Z. Xi, Secure multi-party computation on blockchain: An overview, in: Parallel Architectures, Algorithms and Programming: 10th International Symposium, PAAP 2019, Guangzhou, China, December 12–14, 2019, Revised Selected Papers 10, Springer, 2020, pp. 452–460.

[22] B.B. Gupta, K.-C. Li, V.C. Leung, K.E. Psannis, S. Yamaguchi, et al., Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system, IEEE/CAA J. Autom. Sin. 8 (12) (2021) 1877–1890.

[23] Q. Mei, H. Xiong, Y.-C. Chen, C.-M. Chen, Blockchain-enabled privacy-preserving authentication mechanism for transportation CPS with cloud-edge computing, IEEE Trans. Eng. Manage. (2022).

[24] T. Chen, L. Zhang, K.-K.R. Choo, R. Zhang, X. Meng, Blockchain-based key management scheme in fog-enabled IoT systems, IEEE Internet Things J. 8 (13) (2021) 10766–10778.

[25] X. Zhou, J. Huang, F. Chen, Y. Tang, C. Wang, T. Wang, D. Xie, C. Zhao, A threshold signature scheme without trusted center for blockchain-based medical cyber-physical systems, 2021.

[26] A.K. Das, B. Bera, S. Saha, N. Kumar, I. You, H.-C. Chao, AI-envisioned blockchain-enabled signature-based key management scheme for industrial cyber–physical systems, IEEE Internet Things J. 9 (9) (2021) 6374–6388.

[27] T.A. Alghamdi, R. Khalid, N. Javaid, A survey of blockchain based systems: Scalability issues and solutions, applications and future challenges, IEEE Access (2024).

[28] E. Harjula, T. Kumar, J. Islam, M. Ejaz, I. Kovacevic, Distributed network and service architecture for future digital healthcare, Finn. J. EHealth EWelfare 14 (1) (2022) 6–18.

[29] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, G. Dhiman, Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives, J. Food Quality 2021 (2021).

[30] P.M. Rao, B. Deebak, Security and privacy issues in smart cities/industries: Technologies, applications, and challenges, J. Ambient. Intell. Humaniz. Comput. (2022) 1–37.

[31] C. De Alwis, P. Porambage, K. Dev, T.R. Gadekallu, M. Liyanage, A survey on network slicing security: Attacks, challenges, solutions and research directions, IEEE Commun. Surv. Tutor. (2023).

[32] J. Zheng, C. Dike, S. Pancari, Y. Wang, G.C. Giakos, W. Elmannai, B. Wei, An in-depth review on blockchain simulators for IoT environments, Futur. Internet 14 (6) (2022) 182.

[33] M.S. ur Rahman, M.A. Islam, M.A. Uddin, G. Stea, A survey of blockchain-based IoT ehealthcare: Applications, research issues, and challenges, 2022.

[34] E.M. Adere, Blockchain in healthcare and IoT: A systematic literature review, Array (2022) 100139.

[35] J.W. Heo, G.S. Ramachandran, A. Dorri, R. Jurdak, Blockchain data storage optimisations: A comprehensive survey, ACM Comput. Surv. (2024).

[36] A. Shahidinejad, J. Abawajy, An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT, ACM Comput. Surv. (2024).

[37] M. Xu, Y. Guo, C. Liu, Q. Hu, D. Yu, Z. Xiong, D. Niyato, X. Cheng, Exploring blockchain technology through a modular lens: A survey, ACM Comput. Surv. 56 (9) (2024) 1–39.

[38] Y. Liu, J. Wang, Z. Yan, Z. Wan, R. Jäntti, A survey on blockchain-based trust management for internet of things, IEEE Internet Things J. 10 (7) (2023) 5898–5922.

[39] A.A. Khan, S. Bourouis, M. Kamruzzaman, M. Hadjouni, Z.A. Shaikh, A.A. Laghari, H. Elmannai, S. Dhahbi, Data security in healthcare industrial internet of things with blockchain, IEEE Sens. J. (2023).

[40] P.M. Rao, B.D. Deebak, A comprehensive survey on authentication and secure key management in internet of things: Challenges, countermeasures, and future directions, Ad Hoc Netw. 146 (2023) 103159.

[41] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, A survey on the adoption of blockchain in IoT: Challenges and solutions, Blockchain Res. Appl. 2 (2) (2021) 100006.

[42] M. El-Hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, A survey of internet of things (IoT) authentication schemes, Sensors 19 (5) (2019) 1141.

[43] A.K. Das, A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks, Peer-To-Peer Netw. Appl. 9 (1) (2016) 223–244.

[44] Q. Jiang, J. Ma, X. Lu, Y. Tian, An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks, Peer-To-Peer Netw. Appl. 8 (6) (2015) 1070–1081.

[45] M. Wazid, J. Singh, A.K. Das, S. Shetty, M.K. Khan, J.J. Rodrigues, ASCP-IoMT: AI-enabled lightweight secure communication protocol for internet of medical things, IEEE Access (2022).

[46] P. Mall, R. Amin, A.K. Das, M.T. Leung, K.-K.R. Choo, PUF-based authentication and key agreement protocols for IoT, WSNs and smart grids: A comprehensive survey, IEEE Internet Things J. (2022).

[47] F. Javed, K. Antevski, J. Mangues-Bafalluy, L. Giupponi, C.J. Bernardos, Distributed ledger technologies for network slicing: A survey, IEEE Access 10 (2022) 19412–19442.

[48] S. Singh, A.S. Hosen, B. Yoon, Blockchain security attacks, challenges, and solutions for the future distributed IoT network, IEEE Access 9 (2021) 13938–13959.

[49] S. Latif, Z. Idrees, Z. e Huma, J. Ahmad, Blockchain technology for the industrial internet of things: A comprehensive survey on security challenges, architectures, applications, and future research directions, Trans. Emerg. Telecommun. Technol. 32 (11) (2021) e4337.

[50] B. Deebak, F.H. Memon, S.A. Khowaja, K. Dev, W. Wang, N.M.F. Qureshi, C. Su, Lightweight blockchain based remote mutual authentication for AI-empowered IoT sustainable computing systems, IEEE Internet Things J. (2022).

[51] A. Vangala, B. Bera, S. Saha, A.K. Das, N. Kumar, Y. Park, Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems, IEEE Sens. J. 21 (14) (2020) 15824–15838.

[52] M. Wazid, A.K. Das, R. Hussain, N. Kumar, S. Roy, BUAKA-CS: Blockchain-enabled user authentication and key agreement scheme for crowdsourcing system, J. Syst. Archit. 123 (2022) 102370.

[53] M. Elkhodr, S. Khan, E. Gide, A novel semantic IoT middleware for secure data management: Blockchain and AI-driven context awareness, Futur. Internet 16 (1) (2024) 22.

[54] K. Zaghouani, B. Djamaa, A. Yachir, DRDChain: A blockchain-based distributed resource directory for the internet of things, Clust. Comput. 27 (3) (2024) 3853–3874.

[55] S.S. Panda, D. Jena, B.K. Mohanta, S. Ramasubbareddy, M. Daneshmand, A.H. Gandomi, Authentication and key management in distributed IoT using blockchain technology, IEEE Internet Things J. 8 (16) (2021) 12947–12954.

[56] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.

[57] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, Y. Yang, A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling, ACM Comput. Surv. 53 (1) (2020) 1–32.

[58] K. Zaghouani, A. Yachir, B. Djamaa, A. Boutouba, Adoption and application of blockchain technology in IoT: Survey and open issues, in: 2023 International Conference on Advances in Electronics, Control and Communication Systems, ICAECCS, IEEE, 2023, pp. 1–6.

[59] S. Banerjee, B. Bera, A.K. Das, S. Chattopadhyay, M.K. Khan, J.J. Rodrigues, Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT, Comput. Commun. 169 (2021) 99–113.

[60] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, E. Di Sciascio, Supply chain object discovery with semantic-enhanced blockchain, in: Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems, 2017, pp. 1–2.

[61] A. Vangala, A.K. Das, N. Kumar, M. Alazab, Smart secure sensing for IoT-based agriculture: Blockchain perspective, IEEE Sens. J. 21 (16) (2020) 17591–17607.

[62] B. Bera, A. Vangala, A.K. Das, P. Lorenz, M.K. Khan, Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment, Comput. Stand. Interfaces 80 (2022) 103567.

[63] M.P. Caro, M.S. Ali, M. Vecchio, R. Giaffreda, Blockchain-based traceability in agri-food supply chain management: A practical implementation, in: 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany, IOT Tuscany, IEEE, 2018, pp. 1–4.

[64] H.-T. Wu, C.-W. Tsai, An intelligent agriculture network security system based on private blockchains, J. Commun. Netw. 21 (5) (2019) 503–508.
[65] J. Arshad, M.A.B. Siddique, Z. Zulfiqar, A. Khokhar, S. Salim, T. Younas, A.U. Rehman, A. Asad, A novel remote user authentication scheme by using private blockchain-based secure access control for agriculture monitoring, in: 2020 International Conference on Engineering and Emerging Technologies, ICEET, IEEE, 2020, pp. 1–9.
[66] A. Vangala, A.K. Sutrala, A.K. Das, M. Jo, Smart contract-based blockchain-envisioned authentication scheme for smart farming, IEEE Internet Things J. 8 (13) (2021) 10792–10806.
[67] J. Hua, X. Wang, M. Kang, H. Wang, F.-Y. Wang, Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping, in: 2018 IEEE Intelligent Vehicles Symposium, IV, IEEE, 2018, pp. 97–101.
[68] J.P.d.B. Gonçalves, H.C. de Resende, R.d.S. Villaca, E. Municio, C.B. Both, J.M. Marquez-Barja, Distributed network slicing management using blockchains in E-health environments, Mob. Netw. Appl. 26 (5) (2021) 2111–2122.
[69] B. Mallikarjuna, D. Kiranmayee, V. Saritha, P.V. Krishna, Development of efficient E-health records using IoT and blockchain technology, in: ICC 2021-IEEE International Conference on Communications, IEEE, 2021, pp. 1–7.
[70] A.I. Taloba, A. Rayan, A. Elhadad, A. Abozeid, O.R. Shahin, R.M. Abd El-Aziz, A framework for secure healthcare data management using blockchain technology, Int. J. Adv. Comput. Sci. Appl. 12 (12) (2021).
[71] J.W. Kim, S.J. Kim, W.C. Cha, T. Kim, A blockchain-applied personal health record application: Development and user experience, Appl. Sci. 12 (4) (2022) 1847.
[72] M. Zarour, M.T.J. Ansari, M. Alenezi, A.K. Sarkar, M. Faizan, A. Agrawal, R. Kumar, R.A. Khan, Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records, IEEE Access 8 (2020) 157959–157973.
[73] A.I. Khan, A. ALGhamdi, F.J. Alsolami, Y.B. Abushark, A. Almalawi, A.M. Ali, A. Agrawal, R. Kumar, R.A. Khan, Integrating blockchain technology into healthcare through an intelligent computing technique, CMC-Comput. Mater. Continua 70 (2022) 2835–2860.
[74] M. Ejaz, T. Kumar, I. Kovacevic, M. Ylianttila, E. Harjula, Health-blockedge: Blockchain-edge framework for reliable low-latency digital healthcare applications, Sensors 21 (7) (2021) 2502.
[75] S. Bittins, G. Kober, A. Margheri, M. Masi, A. Miladi, V. Sassone, Healthcare data management by using blockchain technology, in: Applications of Blockchain in Healthcare, Springer, 2021, pp. 1–27.
[76] M. Ciampi, A. Esposito, F. Marangio, M. Sicuranza, G. Schmid, Modernizing healthcare by using blockchain, in: Applications of Blockchain in Healthcare, Springer, 2021, pp. 29–67.
[77] M. Vahdati, K. Gholizadeh HamlAbadi, A.M. Saghiri, IoT-based healthcare monitoring using blockchain, in: Applications of Blockchain in Healthcare, Springer, 2021, pp. 141–170.
[78] B. Ikharo, A. Obiagwu, C. Obasi, S.U. Hussein, P. Akah, Security for internet-of-things enabled E-health using blockchain and artificial intelligence: A novel integration framework, in: 2021 1st International Conference on Multidisciplinary Engineering and Applied Science, ICMEAS, IEEE, 2021, pp. 1–4.
[79] P. Tagde, S. Tagde, T. Bhattacharya, P. Tagde, H. Chopra, R. Akter, D. Kaushik, M. Rahman, et al., Blockchain and artificial intelligence technology in e-Health, Environ. Sci. Pollut. Res. 28 (38) (2021) 52810–52831.
[80] G. Nagasubramanian, R.K. Sakthivel, R. Patan, A.H. Gandomi, M. Sankayya, B. Balusamy, Securing e-health records using keyless signature infrastructure blockchain technology in the cloud, Neural Comput. Appl. 32 (3) (2020) 639–647.
[81] M.A. Almaiah, F. Hajjej, A. Ali, M.F. Pasha, O. Almomani, A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS, Sensors 22 (4) (2022) 1448.
[82] N. Garg, M.S. Obaidat, M. Wazid, A.K. Das, D.P. Singh, SPCS-IoTEH: Secure privacy-preserving communication scheme for IoT-enabled e-health applications, in: ICC 2021-IEEE International Conference on Communications, IEEE, 2021, pp. 1–6.
[83] Y. Wang, Z. Su, Q. Xu, R. Li, T.H. Luan, Lifesaving with RescueChain: Energy-efficient and partition-tolerant blockchain based secure information sharing for UAV-aided disaster rescue, in: IEEE INFOCOM 2021-IEEE Conference on Computer Communications, IEEE, 2021, pp. 1–10.
[84] T. Rana, A. Shankar, M.K. Sultan, R. Patan, B. Balusamy, An intelligent approach for UAV and drone privacy security using blockchain methodology, in: 2019 9th International Conference on Cloud Computing, Data Science & Engineering, Confluence, IEEE, 2019, pp. 162–167.
[85] M.S. Kumar, S. Vimal, N. Jhanjhi, S.S. Dhanabalan, H.A. Alhumyani, Blockchain based peer to peer communication in autonomous drone operation, Energy Rep. 7 (2021) 7925–7939.
[86] G. Li, B. He, Z. Wang, X. Cheng, J. Chen, Blockchain-enhanced spatiotemporal data aggregation for UAV-assisted wireless sensor networks, IEEE Trans. Ind. Inform. (2021).
[87] X. Xu, H. Zhao, H. Yao, S. Wang, A blockchain-enabled energy-efficient data collection system for UAV-assisted IoT, IEEE Internet Things J. 8 (4) (2020) 2431–2443.
[88] M.H. Meng, Y. Qian, A blockchain aided metric for predictive delivery performance in supply chain management, in: 2018 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI, IEEE, 2018, pp. 285–290.
[89] S. Jabbar, H. Lloyd, M. Hammoudeh, B. Adebisi, U. Raza, Blockchain-enabled supply chain: analysis, challenges, and future directions, Multimedia Syst. 27 (4) (2021) 787–806.
[90] P.K. Wan, L. Huang, H. Holtskog, Blockchain-enabled information sharing within a supply chain: A systematic literature review, IEEE Access 8 (2020) 49645–49656.
[91] M.A. Agi, A.K. Jha, Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption, Int. J. Prod. Econ. 247 (2022) 108458.
[92] J. Li, A. Maiti, M. Springer, T. Gray, Blockchain for supply chain quality management: Challenges and opportunities in context of open manufacturing and industrial internet of things, Int. J. Comput. Integr. Manuf. 33 (12) (2020) 1321–1355.
[93] S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management, Int. J. Prod. Res. 57 (7) (2019) 2117–2135.
[94] M. Shoaib, M.K. Lim, C. Wang, An integrated framework to prioritize blockchain-based supply chain success factors, Ind. Manag. Data Syst. (2020).
[95] U. Javaid, B. Sikdar, A checkpoint enabled scalable blockchain architecture for industrial internet of things, IEEE Trans. Ind. Inform. 17 (11) (2020) 7679–7687.
[96] M. Kaur, M.Z. Khan, S. Gupta, A. Alsaeedi, Adoption of blockchain with 5G networks for industrial IoT: Recent advances, challenges, and potential solutions, IEEE Access (2021).
[97] X. Lin, J. Zhang, L. Xiang, X. Ge, Energy consumption optimization for UAV assisted private blockchain-based IIoT networks, in: 2021 IEEE 94th Vehicular Technology Conference, VTC2021-Fall, IEEE, 2021, pp. 1–7.
[98] M. Liu, F.R. Yu, Y. Teng, V.C. Leung, M. Song, Performance optimization for blockchain-enabled industrial internet of things (IIoT) systems: A deep reinforcement learning approach, IEEE Trans. Ind. Inform. 15 (6) (2019) 3559–3570.
[99] V.R. Kebande, A.I. Awad, Industrial internet of things ecosystems security and digital forensics: Achievements, open challenges, and future directions, ACM Comput. Surv. 56 (5) (2024) 1–37.
[100] M.S. Rahman, I. Khalil, N. Moustafa, A.P. Kalapaaking, A. Bouras, A blockchain-enabled privacy-preserving verifiable query framework for securing cloud-assisted industrial internet of things systems, IEEE Trans. Ind. Inform. (2021).
[101] Q. Wang, X. Zhu, Y. Ni, L. Gu, H. Zhu, Blockchain for the IoT and industrial IoT: A review, Internet Things 10 (2020) 100081.
[102] W. Fei, H. Ohno, S. Sampalli, A systematic review of IoT security: Research potential, challenges, and future directions, ACM Comput. Surv. 56 (5) (2023) 1–40.
[103] S. Son, J. Lee, M. Kim, S. Yu, A.K. Das, Y. Park, Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain, IEEE Access 8 (2020) 192177–192191.
[104] P. Bagga, A.K. Sutrala, A.K. Das, P. Vijayakumar, Blockchain-based batch authentication protocol for internet of vehicles, J. Syst. Archit. 113 (2021) 101877.
[105] A.K. Das, M. Wazid, N. Kumar, M.K. Khan, K.-K.R. Choo, Y. Park, Design of secure and lightweight authentication protocol for wearable devices environment, IEEE J. Biomed. Heal. Inform. 22 (4) (2017) 1310–1322.
[106] D. Bakkiam Deebak, F. AL-Turjman, Lightweight privacy-aware secure authentication scheme for cyber-physical systems in the edge intelligence era, Concurr. Comput.: Pr. Exp. (2021) e6510.
[107] B.D. Deebak, F. Al-Turjman, Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things, IEEE J. Sel. Areas Commun. 39 (2) (2020) 346–360.
[108] A.-T. Fadi, B.D. Deebak, Seamless authentication: For IoT-big data technologies in smart industrial application systems, IEEE Trans. Ind. Inform. 17 (4) (2020) 2919–2927.
[109] A.K. Das, B. Bera, M. Wazid, S.S. Jamal, Y. Park, On the security of a secure and lightweight authentication scheme for next generation IoT infrastructure, IEEE Access 9 (2021) 71856–71867.
[110] M. Rana, A. Shafiq, I. Altaf, M. Alazab, K. Mahmood, S.A. Chaudhry, Y.B. Zikria, A secure and lightweight authentication scheme for next generation IoT infrastructure, Comput. Commun. 165 (2021) 85–96.
[111] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S.M. Pournaghi, M.-A. Doostari, LAPTAS: Lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT, Wirel. Netw. 27 (2) (2021) 1389–1412.
[112] S. Challa, M. Wazid, A.K. Das, N. Kumar, A.G. Reddy, E.-J. Yoon, K.-Y. Yoo, Secure signature-based authenticated key establishment scheme for future IoT applications, Ieee Access 5 (2017) 3028–3043.

[113] S. Velliangiri, R. Manoharn, S. Ramachandran, V.R. Rajasekar, Blockchain based privacy preserving framework for emerging 6G wireless communications, IEEE Trans. Ind. Inform. (2021).
[114] S.A. Abdel Hakeem, H.H. Hussein, H. Kim, Security requirements and challenges of 6G technologies and applications, Sensors 22 (5) (2022) 1969.
[115] R. Ali, A.K. Pal, S. Kumari, M. Karuppiah, M. Conti, A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring, Future Gener. Comput. Syst. 84 (2018) 200–215.
[116] F.O. Catak, M. Kuzlu, E. Catak, U. Cali, D. Unal, Security concerns on machine learning solutions for 6G networks in mmwave beam prediction, Phys. Commun. 52 (2022) 101626.
[117] C.-L. Chen, J. Yang, W.-J. Tsaur, W. Weng, C.-M. Wu, X. Wei, Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIOT's application, Sensors 22 (3) (2022) 1146.
[118] D. Dolev, A. Yao, On the security of public key protocols, IEEE Trans. Inform. Theory 29 (2) (1983) 198–208.
[119] R. Canetti, H. Krawczyk, Universally composable notions of key exchange and secure channels, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2002, pp. 337–351.
[120] A. Paverd, A. Martin, I. Brown, Modelling and Automatically Analysing Privacy Properties for Honest-But-Curious Adversaries, Tech. Rep., 2014.
[121] A.K. Mishra, M. Wazid, D.P. Singh, A.K. Das, J. Singh, A.V. Vasilakos, Secure blockchain-enabled authentication key management framework with big data analytics for drones in networks beyond 5g applications, Drones 7 (8) (2023) 508.
[122] X. Wang, W. Wang, A. Liu, W. Liu, Z. Zhang, W. Li, PIA-a secure and efficient identity authentication scheme in telemedicine via the PUF method, Sci. Rep. 15 (1) (2025) 6846.
[123] O.A. Khashan, Blockchain-machine learning fusion for enhanced malicious node detection in wireless sensor networks, Knowl.-Based Syst. 304 (2024) 112557.
[124] A.A. Almuqren, Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions, J. Cyber Secur. Risk Audit. 1 (1) (2025) 1–11.
[125] J. Hu, X. Yang, L.-X. Yang, A framework for detecting false data injection attacks in large-scale wireless sensor networks, Sensors 24 (5) (2024) 1643.
[126] H. Xu, Y. Li, O. Balogun, S. Wu, Y. Wang, Z. Cai, Security risks concerns of generative AI in the IOT, IEEE Internet Things Mag. 7 (3) (2024) 62–67.
[127] D. Mishra, D. Dharminder, P. Yadav, Y.S. Rao, P. Vijayakumar, N. Kumar, A provably secure dynamic ID-based authenticated key agreement framework for mobile edge computing without a trusted party, J. Inf. Secur. Appl. 55 (2020) 102648.
[128] V. Odelu, A.K. Das, S. Kumari, X. Huang, M. Wazid, Provably secure authenticated key agreement scheme for distributed mobile cloud computing services, Future Gener. Comput. Syst. 68 (2017) 74–88.
[129] F. Wu, L. Xu, S. Kumari, X. Li, An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks, Multimedia Syst. 23 (2) (2017) 195–205.
[130] F. Wu, L. Xu, S. Kumari, X. Li, An improved and provably secure three-factor user authentication scheme for wireless sensor networks, Peer-To-Peer Netw. Appl. 11 (1) (2018) 1–20.
[131] M. Sidorov, M.T. Ong, R.V. Sridharan, J. Nakamura, R. Ohmura, J.H. Khor, Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains, IEEE Access 7 (2019) 7273–7285.
[132] K. Mahmood, S.A. Chaudhry, H. Naqvi, S. Kumari, X. Li, A.K. Sangaiah, An elliptic curve cryptography based lightweight authentication scheme for smart grid communication, Future Gener. Comput. Syst. 81 (2018) 557–565.
[133] S. Jangirala, A.K. Das, A.V. Vasilakos, Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment, IEEE Trans. Ind. Inform. 16 (11) (2019) 7081–7093.
[134] U. Mujahid, M. Najam-ul Islam, S. Sarwar, A new ultralightweight RFID authentication protocol for passive low cost tags: KMAP, Wirel. Pers. Commun. 94 (3) (2017) 725–744.
[135] M. Wazid, A.K. Das, S. Shetty, J. JPC Rodrigues, Y. Park, LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment, Sensors 19 (24) (2019) 5539.
[136] N. Garg, M. Wazid, A.K. Das, D.P. Singh, J.J. Rodrigues, Y. Park, BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment, IEEE Access 8 (2020) 95956–95977.
[137] M. Shariq, K. Singh, M.Y. Bajuri, A.A. Pantelous, A. Ahmadian, M. Salimi, A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario, Sustain. Cities Soc. 75 (2021) 103354.
[138] M. Vivekanandan, et al., BIDAPSCA5G: Blockchain based internet of things (IoT) device to device authentication protocol for smart city applications using 5G technology, Peer-To-Peer Netw. Appl. 14 (1) (2021) 403–419.
[139] A. Vangala, A.K. Das, Y. Park, S.S. Jamal, Blockchain-based robust data security scheme in IoT-enabled smart home, CMC-Comput. Mater. Continua 72 (2) (2022) 3549–3570.
[140] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Annual International Cryptology Conference, Springer, 1999, pp. 388–397.
[141] S. Amjad, S. Abbas, Z. Abubaker, M.H. Alsharif, A. Jahid, N. Javaid, Blockchain based authentication and cluster head selection using DDR-LEACH in internet of sensor things, Sensors 22 (5) (2022) 1972.
[142] T. Sylla, L. Mendiboure, M.A. Chalouf, F. Krief, Blockchain-based context-aware authorization management as a service in IoT, Sensors 21 (22) (2021) 7656.
[143] J. Hu, M.J. Reed, M. Al-Naday, N. Thomos, Hybrid blockchain for IoT—energy analysis and reward plan, Sensors 21 (1) (2021) 305.
[144] S. Wadhwa, S. Rani, S. Verma, J. Shafi, M. Wozniak, Energy efficient consensus approach of blockchain for IoT networks with edge computing, Sensors 22 (10) (2022) 3733.
[145] S.-C. Cha, J.-F. Chen, C. Su, K.-H. Yeh, A blockchain connected gateway for BLE-based devices in the internet of things, Ieee Access 6 (2018) 24639–24649.
[146] M. Daghmehchi Firoozjaei, A. Ghorbani, H. Kim, J. Song, Hy-bridge: A hybrid blockchain for privacy-preserving and trustful energy transactions in internet-of-things platforms, Sensors 20 (3) (2020) 928.
[147] A.D. Dwivedi, G. Srivastava, S. Dhar, R. Singh, A decentralized privacy-preserving healthcare blockchain for IoT, Sensors 19 (2) (2019) 326.
[148] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain, J. Med. Syst. 42 (8) (2018) 1–18.
[149] X. Ma, J. Ma, S. Kumari, F. Wei, M. Shojafar, M. Alazab, Privacy-preserving distributed multi-task learning against inference attack in cloud computing, ACM Trans. Internet Technol. (TOIT) 22 (2) (2021) 1–24.
[150] R. Alcarria, B. Bordel, T. Robles, D. Martín, M.-Á. Manso-Callejo, A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities, Sensors 18 (10) (2018) 3561.
[151] M. Yavari, M. Safkhani, S. Kumari, S. Kumar, C.-M. Chen, An improved blockchain-based authentication protocol for IoT network management, Secur. Commun. Netw. 2020 (1) (2020) 8836214.
[152] D. Pengfei, M. Zhaofeng, Z. Yuqing, W. Jingyu, L. Shoushan, Blockchain-enabled privacy protection and access control scheme towards sensitive digital assets management, China Commun. (2024).
[153] J. Miao, Z. Wang, Z. Wu, X. Ning, P. Tiwari, A blockchain-enabled privacy-preserving authentication management protocol for internet of medical things, Expert Syst. Appl. 237 (2024) 121329.
[154] R. Vatambeti, E.P. Krishna, M.G. Karthik, V.K. Damera, Securing the medical data using enhanced privacy preserving based blockchain technology in internet of things, Clust. Comput. 27 (2) (2024) 1625–1637.
[155] C. Patel, A. Pasikhani, P. Gope, J. Clark, User-empowered secure privacy-preserving authentication scheme for digital twin, Comput. Secur. 140 (2024) 103793.
[156] W.-J. Liu, W.-Y. Chiu, W. Hua, Blockchain-enabled renewable energy certificate trading: A secure and privacy-preserving approach, Energy 290 (2024) 130110.
[157] F. Wang, J. Cui, Q. Zhang, D. He, H. Zhong, Blockchain-based secure cross-domain data sharing for edge-assisted industrial internet of things, IEEE Trans. Inf. Forensics Secur. (2024).
[158] A. Namdev, H. Lohiya, Design and implementation of biometric blockchain authentication for VANET security, in: 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science, SCEECS, IEEE, 2024, pp. 1–8.
[159] C. Dhasaratha, M.K. Hasan, S. Islam, S. Khapre, S. Abdullah, T.M. Ghazal, A.I. Alzahrani, N. Alalwan, N. Vo, M. Akhtaruzzaman, Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things, CAAI Trans. Intell. Technol. (2024).
[160] X. Xiang, J. Cao, W. Fan, Lightweight privacy-preserving authentication mechanism in 5G-enabled industrial cyber physical systems, Inform. Sci. 666 (2024) 120391.
[161] A. Padma, M. Ramaiah, Blockchain based an efficient and secure privacy preserved framework for smart cities, IEEE Access (2024).
[162] C. Sandeepa, B. Siniarski, N. Kourtellis, S. Wang, M. Liyanage, A survey on privacy of personal and non-personal data in B5G/6G networks, ACM Comput. Surv. 56 (10) (2024) 1–37.
[163] S. Alraih, I. Shayea, M. Behjati, R. Nordin, N.F. Abdullah, A. Abu-Samah, D. Nandi, Revolution or evolution? Technical requirements and considerations towards 6G mobile communications, Sensors 22 (3) (2022) 762.
[164] M.M. Aslam, L. Du, X. Zhang, Y. Chen, Z. Ahmed, B. Qureshi, Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges, Wirel. Commun. Mob. Comput. 2021 (1) (2021) 1331428.