BLOCKCHAIN-BASED APPROACHES FOR PRIVACY AND SECURITY IN IOT APPLICATIONS: A SYSTEMATIC LITERATURE REVIEW

Naser Hussein, Jihene khoualdi , Ilhem Abdelhedi Abdelmoula and Hella Kaffel Ben Ayed

LIPAH Lab, University of Tunis Elmanar

ABSTRACT

Internet of Things (IoT) has gripped domains with this ubiquitous connectivity, in-the-moment data collection, and autonomous decision-making. But rising numbers of heterogeneous, extremely constrained IoT devices pose serious concerns regarding data privacy, security, and trust management, drawing great attention into these areas in the academic field and on all sides. Thus, blockchain technology came into the limelight for strengthening security and privacy in IoT systems in a decentralized manner, giving the system immutability, transparency, and distributed trust. This study proposes a Systematic Literature Review (SLR) of blockchain-based approaches that aim to enhance the IoT applications' privacy and security, focusing chiefly on healthcare, supply chains, and smart cities. The review uses a structured methodology to find, select, evaluate, and synthesize relevant peer-reviewed studies published between 2018 and 2025 taken from major scientific databases such as IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Scopus. Articles were also examined to narrow the scope of study and set the subject. The selected studies are analyzed and classified based on their security goals (e.g., confidentiality, integrity, authentication), privacy-preserving techniques (e.g., anonymization, differential privacy, zero-knowledge proofs), blockchain configurations (e.g., public, private, consortium), and consensus mechanisms. The findings reveal a growing body of research applying blockchain to a wide range of IoT domains, addressing diverse application domains such as healthcare, smart homes, industrial IoT, and agriculture, and demonstrating its potential to enhance data integrity, access control, and authentication. However, the integration of blockchain in IoT also faces challenges such as scalability, latency, and resource overhead, especially in real-time and constrained environments. This review offers a comprehensive synthesis of the state-of-the-art, identifies current limitations and research gaps, and proposes future research directions for building secure, efficient, privacy-aware, and scalable blockchain-enabled IoT systems.

KEYWORDS

Blockchain, Privacy, Security, IoT, Systematic Literature Review (SLR), Healthcare, Supply Chain, Smart Cities.

1. INTRODUCTION

Rather than one sector, the Internet of Things (IoT) has been globally innovating in various sectors, such as healthcare, education, manufacturing, transportation, agriculture, and smart cities. IoT connects billions of devices and thus enables real-time data collection, automation, and

David C. Wyld et al. (Eds): SESBC, AIFL, NLPTT – 2025
pp. 19-44, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.151502

remote monitoring. Ranging from very simple sensors and actuators to highly complex smart appliances, IoT devices generate a humongous amount of data and seamlessly interact over a wireless network and cloud platform [1]. Rapid adoption of the technology has created several other opportunities-well-recognized for driving operational efficiencies, rapid response, and richer consumer experiences [2]. But it does introduce major challenges of data privacy, protection, and trust due to the heterogeneity, resource constraints, and sometimes physical accessibility of IoT entities. Many of these devices lack the computational power to support strong cryptography, while also being distributed enough to provide a large attack surface. Thus the threats faced by IoT systems are, inter alia, data alteration, unauthorized data access, spoofing, or DoS attack. Threats emerge because of the heterogeneity of protocol and operating system, as a slow application of global standards.

Since IoT applications usually deal with protected information, from personal health data to that concerning critical supply chain activities, their utmost security is a must. According to Vipul Parekh, senior director at the management consultancy, Alvarez &Marsal, protection of data throughout the complex Internet of Things ecosystem is of utmost concern for providers. Because of inherent security flaws, Internet of Things (IoT) devices are a prime target for distributed denial-of-service attacks, malevolent attackers, and data breaches. In response to these challenges, blockchain technology has emerged as a promising solution for enhancing IoT security and privacy, robustness, and untrustworthy authentication to ensure the secure exchange of critical user data between IoT objects. As a decentralized and tamper-resistant ledger, blockchain offers intrinsic support for data integrity, authentication, transparency, and access control—eliminating the need for centralized authorities [3], [4]. Smart contracts further enable secure, automated interactions, while blockchain's cryptographic foundations ensure accountability and verifiability. Consequently, the integration of blockchain with IoT has become a vibrant area of research and development.

Given the rapid growth of this interdisciplinary field, there is a clear need to systematically assess and categorize existing blockchain-based solutions aimed at securing IoT environments. This Systematic Literature Review (SLR) seeks to provide a comprehensive and structured overview of the current landscape, highlighting major contributions, methodologies, limitations, and emerging trends. Focusing on impactful domains such as healthcare, supply chain management, and smart cities, this review aims to guide researchers, practitioners, and system architects in advancing secure, blockchain-enabled IoT ecosystems. Specifically, this study aims to:

- Identify and categorize blockchain-based approaches for enhancing IoT privacy and security.
- Analyze architectural and functional aspects, including consensus mechanisms and privacy-preserving techniques.
- Examine practical challenges, research gaps, and future directions for scalable, secure IoT-blockchain integration.

The remainder of this paper is organized as follows. Section 2 details the SLR methodology used for literature collection and analysis. Section 3 provides background on IoT architectures, security challenges, and blockchain fundamentals. Section 4 presents the findings of the literature review, including a classification of selected studies. Section 5 discusses key insights, limitations, and implications of the analysis. Section 6 outlines open challenges and future research directions. Section 7 concludes with a summary of contributions and final remarks.

2. RESEARCH METHODOLOGY-SYSTEMATIC LITERATURE REVIEW (SLR)

This section describes the systematic process that has been followed to conduct this literature review. Our methodology relies on the established guidelines proposed by Barbara Kitchenham regarding systematic literature reviews in software engineering and computing, in order to fully inform the review process with respect to transparency, replicability, and robustness. The process has three broad phases or stages: Planning the Review, Conducting the Review, and Reporting the Review.

2.1. SLR Framework

The SLR framework has the purpose of defining the structure and principles of this review and ensures it is undertaken with the rigour and repeatability associated with scientific work:

- Planning the Review: This phase involves defining the purpose of the review, creating the research questions, and designing the review protocol.
- The Review: In this phase we complete the review with a structured search, selection of studies, quality appraisal and extraction of data.
- Reporting the Review: The last phase includes synthesising the evidence, analysing the results and reporting them in a structured way which is interpretable.
- The structured process is expected to minimise bias and improve evidence quality in fields with a tendency to varied disciplines and rapidly changing evidence such as blockchain and IoT.

2.2. Research Questions (RQs)

The review is guided by the following research questions:

- RQ1: What blockchain-based approaches have been proposed to address privacy and security challenges in IoT applications?
- RQ2: How do these approaches differ in terms of architecture, consensus mechanisms, and privacy/security goals?
- RQ3: What are the current research gaps, limitations, and potential future directions?

These RQs were formulated to ensure comprehensive coverage of both theoretical and applied contributions and to support future research and practical deployment of secure, blockchain-enabled IoT systems.

2.3. Search Strategy

To ensure completeness and relevance, a carefully designed search strategy was used. Firstly, we selected a set of reputable and comprehensive digital libraries frequently used in computer science and engineering research: IEEE Xplore, ACM Digital Library, ScienceDirect (Elsevier),SpringerLink and Scopus. These databases were chosen for their broad coverage of high-quality, peer-reviewed publications related to both IoT and blockchain technologies. Secondly, we chose the following criteria to retrieve relevant studies:

- Time Span: January 2018 – May 2025
- Language: English only
- Document Type: Peer-reviewed journal articles and conference papers

The time span was chosen to capture developments after the initial surge of blockchain-IoT integrations, focusing on more mature, technical, and applied contributions. Then, we used combinations of the following keywords, adapted with Boolean operators to expand the coverage:

- Primary String:

  "Blockchain" AND "IoT" AND ("Privacy" OR "Security") AND ("Healthcare" OR "Supply Chain" OR "Smart City")

- Secondary String Variants:

  "Blockchain-based IoT privacy" OR "Decentralized IoT security" "Blockchain for secure IoT" OR "IoT data protection using blockchain"

These keywords were iteratively refined and validated through pilot searches to ensure precision and recall.

2.4. Inclusion and Exclusion Criteria

A set of predefined Inclusion and Exclusion criteria were used to ensure the relevance and quality of the selected studies.

- Inclusion Criteria:

This study includes:Articles explicitly focused on the use of blockchain to address privacy and/or security in IoT systems; Studies proposing or evaluating technical methods, architectures, frameworks, or models; Research applied to real-world application domains such as healthcare, smart cities, supply chain, agriculture, etc.; and Publications in peer-reviewed journals or conference proceedings.

- Exclusion Criteria:

This study excludes :Studies unrelated to IoT (e.g., pure blockchain or cryptocurrency research); Papers that discuss blockchain in IoT but not in the context of privacy or security; Non-peer-reviewed content: white papers, posters, workshop summaries, blogs, editorials, and patents; and Articles not available in English or published before 2018.

2.5. Study Selection Process

The study selection process follows a multi-step protocol to filter and identify high-quality and relevant studies for the review. This process ensures that only studies that meet the research objectives and inclusion criteria are retained.

- ***Step 1: Removal of Duplicates***

All retrieved studies from selected digital libraries (IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Scopus) were imported into a reference management tool. Automated and manual filtering was applied to remove duplicate entries that appear across multiple databases. We used the following tools:

- Zotero, an open-source bibliographic management software, was employed to collect, organize, and manage references efficiently.
- Microsoft® Excel was used to log and document decision-making at each stage of the review process, from initial screening to final selection

- ***Step 2: Title and Abstract Screening***

The titles and abstracts of the remaining articles were screened to assess their relevance to the topic of blockchain-based privacy and security in IoT applications.
Studies were excluded if: They did not mention both blockchain and IoT; or They did not discuss privacy or security issues; or They focused on non-technical or purely theoretical aspects; or They were not written in English or peer-reviewed.

- ***Step 3: Full-Text Reading and Selection***

For articles passing the abstract screening, full-texts were reviewed to evaluate whether they met all inclusion criteria. Only those providing: Detailed technical implementation or architecture; and clear use of blockchain to address privacy/security in IoT. Application to real-world domains such as healthcare, smart cities, or supply chains were retained. However, articles lacking methodological depth or relevance were excluded.

2.6. Data Extraction and Synthesis

A structured data extraction form was designed to systematically gather and organize information from the selected studies. The extracted data formed the basis for synthesis, classification, and analysis in later sections. Thus, each study was analyzed to extract the following elements:

- Bibliographic Information: Title, authors, publication year
- IoT Application Domain: E.g., healthcare, supply chain, smart cities, industrial IoT
- Blockchain Type: Public, private, or consortium
- Consensus Mechanism: E.g., Proof of Work (PoW), Proof of Stake (PoS), PBFT, RAFT, etc.
- Privacy/Security Goals: Confidentiality, integrity, access control, anonymity, authentication, non-repudiation
- Privacy-Preserving Techniques: Anonymization, encryption, differential privacy, zero-knowledge proofs, etc.
- Evaluation Methods: Simulations, testbeds, comparative analysis, prototypes, performance metrics
- Key Findings: Summary of contributions, limitations, and results

3. BACKGROUND AND THEORETICAL FOUNDATIONS

3.1. The Internet of Things (IoT): Definition, Characteristics and Applications

3.1.1. IoT's Definition

The basic concept behind Internet of Things (IoT) is to interconnect any product in the physical world with the digital world. The advanced development of technologies like communication capabilities, sensors, smart phones, cloud computing, network virtualization and software will enable items to connect with each other all the time, everywhere. Thus, Iot refers to a network of interconnected, heterogeneous physical devices capable of sensing, processing, and

communicating data autonomously, without human intervention [3]. Various definitions exist in the literature, each emphasizing different aspects [9]. Atzori et al. view IoT through three components: middleware, sensors, and information [4]. Gubbi et al. define it as the interconnection of sensing and actuation devices that share information across platforms using a unified, cloud-based framework [5]. Tan et al. focus on smart objects with virtual identities interacting in social, environmental, and user contexts [6]. Haller et al. offer a technology-agnostic definition based on mobility and service integration[7]. Davoli et al. emphasize the network structure, likening IoT to a physical Internet[8]. For this survey, the adopted definition is from the European Commission (DG INFSO) and EPoSS, which describes IoT as "objects with virtual identities and personalities operating in smart spaces using intelligent interfaces to connect and communicate in social, environmental, and user contexts"[10].

3.1.2. IoT Supporting Technologies

Several technologies support the concept of IoT: identification technology, networks and communication technologies, and software and hardware technologies. Wireless Sensor Networks (WSN) and Radio-Frequency Identification (RFID) are expected to play key roles as enablers of identification technology in IoT [2, 6, 13, 21]. Both wired and wireless technologies (e.g., GSM, UMTS, Wi-Fi, Bluetooth, ZigBee) are essential to connect billions of devices and services [22–24]. Research in nanoelectronics focuses on miniaturization, low cost, and increased functionality in designing wireless identifiable systems [13]. Smart devices with enhanced inter-device communication will lead to intelligent systems with high degrees of autonomy, facilitating rapid IoT application deployment and creating new services.

3.1.3. IoT Application Domains

The Internet of Things (IoT) has become integral to numerous sectors, enabling automation, real-time monitoring, and intelligent decision-making across both personal and industrial contexts [1], [2]. In agriculture, IoT facilitates precision farming by monitoring environmental parameters such as soil moisture, temperature, and humidity, thereby optimizing irrigation and fertilizer use to enhance crop yields and resource efficiency [3], [4]. In smart homes, IoT technologies automate lighting, heating, and security systems. Devices like Amazon Echo and Google Home exemplify this trend, with over 309 million smart homes projected globally by 2024 [5], [6]. Wearables such as smartwatches and fitness trackers collect health-related data to support personal well-being and medical diagnostics. Tech giants like Apple and Samsung lead the IoT wearables market, which has shown rapid growth [7]. In healthcare, IoT enables remote patient monitoring, smart hospital infrastructure, and emergency detection systems for elderly care [8]. Insurance providers also integrate wearables to personalize health plans and encourage preventive care [9]. In industry and manufacturing, IoT improves operational efficiency through real-time asset tracking (e.g., RFID, GPS), predictive maintenance, and automated quality control [10], [11]. Retailers employ IoT for inventory management and customer behavior analysis [12]. In transportation, IoT supports smart mobility via route optimization, autonomous vehicles, and fleet monitoring, contributing to traffic efficiency and reduced emissions [13]. Similarly, in energy and utilities, smart grids and sensor-based monitoring systems enhance energy efficiency, reduce waste, and improve outage response [14]. Smart cities leverage IoT for applications such as intelligent traffic control, waste management, and energy optimization. Cities like Singapore and Oslo exemplify large-scale IoT deployments to improve urban living conditions [15]. In hospitality, IoT streamlines hotel operations, enables personalized guest experiences, and simplifies check-in/out procedures [16]. Finally, IoT contributes to environmental sustainability by monitoring air and water quality, optimizing waste treatment, and supporting pollution mitigation strategies through data analytics [17].

3.1.4. IoT Layered Architecture : From Three to Five Layers

The Internet of Things (IoT) is built on a network of interconnected embedded sensors and devices that typically feature modest processing capabilities, limited memory, low power use, and unique identifiers. To ensure seamless integration, scalability, and intelligent operation across these diverse systems, IoT relies on a multi-layered architecture. This approach promotes modularity, interoperability, and efficiency, enabling the transformation of raw environmental data into actionable services and solutions—crucial for smart applications in healthcare, industry, agriculture, and urban infrastructure.While numerous studies propose IoT architectures with varying layer structures, from three-layer to five-layer architecture. The foundational three-layer model remains the simplest and most commonly used. While the three-layer architecture excels in ease of deployment for small-scale systems, it falls short in scalability and lacks dedicated layers for data processing and business logic. To address such limitations and add more granularity to data handling and service provisioning, researchers and industry practitioners often introduce a fourth "support" (or middleware) layer, positioned between the network and application layers. The five-layer model provides finer granularity and is often used in research to better address functional and security aspects. It adds more structure and control, making it well-suited for complex, enterprise-grade IoT deployments that demand strategic coordination and scalable governance. Layered architectures provide a modular, scalable, and security-aware way to design IoT systems. As illustrated in the Table 2 below, while the three-layer architecture offers a basic overview, the four- and five-layer models offer greater clarity and control—especially useful in complex applications where data processing, service orchestration, and security must be tightly managed. Choosing the appropriate architecture depends on the use case, performance requirements, and security posture of the target IoT environment.

Table 2. Comparison of the Architectures

Layer Name	Function	Technologies and Components	Three Layer	Four Layer	Five Layer
1- Perception Layer	This is the bottom layer, responsible for detecting and collecting data from the physical environment using sensors, RFID tags, cameras, GPS modules,	Sensors, actuators, RFID readers, smart devices	**x**	**x**	**x**
2- Network Layer	Acts as a channel for data exchange from sensors, actuators, and gateways to data processing and application layers. It transmits the data collected from the perception layer to the processing system or cloud infrastructure using communication protocols	Wi-Fi, Bluetooth, Zigbee, 4G/5G, LoRaWAN, NB-IoT	**x**	**x**	**x**
3- Middleware Layer	Positioned between the network and application layers, this layer handles data management, storage, processing, and service abstraction	Middleware platforms, edge computing, fog computing, cloud platforms.		**x**	**x**
4- Processing Layer	Dedicated to analyzing, processing, and storing large volumes of IoT data, often using big data analytics, AI, and ML algorithms	Big data platforms (Hadoop, Spark), databases, data lakes, analytics engines.			**x**
5- Application Layer	This layer delivers specific services to users, depending on the use case (e.g., smart home, healthcare, agriculture, industrial monitoring).	Cloud computing platforms, mobile/web interfaces, analytics dashboards.	**x**	**x**	**x**

In this paper, we adopt the five-layer IoT architecture, typically comprising five key layers, each serving distinct roles in data collection, communication, processing, and user interaction.

1. ***Perception Layer (Sensing Layer):*** Sensors and actuators that detect and measure environmental conditions or events (e.g. temperature, humidity, motion). Actuators execute actions in response to control commands or stimuli. The sensors convert physical parameters into digital signals, while actuators perform actions based on control signals, enabling interaction with the physical world.
2. ***Network Layer (Transmission Layer):*** serves as the communication backbone of the IoT architecture, ensuring seamless interoperability among connected devices. It is responsible for transmitting the data collected from the perception layer to the processing system or cloud infrastructure using communication protocols[33].It ensures reliable, efficient, and secure communication, often through the use of gateways and routers that manage data routing, protocol translation and forward data across heterogeneous networks.
3. ***Support Layer (or Middleware Layer):*** handles data management, storage, processing, and service abstraction. It incorporates Middleware platforms, fog, edge, or cloud computing technologies—to bolster scalability, enhance processing capabilities, and improve system efficiency[30, 31]. It provides interfaces and APIs to decouple devices from applications, facilitates interoperability, and optimizes resource use.
4. ***Processing Layer***:dedicated to analyzing, processing, and storing large volumes of IoT data, often using big data analytics, AI, and ML algorithms.it enables intelligent decision-making and automation based on real-time and historical data.It comprises edge devices, cloud computing platforms, big data platforms (Hadoop, Spark), databases, data lakes, analytics engines. data centers, and servers where data is processed, analyzed, and stored. It cleans, filters, and processes data collected from the network layer. It performs complex data analysis, processes the information received from the network layer, and stores the processed data. It interprets the data, applies machine learning, artificial intelligence, and analytics to derive insights, and supports decision-making based on the findings. Additionally, it stores the results for future use, improving efficiency and responsiveness.
5. ***Application Layer :*** is the topmost layer where end-user applications and services operate. It bridges the technical IoT infrastructure with end users, adding business and societal value. It is user-centric and focuses on implementing various applications of IoT devices, such as healthcare monitoring, smart home systems, industrial automation, smart agriculture and smart transportation systems. It delivers the results of data processing performed in the data processing layer to users or other systems [32]. The application layer performs functions on behalf of the user, providing a user-friendly interface and facilitating user interactions with IoT devices and service personalization. It translates processed data into meaningful user actions. It delivers tailored services and interfaces (dashboards, APIs) based on the processed data.

3.2. Security and Privacy Challenges in IoT Systems

The Internet of Things (IoT) is transforming industries by enabling pervasive connectivity, automation, and real-time decision-making. However, the same characteristics that make IoT valuable—ubiquity, heterogeneity, and scalability—also introduce critical security and privacy challenges that must be addressed to ensure safe and reliable deployment.

3.2.1. Security Challenges in IoT Systems

Security is a foundational requirement for IoT systems, driven by several critical factors including a broad threat landscape, resource constraints, protocol diversity, and challenges in resilience and update management. Firstly, IoT networks are prime targets for cyberattacks, including unauthorized access, data tampering, eavesdropping, and Distributed Denial-of-Service (DDoS) attacks [41]. Their distributed nature and connectivity expose multiple attack surfaces. Secondly, resource constraints on many IoT devices—such as limited CPU power, memory, and energy—make the implementation of traditional security mechanisms difficult. Deploying strong encryption, mutual authentication, access control, and secure firmware updates often requires adaptations in the form of lightweight and efficient solutions. Thirdly, protocol diversity introduces further complexity. The IoT landscape includes various wireless communication standards like Wi-Fi, Bluetooth, Zigbee, and LoRaWAN, each with its own security assumptions and mechanisms. Integrating these into a unified, end-to-end secure communication framework is challenging and often creates vulnerabilities that attackers can exploit [42]. Finally, maintaining system resilience and secure update management is a persistent challenge. Ensuring all devices across the network are regularly patched and protected against emerging threats requires secure boot mechanisms, authenticated update channels, and rollback protections. However, many current IoT deployments lack such features, leaving devices exposed to long-term exploitation.

3.2.2. Privacy Challenges in IoT Systems

Privacy remains a critical concern in IoT environments, driven by several factors including continuous data collection, vulnerabilities across the data lifecycle, limited mitigation capabilities, and gaps in regulatory enforcement and standardization. Firstly, IoT devices constantly collect, transmit, and process user data—from environmental conditions to highly sensitive personal information such as health metrics. This data passes through multiple stages, including sensing, aggregation, and analytics. At each phase, it is susceptible to interception, profiling, and inference attacks, significantly increasing the risk of unauthorized surveillance and identity exposure [43]. Secondly, privacy risks emerge across the entire data lifecycle. Sensor data can unintentionally reveal patterns of user behavior. Centralized nodes used for processing and storage may become attractive targets for large-scale data breaches. Furthermore, AI and machine learning models trained on this data can inadvertently enable inference attacks, where seemingly non-sensitive information is used to deduce private attributes. Thirdly, privacy-preserving techniques such as data anonymization, differential privacy, and secure aggregation have been introduced to mitigate these threats [44]. However, their adoption is often limited by computational constraints, lack of interoperability, and inconsistent implementation across devices. Finally, although legal frameworks like GDPR and CCPA impose requirements for user consent, data transparency, and the right to erasure, IoT systems frequently lack the built-in mechanisms needed to comply uniformly. The absence of standardized security and privacy architectures across platforms leaves networks vulnerable, where a single compromised device can jeopardize the privacy of the entire ecosystem [44].

In summary, robust and resilient security solutions are essential for protecting IoT systems from the wide range of threats that stem from their interconnected and resource-constrained nature. Addressing these privacy challenges requires not only technical solutions but also regulatory enforcement and cross-platform coordination to ensure trustworthy and privacy-respecting IoT deployments. To address these concerns, security and privacy must be incorporated across all layers of the IoT stack—from hardware and firmware to networking and cloud services—ensuring security-by-design and privacy-by-design principles are respected [43].

While security and privacy are critical to IoT systems, other design considerations also play a vital role in their effectiveness and widespread adoption. Scalability is essential to accommodate the growing number of connected devices without degrading performance. Interoperability ensures seamless communication among heterogeneous devices by promoting the use of standardized protocols and APIs. Reliability, through fault tolerance and high availability, is particularly crucial in mission-critical domains like healthcare and industrial automation. Successful system integration with existing enterprise infrastructure is necessary for operational continuity and scalability. Additionally, a user-friendly experience enhances adoption, while attention to environmental impact—such as energy efficiency and sustainable materials—supports responsible IoT deployment.

3.3. Blockchain Architectures and Technical Foundations

3.3.1. Blockchain Fundamentals

Blockchain systems can be broadly categorized based on their access permissions and governance models, which define who can participate in the network, access data, read from or write to the distributed ledger and contribute to consensus. Moreover, various blockchain deployment strategies can be pursued depending on the application domains. Predominantly, three main types of blockchains emerge from these strategies, which are : Public, Private and hybrid blockchains.

- ***Public Blockchain:***are fully decentralized and permissionless networks where anyone can read, write, and participate in consensus without authorization. These systems, such as Bitcoin and Ethereum, promote transparency and scalability, often supporting thousands of nodes. However, they raise significant privacy concerns, as all transactions are publicly visible despite pseudonymity, and they suffer from performance issues such as high latency, low throughput, and excessive energy consumption. They are also vulnerable to majority (51%) attacks due to their open nature [5].
- ***Private Blockchain:*** operate within a controlled environment, restricting participation to invited or authorized entities. Managed by a central authority or consortium, they offer enhanced privacy, performance, and governance—making them well-suited for enterprise applications that require data confidentiality and regulatory compliance. Only designated nodes can access the ledger, validate transactions, or participate in consensus, and all activities are governed by clearly defined policies [5].
- ***HybridHybrid (Consortium or Federated) Blockchains:***combine features of both public and private models. While data may be publicly visible, only selected participants—such as trusted organizations or institutions—can validate or write to the ledger. This structure provides a balance between transparency and control and is ideal for applications like decentralized identity systems, financial services, and regulatory-compliant supply chains. Initiatives like the Sovrin Foundation and Central Bank Digital Currency (CBDC) platforms are examples of this model in practice [6].

3.3.2. Technical Characteristics of Blockchain

Blockchain integrates several current technologies to provide a secure, decentralized platform for multi-party trust. Developed blockchain systems have some defining characteristics that are [7]:

- ***Transparency:*** All peer nodes on the network maintain a full replica of the ledger and can verify all transactions within the network. Decentralized design gives complete traceability and transparency.

- ***Tamper-proof Traceability:*** Transactions, once authenticated and recorded, cannot be altered or deleted. The records are all timestamped and linked with cryptographic hashes, allowing complete auditability of transactions.
- ***Privacy and Security:*** Consensus and cryptographic properties of Blockchain allow nodes to act trustless, verifying transactions individually without knowing other parties' identities, thus providing user privacy.
- ***High Reliability:*** All nodes contribute to network stability by maintaining the ledger and validating transactions. Byzantine Fault Tolerance (BFT) is available in the system; thus the system can withstand node failures and attacks.

3.3.3. Consensus Algorithms

Consensus mechanisms are a necessary element of trust and consistency in decentralized systems. The blockchain platforms studied utilize different types of consensus protocols, with every protocol exhibiting different features and trade-offs [7] .

- Proof of Work (PoW): A consensus method that requires participants or nodes to solve complex computational problems that favor nodes with advancements in computing power.
- Proof of Stake (PoS): A consensus method that chooses validators based on the number and type of cryptocurrency owned and staked.
- Proof of Authority (PoA): A consensus method that depends on a limited number of validators who are trusted specifically by the specific consensus members and authority.
- Proof of Elapsed Time (PoET): A consensus method that determines the node that is selected at random and then based on previously agreed-to consensus
- validating criteria of the node's trusted execution environment.
- Delegated Proof of Stake (DPoS): A consensus method that requires stakeholders or communities to vote and elect validators, or nodes, to perform the actions of consensus on their behalf and do so for a limited amount of time (however votes can be revoked and node associations ended).

3.3.4. Blockchain as a Solution to IoT Challenges

Blockchain technology—with its decentralized architecture, immutability, and cryptographic integrity—offers promising solutions to many of the challenges facing IoT systems. When integrated with IoT, blockchain introduces several key benefits. By eliminating the need for centralized control, blockchain enhances security and data integrity, reducing single points of failure and protecting against unauthorized access and tampering [8]. Through the use of smart contracts, blockchain enables autonomous, rule-based interactions among IoT devices, thereby automating processes and cutting operational costs—particularly in complex sectors like logistics and supply chains. It also improves transaction speed and auditability, allowing fast, traceable, and verifiable exchanges of data between multiple entities, which is essential in ecosystems such as agri-food or manufacturing. Traditional IoT infrastructures often struggle with scalability and vulnerability due to centralized architectures. Blockchain addresses these issues through decentralization, enabling fault-tolerant and scalable systems [10], and supports efficient device-to-device communication without central bottlenecks [11]. Furthermore, it facilitates secure firmware deployment, data validation via consensus, and cost efficiency by removing intermediaries. Its unified data layer supports interoperability across heterogeneous devices [15], while decentralized identity management ensures secure and scalable authentication [16]. Lastly, blockchain’s inherent resilience strengthens the robustness and reliability of the overall IoT infrastructure [11], [17].

4. LITERATURE REVIEW FINDINGS

4.1. Overview of Selected Studies

An initial pool of 195 research articles was identified through digital library searches. After filtering out reviews, short papers, book chapters, and inaccessible documents, 55 studies were excluded. The remaining 140 articles were further screened based on title and abstract using defined inclusion and exclusion criteria, reducing the selection to 95. Following a full-text assessment, only 58 studies were retained for in-depth evaluation and discussion.

To analyze the selected studies, a thematic analysis and taxonomy-based classification approach was applied. Articles were grouped by application domain and blockchain architecture, then analyzed using comparative tables and visual charts that categorized them by consensus mechanisms and their privacy/security objectives. This enabled the identification of recurring patterns, trade-offs, and domain-specific trends. Finally, the review highlighted research gaps and emerging challenges to guide future investigations in this evolving field.

An analysis of publication trends from 2018 to 2025 reveals a steady increase in research focusing on IoT, security, privacy, and agri-food supply chains. The distribution of these studies by year, publication venues, and countries. The selected studies have been classified based on their main IoT application domains, including smart healthcare, smart homes, industrial IoT, agriculture, smart cities, and supply chain management, as illustrated in Figure 1.

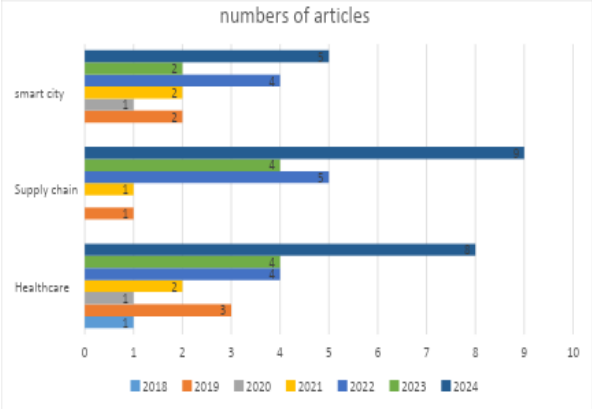

Figure 1: Classification of relevant articles published annually from 2018 to 2024 per Application Domain

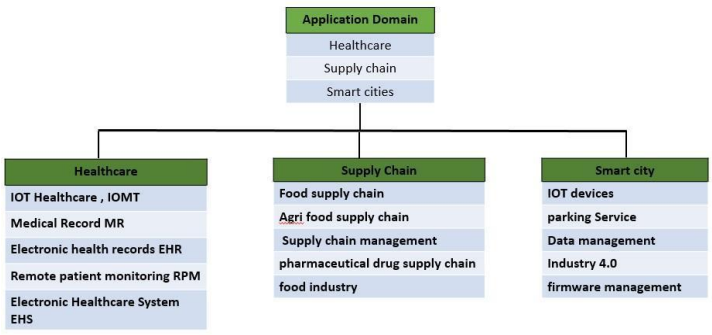

Figure.2 The IOT Application domains

4.2. Overview of Blockchain-Based IoT Solution for Security and Privacy

This section presents a survey of blockchain-based approaches designed to address various security and privacy challenges in IoT systems. It highlights how different blockchain architectures, platforms, and mechanisms are leveraged to enhance data integrity, confidentiality, access control, and overall system trustworthiness. The following tables 4,5 and 6 summarize a selection of recent studies in healthcare, supply chains and smart cities that address security and privacy challenges in IoT systems throughblockchain-based solutions. Each entry outlines the specific problems targeted by the study, the advantages offered by blockchain (such as decentralization, immutability, and cryptographic security), and the technical choices made, including blockchain type (public, private, or consortium), platforms (e.g., Ethereum), consensus mechanisms (e.g., PoW, PoA, or PoC), and whether smart contracts or decentralized storage (e.g., IPFS) were employed. Additionally, each study is evaluated based on the key security and privacy considerations it addresses, including confidentiality, integrity, access control, authentication, traceability, availability, and interoperability. This comparative analysis provides insight into how blockchain configurations are being tailored to meet the distinct requirements of secure and privacy-preserving IoT applications. Below is a detailed analysis of these improvements, based on a systematic literature review of peer-reviewed research (2018–2025). From a total of 75 studies on blockchain applications in IoT, research specifically focusing on enhancing data privacy and access control was selected for analysis. These studies cover a range of topics including proposed solutions, system evaluations, and comprehensive surveys, as summarized in Tables 3, 4, and 5. Blockchain technology enhances data privacy in IoT applications by leveraging decentralization, cryptographic security, and immutable audit trails. This is particularly impactful in sectors like healthcare and smart cities, where sensitive data requires robust protection against breaches and unauthorized access. Additionally, the review explores how blockchain can be leveraged to strengthen data security, particularly in relation to data storage from connected devices, as discussed in studies such as [17], [19], [20], [21], and [22]. Security concerns are addressed in works like [23] through [31], while issues related to storage capacity and off-chain data management are examined in [20], [29], [32], [33], [34], [35], and [36]. Most of these studies offer practical recommendations for addressing identified challenges and improving the secure integration of blockchain within IoT systems.

Table 3: Comparative Analysis of Blockchain-Based IoT Security and Privacy Solutions in Healthcare

Pap.	Year	Problems	Advantage of Blockchain	Type NET/ Platform	Consensus	Smart contract-storage	Security and Privacy Considerations
[32]	2022	Security and privacy issues Lack integrity Low scalability, SPOF	Decentralization Distributed, Immutability, Security	Private, Permission Ethereum	POA	Smart contract IPFS	Confidently, Integrity, Access control, privacy
[37]	2023	DDos Attack, Data theft, hacking, SPOF, High energy consumption	Decentralization Distributed, Immutability, Security,	Ethereum, private	POW	Smart contract IPFS,	Security, Privacy, Traceability, Transparency, Confidently, Reliability,
[23]	2022	Interoperability issues, Exchange data, Lack of competence, Trust,	Decentralization, Distributed, Immutability,	Ethereum, Private,	POA	Smart contrac IPFS	Confidently, Authorization, Access control, Traceability, Transparency, Interoperability

		Data management, Security threats					auditability,
[17]	2022	Data stored, SPOF Data security, Privacy issues, Attacks Scalability	Decentralization, Distributed, Cryptographic Immutability,	Ethereum , Private,	POA	Smart contract	Confidently, Accesses control, Privacy, Integrity, Transparency,
[38]	2024	Scalability, limited functionality, high execution costs, resource consumption	Decentralization Cryptographic, Immutability,	Ethereum , private	POA	Smart contract IPFS	Confidently, Integrity, Availability, Transparency, Scalability,
[39]	2023	Data sharing, Security and privacy issues Attacks, Data breaches	Decentralization, Cryptographic,	Ethereum , Consortium,	POC	Smart contract	Access control, Availability, Authentication, privacy, Confidently, Transparency,
[40]	2023	Security and privacy issues, scalability	Decentralization Immutability, Cryptographic	Ethereum , private	POA	Smart contract	confidentiality Privacy, Access Control, Scalability,
[19]	2020	Data transfer security, Security and privacy issues, Data theft, Data leakage	Distributed, Immutability, Cryptographic	Blockchain, Permissioned,	NA	On Blockchain	Integrity, Authentication Authorization, Security, Privacy, Anonymity
[20]	2023	Security and privacy issues, Data security, Data storage	Decentralization, Distributed Security	Ethereum , Private, permissioned	POA	Smart contract IPFS	Confidently Integrity Availability, access control Authentication Nonrepudiation, PRIVACY
[33]	2021	secure storage issues, Access control issues, Security and privacy issues, Malicious,	Decentralization, Immutability Distributed	Ethereum , Public	POW	Smart contract, IPFS	Confidently, Access Control Authorization, Privacy
[24]	2019	Privacy and security issues, DDos,	Decentralization, Immutability, Distributed	Permissioned, overly network	POA	Smart contract, cloud	Confidently, Integrity, Availability Authorization, privacy
[41]	2019	Secure storage data, Data integrity, Data management	Decentralization, Immutability, Distributed	Ethereum , permissioned	POW	Smart contract, IPFS	Confidently, Integrity, Access control Privacy,
[34]	2019	Security and privacy data, Transfer data, Attacks	Distributed, Cryptographic	Permissioned ,overly network)	POA	Smart contract cloud	Confidently, Integrity, Availability Authorization Privacy
[35]	2022	Security and privacy issues,	Decentralization, Cryptographic,	Ethereum ,	POA	Smart contract,	confidentiality integrity, authentication, access

		SPOF	Immutability, Distributed,	private and consortium,		IPFS	control, authorization, Privacy, Scalability,
[42]	2018	Security and privacy issues, Attacks	Decentralization Immutability, Distributed	Ethereum, Private, permissioned	POA	Smart contract, IPFS	integrity, access control, Privacy,
[43]	2024	Security and privacy issues, Huge medical data,	Decentralization Immutability, Distributed	Ethereum, permissioned	POA	Smart contract, IPFS	confidentiality integrity, authentication access control, Privacy, Scalability
[36]	2024	Security and privacy issues, SPOF,	Decentralization Immutability, Distributed	Ethereum	POW	Smart contract, IPFS	confidentiality integrity, authentication Transparency scalability
[44]	2024	Security and privacy issues	Decentralization Immutability, Distributed	Ethereum Private	NA	Smart contract, IPFS	confidentiality integrity, authentication, privacy Transparency
[45]	2022	Attacks, Cybercrimes, High cost	Decentralization Immutability, Distributed	Ethereum Private	NA	Smart contract, IPFS	Authorization access control, Transparency Trust scalability
[25]	2024	Security issues Attacks, Manipulation,	Decentralization Immutability, Distributed	Ethereum,	POW	Smart contract IPFS	confidentiality integrity, authentication, access control, privacy, transaparancy
[46]	2024	Data sharing issues, Low Scalability, Storage Data,	Decentralization Cryptographic,	Ethereum	POW	Smart contract IPFS	authentication, integrity, privacy, Access control, Scalability,
[47]	2024	Tamperproof personal health data (PHD) management issues	Decentralization Cryptographic,	Ethereum Permissioned	POW	Smart contract IPFS	authentication, integrity, Access control Privacy Scalability
[48]	2024	Attacks, Storage problem High cost,	Modular Architecture, Pluggable Consensus	HyperledgerFabric permissioned	CFT		authentication, Anonymity, Traceability,

Table 4: Comparative Analysis of Blockchain-Based IoT Security and Privacy Solutions in Supply chain

Pap.	**Year**	**Problems**	**Advantage of BC**	**Type NET/ Platform**	**Consensus**	**Smart ontract-storage**	**Security and privacy Considerations**
[50]	2022	SPOF, counterfeit, Attacks, Scalability issues	Decentralized, Immutability, Distributed,	Ethereum, private	POA	Smart contract, IPFS	Confidently, Authentication, Access control, Traceability, Transparency, Scalability, Throughput,

[51]	2023	Sustainability, Not used resource, Wasting foods, No trust, Data management	Decentralized, Immutability cryptographic	Ethereum EVM, Private	NA	Smart contract IPFS	Authentication Privacy Transparency traceability
[52]	2019	Data invisibility, Data management, Data tampering, Attacks, Trust issues,	Decentralized, Distributed,	Ethereum,	POA	Smart contract, IPFS	Confidently, Privacy Traceability
[53]	2022	Attacks, SPOF, Data tampered, Leakage of Data,	Decentralized, Distributed, Immutability,	Ethereum,	NA	smart contract, IPFS	Confidently, Integrity, Authentication, Privacy, Traceability
[54]	2023	Counterfeit drug, Fraud, Interoperability issues,	Decentralized distributed	Hyper ledger, Permission	NA	NA	Confidently Traceability Transparency
[55]	2022	Security and privacy issues, Data management, Attacks,	Decentralized, Distributed, Immutability,	Ethereum, Public	POW	Smart contracts IPFS	Confidently, Integrity, Availability, Privacy, traceability, transparency,
[56]	2021	no provenance, less transparency, trust issue, Storage problems, Attacks,	Decentralized, Distributed, Immutability	Ethereum,	POA	Smart contracts IPFS,	Integrity, Authorization, Access control, traceability, transparency, Trust
[57]	2022	Product tampering, Delays stages, Low Inefficiency, Exchange Data	Decentralized, Distributed, Immutability Reduce risk,	Ethereum,	POC	Smart contracts IPFS,	authorization, Transparency, traceability
[58]	2022	Security and privacy issues, SPOF, Attacks, Data management, Data tampered,	Decentralized, Distributed, Immutability	Ethereum, Permissioned	POA	Smart contracts IPFS,	Confidently, Integrity, Availability, Privacy, Access control traceability, Transparency, Scalability
[59]	2023	Information asymmetry in the pharmaceutical sector Attacks, Fraud,	Decentralized, Distributed, Immutability	Ethereum, Private Permissioned	POW Or POS Or POA	Smart contracts IPFS,	Integrity, Authorization, Availability, Privacy, Traceability,
[60]	2024	stakeholders, has become complex and vulnerable towards malicious attacks	Decentralized, Distributed, Immutability	Ethereum, Private, Permissioned	POA	Smart contracts IPFS	Confidently Integrirty Traceability Transparency privacy
[61]	2024	Theft,	Decentralized,	Ethereum	POA	Smart	Confidently,

		SPOf	Cryptographic Immutability			contracts IPFS	Integrity Traceability, Privacy, Trust, Transparency
[62]	2024	SPOf a privacy-centric solution that security, and privacy.	Decentralized, Cryptographic Immutability	Polkadot	NPOS	Smart contracts IPFS	Integrity Privacy Access control Scalability
[63]	2023	transparency, data visibility, and security challenges	Cryptographic	Ethereum	POC	Smart contract	Confidently authentication Access control Transparency Scalability
[26]	2024	security threats security issues e-commerce platform	Cryptographic Decentralized	Ethereum private	POA	NA	Integrity Authentication Privacy Traceability
[64]	2024	counterfeit product security threats	Cryptographic Decentralized	Hyperledg er Sawtooth private permission	PoET	NA	Traceability Scalability Transparency
[21]	2024	Security and privacy issues	Decentralized Immutability Cryptographic	Ethereum	POW	Smart contracts IPFS	Confidently Integrity Access control Transparency Authentication Privacy
[65]	2024	Security and privacy issues	Decentralized Immutability	Ethereum	POS	Smart contracts	Confidently Integrity Access control Authentication Transparency Traceability
[66]	2024	Trust and data management issues	Decentralized Immutability	Ethereum Private	POA	Smart contracts IPFS	Confidently Authentication Transparency Authentication Traceability
[67]	2024	challenging to monitor	Decentralized Immutability Cryptographic	Ethereum Private	POA	Smart contracts	Authenticity Transparency Traceability

Table 5: Comparative Overview of Blockchain-Enabled IoT Security and Privacy Approaches in Smart Cities

Pap.	**Year**	**problems**	**Advantage of BC**	**Type NET/ Platform**	**Consen sus**	**Smart contract-storage**	**Security Consideration**
[68]	2023	Cybersecurity risk, Attacks,	Cryptographic , Decentralized, Transparency, Democracy, Immutability	Ethereum,	POW	smart contract,	Confidently, Authentication ,
[27]	2023	Security issues, Trust,	Decentralized, Distributed	Ethereum,	POW	Smart contract	Confidently, Authentication , Authorization

[28]	2019	Security issues, Attacks, Data Storage	Decentralized, Distributed	Hyper ledger Fabric, Private,	NA	IPFS	Integrity, Confidently, Transparency,
[69]	2019	Security issues, Attacks, SPOF, Data storage,	Decentralization, Cryptographic Distributed,	Ethereum, Private,	POW	Smart contract IPFS,	Confidently, Integrity,
[29]	2020	Security issues, Storage issues, SPOF, Third party,	Decentralization, Distributed	Ethereum, Public,	POW	IPFS	Security, Authorization, Transparency,
[70]	2021	SPOF, Security and privacy issues, Attacks, Third party,	Distributed, Immutability, Distributed,	Quorum Blockchain Network QBN	NA	IPFS	Confidently, Integrity, Availability, Privacy,
[30]	2022	Security issues, SPOF, Attacks,	Distributed, Decentralization	Ethereum private permission	NA	Smart contract	Confidently, Authentication, Authorization, Privacy,
[31]	2022	Security issues, Attacks, Bottleneck,	Decentralized, Distributed, Immutability,	NEO blockchain	(dBFT)	Smart contract	Confidently, Integrity. Authentication,
[71]	2021	Privacy issues, Attacks,	Cryptographic, Decentralized, Distributed	Ethereum, Consortum,	POA	Smart contract IPFS,	Access control, Privacy, Authorization,
[72]	2024	unauthorized access and fraud	Cryptographic, Decentralized, Distributed	Blockhain	PUF	Smart contract	Confidently Integrity Authentication, Authorization, Transparency,
[22]	2024	Challenge of enhancing secure storage and transmission	Cryptographic, Decentralized, Distributed	Ethereum	POW	Smart contract IPFS,	Confidently Integrity Authentication, Authorization, Transparency
[73]	2024	IOT device	Cryptographic, Decentralized, Distributed				Confidently Integrity Authentication, Transparency
[74]	2024	Data Management issues	Cryptographic, Decentralized, Distributed	Ethereum	POW	Smart contract IPFS,	Confidently Integrity Authentication,
[75]	2024	Security issues, IOT Device	Decentralized, Distributed	Ethereum permissioned	POA	Smart contract IPFS,	Confidently Integrity, Authorization, Trust

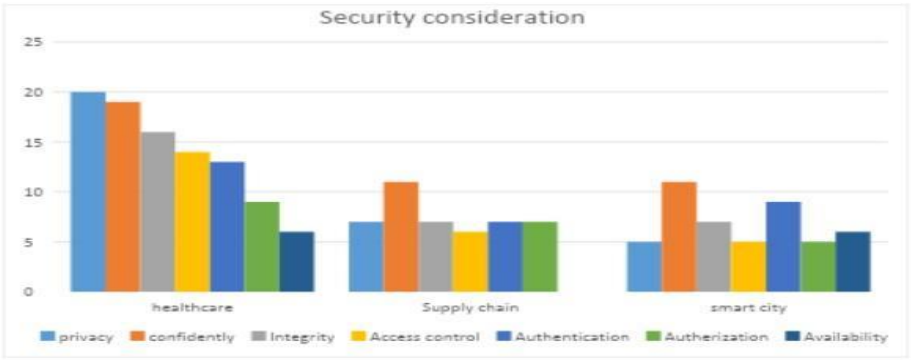

Figure 3: Security consideration to the IOT Application

4.3. Security Considerations and Standards in Blockchain-Based IoT Implementations

Ensuring robust security and privacy is essential for the successful deployment of blockchain-based IoT systems. This section presents a classification of selected studies based on the security objectives, threat models, and standards addressed in their blockchain integration strategies. Several studies specifically focus on countering well-known IoT threats such as Sybil attacks, Denial of Service (DoS), man-in-the-middle, and eavesdropping. These threats are mitigated through a range of security mechanisms, including access control, authentication, data integrity assurance, non-repudiation, and system resilience, as illustrated in Figure 3. To enhance data privacy, many studies incorporate advanced privacy-preserving techniques such as homomorphic encryption, zero-knowledge proofs (ZKPs), differential privacy, mixing protocols, and data anonymization. These techniques are critical in safeguarding sensitive user and device data within decentralized environments. Table 6 provides a comprehensive overview of the key security and privacy considerations addressed by blockchain-based IoT solutions across various application domains, including healthcare, smart cities, and supply chains. The table categorizes selected studies by year and highlights the specific security parameters each one focuses on—such as confidentiality, integrity, availability, authentication, authorization, access control, privacy, traceability, transparency, scalability, anonymity, auditability, reliability, and trust management. By mapping these attributes across implementations, the analysis reveals common priorities—such as confidentiality, access control, and privacy—as well as underexplored areas like auditability, trust management, and anonymity. This classification highlights the evolving strategies used to secure IoT ecosystems and provides insight into where further research and standardization are needed.

Table 6: Security considerations and standards for implementing blockchain in IOT

		Security consideration							Parameters or criterions							
Paper	**Year**	**Confidently**	**Integrity**	**Availability**	**Authentication**	**Authorization**	**Access Control**	**Privacy**	**Traceability**	**Transparency**	**Scalability**	**Anonymity**	**Auditability**	**Reliability**	**Trust management**	
[32]	2022	*	*				*	*			*					***Healthcare***
[37]	2023	*						*	*	*				*		
[23]	2022	*				*	*						*		*	
[17]	2022	*	*				*	*		*						
[38]	2021	*	*		*	*	*	*							*	
[49]	2019	*	*	*				*						*	*	
[39]	2023	*		*	*		*	*		*						
[40]	2023	*					*	*		*	*					
[19]	2020		*		*	*		*				*				
[20]	2023	*	*	*	*	*	*	*							*	
[33]	2021	*	*		*	*		*						*	*	
[24]	2019	*	*	*		*		*				*				
[41]	2019	*	*			*		*			*					
[34]	2019	*	*	*		*		*				*				
[35]	2022	*	*		*	*	*	*			*					
[42]	2018			*			*	*	*							
[43]	2024	*	*		*		*	*			*			*		
[36]	2024	*							*	*						
[44]	2024	*	*		*			*		*						
[45]	2022	*			*		*			*					*	
[25]	2024	*	*		*		*	*		*					*	
[46]	2024		*		*		*	*			*					
[47]	2024		*		*		*	*			*					
[48]	2024				*				*			*				
		19	16	6	13	9	14	20	4	8	7	4	1	4	7	
[50]	2022	*			*				*	*	*					Supply Chain
[51]	2023					*			*	*						
[52]	2019	*						*	*							
[53]	2022	*				*			*							
[54]	2023	*							*	*						
[55]	2020		*	*					*	*						
[56]	2021								*	*						
[57]	2022					*			*	*						
[58]	2022	*	*	*			*	*	*		*					

[59]	2023		*			*		*		*						
[60]	2024															
[61]	2024	*	*					*		*	*					*
[62]	2024						*	*		*	*					*
[63]	2023	*			*		*				*	*				
[26]	2024		*		*	*				*						*
[64]	2024	*				*	*	*		*	*	*				
[21]	2024	*	*		*		*	*		*	*					
[65]	2024	*	*		*		*			*	*	*				
[66]	2024	*			*	*				*	*					*
[67]	2024				*					*	*					
		11	7	2	7	7	6	7	18	14	5	0	0	0	4	
[68]	2023	*			*										*	Smart City
[27]	2023	*			*	*						*				
[28]	2019		*								*				*	
[69]	2019	*	*									*				
[29]	2020			*	*						*					*
[70]	2021	*	*	*				*							*	
[30]	2022	*			*	*	*	*	*							
[31]	2022	*	*		*			*				*				
[71]	2021						*	*					*			
[72]	2024	*		*	*	*					*					
[73]	2024	*		*	*			*			*		*			
[22]	2024	*	*	*	*		*				*		*			
[74]	2024	*	*	*	*			*			*			*		*
[75]	2024	*	*			*						*			*	
		11	7	6	9	4	3	5	1	6	4	3	1	2	3	

5. DISCUSSION

Blockchain technology significantly strengthens security and privacy in IoT systems by tackling fundamental vulnerabilities. Its decentralized architecture eliminates single points of failure, while immutable ledgers ensure data cannot be tampered with after recording. Advanced cryptographic methods—including encryption, zero-knowledge proofs, and anonymization—further safeguard sensitive information. Smart contracts play a crucial role by automating access control, allowing data sharing exclusively with authorized entities. In healthcare, blockchain facilitates secure management of patient data collected from IoT devices such as wearables and remote monitors. Encrypted health records remain accessible only through patient-held private keys, with smart contracts enforcing dynamic consent policies aligned with regulations like HIPAA. This framework also provides transparent audit trails and ensures data integrity by hashing real-time medical readings, thereby supporting reliable diagnostics. For smart city applications, blockchain enhances citizen privacy by anonymizing sensor data and enabling residents to interact with urban services via pseudonymous identities. Permissioned blockchains allow secure and confidential cross-agency data exchange without exposing raw datasets. In supply chains, blockchain offers traceability and transparency by recording product information and transactions immutably, preventing fraud and unauthorized data manipulation. Despite these benefits, challenges remain. Scalability issues arise from the high computational demands of consensus algorithms, which can strain resource-limited IoT devices. Interoperability between blockchain platforms and legacy IoT systems also requires further development to ensure seamless integration. To address these concerns, research is focusing on lightweight consensus

mechanisms, hybrid on/off-chain solutions, and standardized privacy frameworks that span multiple domains. Overall, blockchain presents a robust foundation for enhancing privacy and security in IoT across healthcare, smart cities, and supply chains. While promising, its widespread adoption depends on overcoming technical and operational challenges through continued innovation and optimization.

6. CONCLUSION

The advent of blockchain technology presents a transformative approach to enhancing scalability, data integrity, and privacy by ensuring consensus and trust across distributed systems. This article offers a comprehensive comparison of numerous IoT-focused studies, providing valuable insights for researchers and practitioners on blockchain applications in healthcare, supply chain management, and smart cities, along with practical recommendations for privacy preservation.

Blockchain integration with IoT not only strengthens security and privacy but also facilitates automation, transparency, interoperability, and long-term system resilience, positioning it as a pivotal technology for future interconnected ecosystems. However, several critical challenges remain, including scalability limitations, energy efficiency concerns, and the need for lightweight consensus mechanisms suited for resource-constrained IoT devices. Interoperability across diverse blockchain platforms and IoT standards, alongside evolving legal, ethical, and regulatory considerations, further complicate widespread adoption.

Future research should emphasize enhancing consensus protocols, exploring synergistic integration with edge computing and artificial intelligence, and addressing compliance frameworks to build user trust. Compared to previous works, this survey provides an in-depth analysis of security and privacy-preserving strategies in blockchain-IoT environments, highlighting ongoing design challenges and emerging solutions.

Looking forward, blockchain's role in IoT holds immense promise—from securing smart cities and autonomous systems to optimizing supply chains and personalized healthcare. Despite persistent obstacles, continuous innovation is set to establish blockchain-enabled IoT as a foundational pillar of tomorrow's digital infrastructure.

REFERENCES

[1] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," 2016. [Online]. Available: http://arxiv.org/abs/1608.05187

[2] N. Abbas, M. Asim, N. Tariq, T. Baker, and S. Abbas, "A mechanism for securing IoT-enabled applications at the fog layer," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, p. 16, 2019.

[3] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Addressing Security and Privacy Issues of IoT Using Blockchain Technology," *IEEE Internet Things J*, vol. 8, no. 2, pp. 881–888, 2021, doi: 10.1109/JIOT.2020.3008906.

[4] Y. Rahulamathavan, R. C. W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in *11th IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2017*, IEEE, 2018, pp. 1–6.

[5] R. Lai and D. LEE KuoChuen, "Blockchain – From Public to Private," in *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*, Elsevier, 2018, pp. 145–177.

[6] A. Tobin and D. Reed, "The Inevitable Rise of Self-Sovereign Identity," *White paper*, vol. 29, no. September 2016, p. 10, 2017, [Online]. Available: https://sovrin.org/library/

[7] L. Wang, Y. Ma, L. Zhu, X. Wang, H. Cong, and T. Shi, "Design of integrated energy market cloud service platform based on blockchain smart contract," *International Journal of Electrical Power & Energy Systems*, vol. 135, p. 107515, Feb. 2022, doi: 10.1016/j.ijepes.2021.107515.

[8] Horwitz Lauren and L. Rosencrance, "How Blockchain Technology Can Benefit the Internet of Things," IoT World Today. Accessed: Jun. 14, 2025. [Online]. Available: https://www.iotworldtoday.com/iiot/how-blockchain-technology-can-benefit-the-internet-of-things#close-modal

[9] L. Peng, W. Feng, Z. Yan, Y. Li, X. Zhou, and S. Shimizu, "Privacy preservation in permissionlessblockchain: A survey," *Digital Communications and Networks*, vol. 7, no. 3, pp. 295–307, Aug. 2021.

[10] IBM, "Empowering the edge - Practical insights on a decentralized Internet of Things IBM Institute for Business Value," IBM Institute for Business Value. Accessed: Jun. 14, 2025. [Online]. Available: https://docslib.org/doc/4604671/empowering-the-edge-practical-insights-on-a-decentralized-internet

[11] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

[12] P. K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018, doi: 10.1109/ACCESS.2017.2757955.

[13] M. Samaniego and R. Deters, "Hosting virtual IoT resources on edge-hosts with blockchain," in *Proceedings - 2016 16th IEEE International Conference on Computer and Information Technology, CIT 2016, 2016 6th International Symposium on Cloud and Service Computing, IEEE SC2 2016 and 2016 International Symposium on Security and Privacy in Social Netwo*, IEEE, 2017, pp. 116–119. doi: 10.1109/CIT.2016.71.

[14] D. Kundu, "Blockchain and Trust in a Smart City," *Environment and Urbanization ASIA*, vol. 10, no. 1, pp. 31–43, 2019, doi: 10.1177/0975425319832392.

[15] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/IJWGS.2018.095647.

[16] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future generation computer systems*, vol. 82, pp. 395–411.

[17] D. Mohan, L. Alwin, P. Neeraja, K. D. Lawrence, and V. Pathari, "A private Ethereumblockchain implementation for secure data handling in Internet of Medical Things," *J ReliabIntell Environ*, vol. 8, no. 4, pp. 379–396, 2022, doi: 10.1007/s40860-021-00153-2.

[18] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *Journal of Network and Computer Applications*, vol. 177, p. 102857, 2021, doi: 10.1016/j.jnca.2020.102857.

[19] R. Bosri, A. R. Uzzal, A. Al Omar, M. Z. A. Bhuiyan, and M. S. Rahman, "HIDEchain: A user-centric secure edge computing architecture for healthcare IoT devices," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2020*, IEEE, 2020, pp. 376–381. doi: 10.1109/INFOCOMWKSHPS50562.2020.9162729.

[20] D. Rani, R. Kumar, and N. Chauhan, " A secure framework for IoT -based healthcare using blockchain and IPFS ," *Security and Privacy*, vol. 7, no. 2, p. 348, 2024, doi: 10.1002/spy2.348.

[21] H. Saraswat, M. Manchanda, and S. Jasola, *An efficient secure predictive demand forecasting system using Ethereum virtual machine*. IET Blockchain, 2024. doi: 10.1049/blc2.12068.

[22] T. Wang, K. Chen, Z. Zheng, J. Guo, X. Zhao, and S. Zhang, "PrivShieldROS: An Extended Robot Operating System Integrating Ethereum and Interplanetary File System for Enhanced Sensor Data Privacy," *Sensors*, vol. 24, no. 10, p. 3241, 2024, doi: 10.3390/s24103241.

[23] S. K. Rana *et al.*, "Blockchain Technology and Artificial Intelligence Based Decentralized Access Control Model to Enable Secure Interoperability for Healthcare," *Sustainability (Switzerland)*, vol. 14, no. 15, p. 9471, 2022, doi: 10.3390/su14159471.

[24] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, "Optimized blockchain model for internet of things based healthcare applications," in *2019 42nd International Conference on Telecommunications and Signal Processing, TSP 2019*, IEEE, 2019, pp. 135–139. doi: 10.1109/TSP.2019.8769060.

[25] K. V. Deshpande, J. Shikshan, and P. Mandal, "MedBlock : Revolutionizing Healthcare Data Management through Blockchain MedBlock : Revolutionizing Healthcare Data Management through Blockchain and IPFS," 2024.

[26] S. Asaithambi, L. Ravi, M. Devarajan, A. S. Almazyad, G. Xiong, and A. W. Mohamed, "Enhancing enterprises trust mechanism through integrating blockchain technology into e-

commerce platform for SMEs," *Egyptian Informatics Journal*, vol. 25, p. 100444, 2024, doi: 10.1016/j.eij.2024.100444.

[27] R. Singh, S. Sturley, B. Sharma, and I. Ben Dhaou, "Blockchain-enabled Device Authentication and Authorisation for Internet of Things," in *1st International Conference in Advanced Innovation on Smart City, ICAISC 2023 - Proceedings*, IEEE, 2023. doi: 10.1109/ICAISC56366.2023.10084957.

[28] M. Son and H. Kim, "Blockchain-based secure firmware management system in IoT environment," in *International Conference on Advanced Communication Technology, ICACT*, IEEE, 2019, pp. 142–146.

[29] A. I. El Sayed, M. A. Aziz, and M. H. A. Azeem, "Blockchain Decentralized IoT Trust Management," in *2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies, 3ICT 2020*, IEEE, 2020, p. 3. doi: 10.1109/3ICT51146.2020.9311998.

[30] M. Turki, B. Dammak, and R. Mars, "A Private Smart parking solution based on Blockchain and AI," in *Proceedings of the 2022 15th IEEE International Conference on Security of Information and Networks, SIN 2022*, IEEE, 2022. doi: 10.1109/SIN56466.2022.9970548.

[31] O. Umoren, R. Singh, S. Awan, Z. Pervez, and K. Dahal, "Blockchain-Based Secure Authentication with Improved Performance for Fog Computing," *Sensors*, vol. 22, no. 22, p. 8969, 2022.

[32] K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 329–343, 2022, doi: 10.1016/j.eij.2022.02.004.

[33] C. Mistry *et al.*, "MedBlock: An AI-enabled and Blockchain-driven Medical Healthcare System for COVID-19," in *IEEE International Conference on Communications*, IEEE, 2021.

[34] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, p. 326, 2019, doi: 10.3390/s19020326.

[35] K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management," *IEEE Trans ComputSocSyst*, vol. 10, no. 4, pp. 1515–1527, 2023.

[36] J. Dutta and S. Barman, "Smart contract and blockchain-based secured approach for storing and sharing electronic health records," *Multimed Tools Appl*, pp. 1–25, 2024, doi: 10.1007/s11042-024-19714-7.

[37] E. Elgamal, W. Medhat, M. A. Elfatah, and N. Abdelbaki, "Blockchain in Healthcare for Achieving Patients' Privacy," in *20th International Learning and Technology Conference, L and T 2023*, IEEE, 2023, pp. 59–64. doi: 10.1109/LT58159.2023.10092352.

[38] N. Sharma and R. Rohilla, "Scalable and Cost-Efficient PoA Consensus-Based Blockchain Solution for Vaccination Record Management," *WirelPersCommun*, vol. 135, no. 2, pp. 1177–1207, 2024.

[39] L. B. Elvas, C. Serrão, and J. C. Ferreira, "Sharing Health Information Using a Blockchain," in *Healthcare (Switzerland)*, vol. 11, no. 2, MDPI, 2023. doi: 10.3390/healthcare11020170.

[40] A. Abbas and M. A. Hamid, "Adapting hybrid approaches for electronic medical record management and sharing using blockchainsharding," *Periodicals of Engineering and Natural Sciences*, vol. 11, no. 1, pp. 5–14, 2023, doi: 10.21533/pen.v11i1.3405.

[41] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[42] K. Azbeg, O. Ouchetto, S. Jai Andaloussi, L. Fetjah, and A. Sekkaki, "Blockchain andIoT for Security and Privacy: A Platform for Diabetes Self-management," in *2018 4th International Conference on Cloud Computing Technologies and Applications, Cloudtech 2018*, IEEE, 2018.

[43] D. Rani, R. Kumar, and N. Chauhan, " A secure framework for IoT -based healthcare using blockchain and IPFS ," *Security and Privacy*, vol. 7, no. 2, p. 348, 2024, doi: 10.1002/spy2.348.

[44] I. Boumezbeur*et al.*, "Secure EHR Sharing Using Blockchain and IPFS," *Studies in Science of Science| ISSN: 1003-2053, 42 (7), 1*, vol. 14, no. 7, p. 42, 2024.

[45] W. Khan, G. Kumbhare, and P. Pugaonkar, "Integrating IoT with Health Record Management System using IPFS and Blockchain," *Int J ComputAppl*, vol. 184, no. 4, pp. 49–52, 2022, doi: 10.5120/ijca2022922001.

[46] K. Tiwari and S. Kumar, "A healthcare data management system: blockchain-enabled IPFS providing algorithmic solutions for increased privacy-preserving scalability and interoperability," 2025. doi: 10.1007/s11227-025-07400-w.

[47] S. Ma and X. Zhang, "Integrating blockchain and ZK-ROLLUP for efficient healthcare data privacy protection system via IPFS," *Sci Rep*, vol. 14, no. 1, p. 11746, 2024, doi: 10.1038/s41598-024-62292-9.

[48] A. Shahidinejad, J. Abawajy, and S. Huda, "Untraceable blockchain-assisted authentication and key exchange in medical consortiums," *Journal of Systems Architecture*, vol. 151, p. 103143, 2024,

[49] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-Based Remote Patient Monitoring in Healthcare 4.0," in *Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing, IACC 2019*, IEEE, 2019, pp. 87–91. doi: 10.1109/IACC48062.2019.8971593.

[50] N. Anita, M. Vijayalakshmi, and S. M. Shalinie, "Blockchain-based anonymous anti-counterfeit supply chain framework," *Sadhana - Academy Proceedings in Engineering Sciences*, vol. 47, no. 4, p. 208, 2022.

[51] G. Sai Radha Krishna and P. Rekha, "Food Supply Chain Traceability System using Blockchain Technology," in *2022 8th International Conference on Signal Processing and Communication, ICSC 2022*, IEEE, 2022, pp. 370–375. doi: 10.1109/ICSC56524.2022.10009418.

[52] Q. Lin, H. Wang, X. Pei, and J. Wang, "Food Safety Traceability System Based on Blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019, doi: 10.1109/ACCESS.2019.2897792.

[53] B. C. Daulatrao, "Agri food supply chain using Ethereum smart contract_TCA," *International Journal of Modern Developments in Engineering and Science*, vol. 1, no. 3, pp. 11–16.

[54] D. H. Tanvir, R. Amin, A. Islam, M. S. Islam, and M. M. Rashid, "Blockchain Interoperability for A Reputation-Based Drug Supply Chain Management," in *2023 6th International Conference on Information Systems and Computer Networks, ISCON 2023*, IEEE, 2023. doi: 10.1109/ISCON57294.2023.10112196.

[55] I. A. Omar, M. Debe, R. Jayaraman, K. Salah, M. Omar, and J. Arshad, "Blockchain-based Supply Chain Traceability for COVID-19 personal protective equipment," *ComputIndEng*, vol. 167, p. 107995, 2022, doi: 10.1016/j.cie.2022.107995.

[56] S. K. Rana *et al.*, "Blockchain-based model to improve the performance of the next-generation digital supply chain," *Sustainability (Switzerland)*, vol. 13, no. 18, p. 10008, 2021, doi: 10.3390/su131810008.

[57] K. Shah, S. Rana, N. Solanki, V. Desai, D. Prajapati, and U. Vasita, "Blockchain-based Pharmaceutical Drug Supply Chain Management System," in *International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME 2022*, IEEE, 2022.

[58] V. Pawar and S. Sachdeva, "CovidBChain: Framework for access-control, authentication, and integrity of Covid-19 data," *ConcurrComput*, vol. 34, no. 28, p. 7397, 2022, doi: 10.1002/cpe.7397.

[59] M. Aslam, S. Jabbar, Q. Abbas, M. Albathan, A. Hussain, and U. Raza, "Leveraging Ethereum Platform for Development of Efficient Tractability System in Pharmaceutical Supply Chain,"*Systems*, vol. 11, no. 4, p. 202, 2023, doi: 10.3390/systems11040202.

[60] P. Pandey and K. Jeberson, "Securing Data Privacy in the Food Supply Chain Using Integrated BC-FL Technology," *Journal of The Institution of Engineers (India): Series B*, pp. 1–6, 2024, doi: 10.1007/s40031-024-01133-9.

[61] L. Amasala, M. Ponnuru, and P. Srideviponmalar, *Secure Goods Storage and Anti-Theft Approach using Ethereum Blockchain*, vol. 233. Procedia Computer Science, 2024. doi: 10.1016/j.procs.2024.03.190.

[62] S. Wilson *et al.*, "Blockchain-Enabled Provenance Tracking for Sustainable Material Reuse in Construction Supply Chains †," *Future Internet*, vol. 16, no. 4, p. 135, 2024, doi: 10.3390/fi16040135.

[63] Y. Madhwal, Y. Yanovich, S. Balachander, K. H. Poojaa, R. Saranya, and B. Subashini, "Enhancing Supply Chain Efficiency and Security: A Proof of Concept for IoT Device Integration With Blockchain," *IEEE Access*, vol. 11, pp. 121173–121189, 2023, doi: 10.1109/ACCESS.2023.3328569.

[64] A. Nawaz, L. Wang, M. Irfan, and T. Westerlund, "Hyperledgersawtooth based supplychain traceability system for counterfeit drugs," *ComputIndEng*, vol. 190, p. 110021, 2024, doi: 10.1016/j.cie.2024.110021.

[65] R. Senta, A. Sawant, and S. Jain, "Enhancing Food Safety and Transparency in the Supply Chain through Polygon Blockchain and Cloud Integration," *International Journal of Computing and Digital Systems*, vol. 20, no. 1, pp. 2210–142, [Online]. Available: http://dx.doi.org/10.12785/ijcds/XXXXXX

[66] Y. J. Su, C. H. Chen, T. Y. Chen, and C. W. Yeah, "Applying Ethereumblockchain and IPFS to construct a multi-party used-car trading and management system," *ICT Express*, vol. 10, no. 2, pp. 306–311, 2024, doi: 10.1016/j.icte.2023.12.007.

[67] M. HaiderSayma, M. R. Hasan, M. Khatun, A. Rajee, and A. Begum, "Detecting the provenance of price hike in agri-food supply chain using private Ethereumblockchain network," *Heliyon*, vol. 10, no. 11, 2024, doi: 10.1016/j.heliyon.2024.e30972.

[68] F. Z. Chentouf and S. Bouchkaren, "Security and privacy in smart city: a secure e-voting system based on blockchain," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1848–1857, 2023, doi: 10.11591/ijece.v13i2.pp1848-1857.

[69] K. Atasen and H. Ustunel, "Designing a Secure IoT Network by Using Blockchain," in *3rd International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2019 - Proceedings*, IEEE, 2019. doi: 10.1109/ISMSIT.2019.8932728.

[70] S. Balakumar and A. R. Kavitha, "Quorum-based Blockchain Network with IPFS to Improve Data Security in IoT Network," *Studies in Informatics and Control*, vol. 30, no. 3, pp. 85–98, 2021, doi: 10.24846/v30i3y202108.

[71] I. T. Javed, F. Alharbi, T. Margaria, N. Crespi, and K. N. Qureshi, "PETchain: A Blockchain-Based Privacy Enhancing Technology," *IEEE Access*, vol. 9, pp. 41129–41143, 2021, doi: 10.1109/ACCESS.2021.3064896.

[72] M. Turki, B. Dammak, and A. Alshahrani, "PufParkChain: Secure and Smart Parking Based on PUF Authentication and Lightweight Blockchain," *IEEE Access*, vol. 12, pp. 65754–65767, 2024,

[73] A. I. Basuki, D. Rosiyadi, H. Susanto, I. Setiawan, and T. I. Salim, "Privacy-preserving reservation model for public facilities based on public Blockchain," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 4, pp. 4418–4429, 2024, doi: 10.11591/ijece.v14i4.pp4418-4429.

[74] O. Zorlu and A. Ozsoy, "A blockchain-based secure framework for data management," *IET Communications*, vol. 18, no. 10, pp. 628–653, 2024, doi: 10.1049/cmu2.12781.

[75] D. Hanggoro, J. H. Windiatmaja, A. Muis, R. F. Sari, and E. Pournaras, "Energy-aware Proof-of-Authority: Blockchain Consensus for Clustered Wireless Sensor Network," *Blockchain: Research and Applications*, p. 100211, 2024, doi: 10.1016/j.bcra.2024.100211.

AUTHORS

Naser Abbas Hussein, University of Technology in Iraq, PhD student in Faculty of Science of Tunis, the University of Tunis El Manar, the research interests include, security, privacy, and identity management in IOT. and currently focus on the use of Blockchain for IOT Applications.