scientific reports

Check for updates

OPEN

Examining the factor's influencing IoT-blockchain based secure transmission services

Ala Alarood[1]✉, Ahmed Ibrahim[1], Adamu Abubakar[2] & Abdulkream Alsulami[3]

This study addresses the critical challenge of ensuring secure data transmission and management in Internet of Things (IoT) systems by proposing a blockchain-based architectural framework. Traditional IoT security models often lack fine-grained architectural validation and user-centric evaluation, leading to gaps in trust, data integrity, and operational transparency. To overcome these limitations, the research introduces a novel framework that integrates Transmission Nodes, Inspection Nodes, Forwarding Nodes, and a Blockchain Security Service to secure sensor data from source to destination. The study employs a mixed-method approach, combining conceptual modeling with subjective evaluation from 32 domain experts across development, administration, and IoT service delivery sectors. Key findings indicate that components like the Blockchain Security Service and Transmission Node scored highly in terms of security effectiveness, data integrity, and reliability, while Inspection Nodes revealed varied perceptions, highlighting areas for improvement. The contributions of this study are fourfold: (1) introducing a user-informed performance assessment model for blockchain-based IoT architectures, (2) validating an operational case scenario using real-world transmission flows, (3) offering a detailed architectural breakdown with defined roles for each node, and (4) establishing a multi-metric evaluation framework incorporating integrity, latency, scalability, and privacy. The findings provide both theoretical and practical insights for enhancing trust and performance in decentralized IoT environments.

Keywords Blockchain, IoT, Security, IoT protocol, Subjective evaluation

The Internet of Things (IoT) has emerged as a powerful catalyst for change in various sectors, facilitating the smooth amalgamation of tangible items with digital networks. The Internet of Things (IoT) facilitates the seamless communication, collection, and sharing of data among devices[1]. This enables the process of automation and enhances effectiveness in diverse industries. For example, in the field of manufacturing, Internet of Things (IoT) sensors can enhance production efficiency by continuously monitoring the performance of equipment in real-time, accurately predicting maintenance requirements, and minimizing periods of inactivity[2].

The IoT sensors are the central components of this networked landscape, playing a crucial role in collecting real-world data[4]. The architecture facilitating these sensors involves an intricate combination of devices, communication protocols, cloud infrastructure, and analytical tools, all operating in synergy to derive significant insights from the extensive flow of sensor data.

In recent years, there has been considerable interest in a system that utilizes blockchain technology to ensure data security and administration through the Internet of Things (IoT). Integrating blockchain technology with IoT devices offers improved security and privacy for data transmission and management[4]. Various scholarly articles provide innovative structures and frameworks to tackle the security obstacles in IoT contexts. These solutions employ the distributed ledger technology of blockchain to guarantee the integrity, immutability, and transparency of data[5,6]. Those proposed systems also include features such as access control, authentication, and encryption techniques to safeguard sensitive healthcare data[7,8]. By utilizing the decentralized nature of blockchain, these systems reduce the requirement for centralized servers, hence diminishing the likelihood of data breaches and unwanted access. Furthermore, the utilization of blockchain technology in IoT communication facilitates safe machine-to-machine (M2M) and human-to-machine (H2M) interactions by means of smart contracts and blockchain transactions. In general, these systems based on blockchain technology offer strong solutions for securing and managing data in IoT applications, especially in healthcare and pandemic management situations. This is one of the crucial motivation of this research.

[1]College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia. [2]Department of Computer Science, International Islamic University Malaysia, Kuala Lumpur, Malaysia. [3]Department of Information Technology at Al-kamil, University of Jeddah, Jeddah, Saudi Arabia. ✉email: aasoleman@uj.edu.sa

Despite the increasing adoption of blockchain in securing Internet of Things (IoT) frameworks, existing research largely overlooks the human-centric evaluation of these systems and fails to adequately break down the architectural components involved in data transmission and security. Current solutions often focus solely on technical simulations without validating the real-world operational effectiveness of architectural elements such as transmission, inspection, and forwarding nodes or the blockchain security service. This gap limits the practical deployment and trustworthiness of such systems.

This study is scoped to investigate the security and performance of IoT data transmission using a blockchain-enhanced architecture. It covers seven architectural variables—IoT Sensor Data Source, IoT Sensor Data Destination, Data Transmission Pattern, Transmission Node, Inspection Node, Forwarding Node, and Blockchain Security Service. The scope includes the design of a conceptual framework, simulation of a realistic data transmission scenario, and validation through subjective evaluation involving 32 experts from relevant stakeholder groups. The study does not include hardware implementation or real-time network deployment, but rather focuses on architectural modeling and performance analysis through structured stakeholder feedback.

There are many research approach toward getting to the root of an IoT-based decentralized data security mechanism by utilizing blockchain technology, but majority of them do not consider subjective evaluation nor they present user-base study associated to their presentation scheme[9]. Most of the previous research technique is designed to tackle the challenges related to data reliability, security, and privacy that can occur in traditional IoT-cloud systems[10]. The solution employs blockchain technology to securely store critical data created in the IoT system[11]. Some even highlighted the need for a mechanism incorporating an Unspent Transaction Output (UTXO) verification technique that relies on the RSA accumulator. This mechanism guarantees a consistent computational complexity for lightweight nodes[12]. Similarly, some study introduces a streamlined architecture for se-curing the sharing of information in the Internet of Things (IoT). This architecture employs a dual chain approach, which combines transaction and data blockchain to achieve distributed storage and ensure the integrity of data[13]. The suggested architecture also integrates a consensus mechanism to improve the efficiency of data registration, transactions, and privacy protection. Furthermore, a suggested data communication system for the Internet of Things (IoT) is based on blockchain technology. This mechanism guarantees the integrity of data and prevents harmful communication by managing and controlling communication tunnels.

Research Question 1 (RQ1): How do architectural components (Transmission Node, Inspection Node, Forwarding Node, Blockchain Security Service) contribute to secure and reliable IoT data transmission?

Hypothesis 1 (H1): Each architectural component of the proposed framework significantly enhances at least one dimension of performance.

Research Question 2 (RQ2): Do expert stakeholders (developers, administrators, IoT service providers) perceive the framework as practical and effective for real-world deployment? Hypothesis 2 (H2): There is a high level of agreement among expert respondents on the effectiveness and operational relevance of the proposed blockchain-integrated IoT architecture.

Research Question 3 (RQ3): Which component of the framework receives the highest and lowest evaluation in terms of performance metrics? Hypothesis 3 (H3): The Blockchain Security Service (BSS) receives the highest evaluation score, while the Inspection Node (IN) demonstrates the most variability in expert perception.

Considering that a lot of effort is put forward toward producing mechanism and technique associated with Blockchain for securing IoT transmissions, the users-and end-users are mostly not involved in almost all the mechanism proposed in the previous studies. The defining characteristic of IoT is its capacity to give concrete advantages by facilitating seam-less communication and service provision among devices, addressing the specific requirements of end-users in various industries. However, in the pursuit of enhanced security through the integration of Blockchain, the users, who are important to the use of IoT, are often excluded from the implemented processes and methods. Users act as intermediates to ensure that IoT provides the necessary services directly to end-users who benefit from IoT connections. These end-users, who come from different fields, have a complex connection with the services provided by IoT. As a result, this current study contributes in the following ways:

- The active involvement of users and end-users in the security architecture driven by Blockchain is crucial for utilizing and extracting benefits from IoT communication. This engagement is essential because of multiple crucial factors. User engagement provides a practical comprehension of the subtleties and prerequisites necessary for efficient IoT security. The experiential knowledge and insights of users regarding their individual demands, concerns, and obstacles in utilizing IoT devices can greatly contribute to the development of more precise and user-friendly security mechanisms.
- Furthermore, the effectiveness of Blockchain-based systems in safeguarding IoT transmissions relies on the active involvement of both users and end-users. Adopting a user-centric approach in design and development can result in the development of security mechanisms that are more inclusive, trustworthy, and effective. The creation of these systems must correspond precisely with the demands, desires, and concerns of the individuals who directly benefit from the services offered by IoT connectivity. This strategy has the potential to completely transform not just the security of IoT, but also the dynamic between technology and its users. It will create an environment based on trust, transparency, and giving consumers more control.

This study presents several key contributions that distinguish it from existing literature on IoT and blockchain integration for secure data transmission and management:

The study uniquely incorporates subjective evaluation from key stakeholders, including developers, system administrators, IoT service providers, and researchers. This user-based validation complements the technical assessment and introduces a practical, real-world dimension to evaluating blockchain-based IoT architectures.

We break down the IoT transmission and security framework into distinct functional components such as the Transmission Node, Inspection Node, Forwarding Node, and Blockchain Security Service. These components are assessed both independently and collectively, offering a granular view of the system's operational dynamics that is often absent in other works.

The proposed architecture is validated using a realistic case scenario that models the actual flow of IoT sensor data from source to destination through blockchain-enhanced nodes. This scenario includes key security operations such as packet header inspection and block-level hashing, providing empirical grounding for the evaluation.

A validated performance assessment model is implemented using defined metrics such as data integrity, transmission reliability, latency, scalability, privacy, and accuracy. This is achieved through structured questionnaire design, expert feedback, and statistical analysis.

This study contributes to the literature by offering a novel, modular, and evaluative IoT-blockchain framework validated through expert insights—addressing both architectural and usability dimensions. It builds upon and extends prior models by integrating user feedback into the performance assessment, focusing on measurable transmission metrics (e.g., latency, scalability, privacy), and breaking down overlooked components such as inspection and forwarding nodes. Unlike most studies that focus solely on simulations or cryptographic efficiency, this research offers an empirical, architecture-driven, and stakeholder-informed contribution that bridges the gap between conceptual design and practical adoption.

With the exception of this section, which is currently being discussed, which provides a summary of the research, the remaining portion of the paper is provided as follows: In the "Related work", the relevant work is presented, and in the "Research methodology", the research methodology is discussed. In "Presentation of the analyticalresults and discussion" portion, the analysis is presented, in "Implication of the study findings", the results of the research are discussed, and in "Conclusions", the implications of the research are presented.

Related work

Blockchain has emerged as a critical enabler for secure IoT environments due to its decentralized, immutable, and transparent nature. In[14], the authors proposed BDLT-IoMT, a novel blockchain framework integrated with Support Vector Machine (SVM)-based machine learning for secure data processing in the Internet of Medical Things (IoMT). This model addresses real-time medical data privacy and decision accuracy. Similarly, a consortium-based architecture, BAIoT-EMS, was developed in[15] to support small and medium enterprises (SMEs) using blockchain and augmented intelligence. The framework ensures secure communication and intelligent decision-making in IoT-driven business ecosystems.

Recent trends show a growing convergence between blockchain and artificial intelligence (AI), particularly in distributed learning environments. In[16], the authors conducted a multi-hierarchical lifecycle review highlighting how blockchain, IoT, and AI collectively enhance vehicular systems, enabling secure, data-driven operations across complex transportation infrastructures. Additionally[17], reviewed blockchain's role in energy conservation systems, emphasizing how AI and thermal fluid modeling can be integrated with decentralized ledgers to improve efficiency in sustainable IoT applications.

To address the scalability and latency issues in blockchain-IoT networks, lightweight consensus mechanisms have gained attention. In[18], B-LPoET was introduced as a middleware architecture employing multithreading to execute lightweight Proof-of-Elapsed Time (PoET) consensus, optimizing security and distributed transaction efficiency. Another study[19] developed a blockchain-based remote sensing framework to securely manage smart city data. This solution leverages distributed ledger capabilities to enhance data traceability, integrity, and trustworthiness in urban sensor networks.

Blockchain's potential in industrial applications is evident in recent work like ORAN-B5G[20], which introduces a next-generation Open Radio Access Network enhanced by machine learning for Industry 5.0. The framework supports beyond-5G communication scenarios, where blockchain ensures secure, high-throughput operations in mission-critical environments.

Extensive prior research exists on a blockchain-based system that utilizes the Internet of Things for data protection and management. The work of numerous individuals is essential in developing mechanisms and techniques linked with Blockchain to ensure the security of IoT transmissions. The study of Luqman and Faridi[21] conducts a thorough investigation into the convergence of blockchain technology with the security aspects of the Internet of Things (IoT). The study provides a clear and precise guide to understanding the complex relationship between blockchain and IoT security. Their thorough examination of vulnerabilities in the Internet of Things (IoT), along with the powerful impact of blockchain in reducing these issues, creates opportunities for future investigations and creative uses. Although there is currently no explicit system specifically designed for leveraging blockchain in IoT to en-sure data security and management, their efforts provide the foundation for a deeper and more sophisticated comprehension of how blockchain might enhance the security of net-worked devices.

Okegbile et al.[22] explores the complexities of a data-sharing system using blockchain technology in the context of cloud-edge computing-based Internet of Things (IoT) networks. The article does not expressly focus on describing a specific blockchain-based system for da-ta security and management in the Internet of Things (IoT). However, its main theme is around the integration of blockchain and cloud-edge computing to promote secure da-ta-sharing systems. The main objective is to assess the effectiveness of this integration by conducting a thorough examination of performance The study highlights the integration of blockchain technology and cloud-edge computing, proposing a new method to improve the security of data-sharing in IoT networks. The study suggests a framework that combines the decentralized and immutable characteristics of blockchain with the agility and proximate processing capabilities of cloud-edge computing. This framework has the ability to enhance data exchange while ensuring security procedures are maintained.

Mannayee and Ramanathan[4] propose a secure and distributed framework for re-source management (SDFRM) in Industry 4.0 contexts, specifically within a distributed and collaborative Industry 4.0 system. The proposed solution integrates privacy-preserving techniques into the Distributed Management Framework (DMF) to provide robust privacy in the Access Control (AC) procedures. The report does not explicitly refer to a system that utilizes blockchain technology for the purposes of data security and management within the context of the Internet of Things. The study highlighted the importance of including a privacy-preserving approach into the Distributed Management Framework (DMF) in order to establish a secure and distributed framework for resource management (SDFRM) in industry 4.0 scenarios.

While Xue et al.[23] present techniques of blockchain and edge computing integration in IoT applications, it fails to provide a blockchain-based solution for IoT data security and administration. The research resides within blockchain technology and the concept of edge computing in integration of blockchain with edge computing on the other hand, the study by Abdullah et al.[5] presents a new and secure architecture called BHIIoT, which utilizes blockchain technology to ensure data security in the healthcare sector. Additionally, it sug-gests a modification in the life cycle of medical wireless sensor networks for the purpose of data administration and optimization. Nevertheless, it fails to explicitly refer to the concept of "Internet of Things" in relation to the security and administration of data. The study presents a secure architecture for ensuring data security in E-healthcare through the utilization of blockchain technology. Additionally, it unveils the establishment of a distributed layered hierarchy to optimize the functionality of a medical wireless sensor network.

The emergence of the Internet of Things (IoT) has introduced a period of networked gadgets, enabling smooth communication and service offering. Nevertheless, this interdependence also pre-sents notable security obstacles. Zhang et al.[6] have addressed these challenges by intro-ducing an innovative method that utilizes consortium blockchain technology to enhance the security of IoT connectivity. Their innovative research centers around creating a decentral-ized service platform with the goal of ensuring secure communications between machines (M2M) and between machines and humans (M2H). Furthermore, their research emphasizes the creation of a streamlined Software Development Kit (SDK) and platform gateways specifically designed for IoT devices with limited resources.

The paper by Shang et al.[24] presents an innovative method for exchanging microgrid data by utilizing the capabilities of blockchain technology in the Internet of Things (IoT) framework. While the article does not specifically provide a specific system for securing and managing IoT data, its main objective is to propose a new approach to improve the security and efficiency of microgrid key management and data sharing using blockchain technology. Utilizing elliptic curve cryptosystem, specifically, the encryption technique within the cryptosystem has been the contribution of the research. This is typical within the approach of ex-changing the microgrid data are formulated and established by the blockchain.

According to Kavitha et al.[7] any healthcare data deserved some sort of privacy, be-because this has to do with some negative aspect of individual. That is why the study conceptualized Internet of Things (IoT) meant for managing healthcare data within a blockchain paradigm. The study revealed that combining these approach, will surely secure healthcare data more appropriately. The suggested methodology improves security measures against potential threats to healthcare data. The study presents a carefully crafted blockchain-based data security solution that aims to strengthen the integrity of healthcare data. The essence of their contribution rests in introducing a novel strategy to enhancing security measures against the various threats that pose a risk to healthcare data. Blockchain technology integration in healthcare data management not only improves security but also redefines trust and transparency. The suggested technique utilizes tamper-proof distributed ledgers to provide a resilient environment where healthcare data is protected from unauthorized adjustments or breaches.

The study conducted by El Majdoubi et al.[25] is a significant and innovative contribution to the field of healthcare data sharing. It introduces the SmartMedChain framework as a revolutionary approach. Although the Internet of Things is not explicitly mentioned, the ide-as of the proposed framework, which is driven by Blockchain technology, align with the fundamental principles of safe and networked data systems that are commonly seen in IoT environments. The implementation of a Privacy Agreement Management system demonstrates a dedication to safeguarding data privacy and ensuring responsibility, guiding the exchange of healthcare data towards a more secure and ethically aligned future in both the Internet of Things (IoT) and the wider healthcare sectors.

Arvind et al.[8] lead an in-depth investigation on the incorporation of a block-chain-based system in the Internet of Things (IoT) environment, focusing on its crucial func-tion in ensuring data security and management, particularly in the context of pandemic management. Their extensive research explores the significant consequences, difficulties, and possibilities of utilizing IoT in pandemic management, while emphasizing the security and privacy issues associated with contact tracing and the use of Big Data as a key aspect of their investigation. There are crucial studies which combine IoT and blockchain intending to enhance security of the system. Crucial to that is the work of Ngabo[26]. It is established that Fog computing among distributed computing was found to be one of the most critical architecture that can utilized IoT, and the security system that can be efficiently for this kind of concept is proof to be the elliptic curve cryptosystem[26]. That is why Ngabo[26] examine how to introduce blockchain in such cases. The study revealed that public blockchain is most suited for fog computing with elliptic curve cryptosystem.

Abbas et al.[27] established that a concept of blockchain-assisted secure data management (BSDMF) is very necessary for healthcare data. Specifically, the research revealed that Internet of Medical Things (IoMT) associated with blockchain can be appropriate in handling secure data management of healthcare. Experimental analysis revealed that the latency in terms of response of the system as well as accuracy in terms of security of the system achieved high performance.

An Industrial Internet of Things (IIoT) is an emerging system where it allows industrial operations round the clock. Typically, Dwivedi et al.[28] revealed that in such system, a blockchain can be crucial. That is why the study

conceptualized a smart contract-based se-cure IIoT. The findings indicate that incorporating a blockchain smart contract can securely prevent IIoT operation over any complex situation.

Uppal et al.[29] proposed a framework associated with health information sharing platform described as "CareBlocks". The framework dwells on blockchain and IoT. The framework was implemented on the medical area. Hence a strategic concept was tested in which data integrity of healthcare system data was experimented. The finding indicates a good performance of data integrity where each data is sure with its separate hash.

Many previous studies on blockchain-based systems for data security and management in the context of the Internet of Things (IoT) have neglected to prioritize a user-centric approach. The mechanisms and techniques proposed in these studies often fail to involve users and end-users. This study focuses on that topic for that reason.

Research methodology

The present research makes use of a mixed-method research technique, which includes both qualitative and quantitative research methods, in order to conduct a comprehensive investigation into the proposed Blockchain-based system for data security and management of Internet of Things." This strategy involves the development and validation of an architecture by means of the collection of data pertaining to particular variables that are obtained from the proposed system. Standardized instruments are utilized in this process.

The proposed architectural framework

The architecture of the Internet of Things (IoT) revolves around the deployment of actual IoT sensors that are strategically placed across the environment. The purpose of these sensors is to gather various parameters, such as temperature, humidity, motion, and pressure. Equipped with communication capabilities, these sensors form the fundamental layer of the architecture and act as the primary sources of data. Their ability to rapidly collect and transmit data is essential for the success of the overall IoT ecosystem.

The proposed architectural framework is developed to enhance secure data transmission in Internet of Things (IoT) environments through blockchain integration. To establish a coherent understanding of the system design, Fig. 1 illustrates the sequential flow of data from generation at sensor nodes to its final delivery at the destination, while undergoing multiple verification and security layers. The framework introduces a modular design encompassing six fundamental components. These components are positioned to handle specific responsibilities across the data transmission lifecycle. First, the Sensor Data Source (SD) serves as the origin of data collection. These are the IoT-enabled devices that initiate data generation based on their real-world interactions, such as temperature monitoring, health diagnostics, or industrial tracking. Once data is generated, it is transmitted to the Transmission Node (TN). This node facilitates the initial data capture, ensures proper formatting, and handles first-layer encryption to secure the payload.

The data then flows to the Inspection Node (IN), a midstream checkpoint responsible for assessing the integrity of data packets. The inspection mechanism leverages blockchain-enabled hash verification and predefined security policies to determine if the data is unaltered and authentic. Packets that pass inspection proceed to the Forwarding Node (FN), where they are assigned block identifiers and cryptographically linked to previous entries, thereby ensuring tamper-evident logging. Next, the data is passed to the Blockchain Security

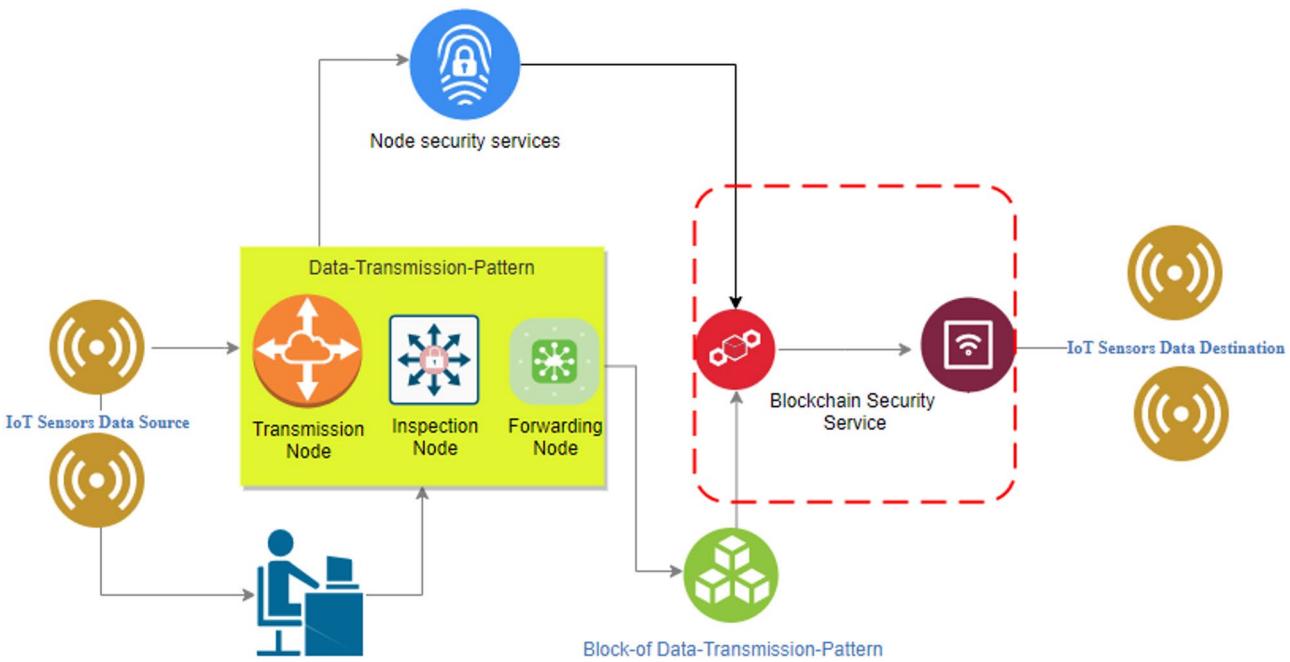

Fig. 1. The proposed conceptual framework.

Service (BSS). This service provides decentralized ledger management, enforces access control policies, validates consensus, and ensures the immutability of the transmitted data across the distributed IoT network. Finally, data reaches the Sensor Data Destination (SDD) where it can be utilized for decision-making, visualization, analytics, or long-term storage.

Each of these architectural elements, as illustrated in Fig. 1, plays a vital role in enabling layered security, data traceability, and performance efficiency. To facilitate a structured evaluation, the architecture is abstracted into the following variables: SD (Sensor Data Source), P (Transmission Pattern), TN (Transmission Node), IN (Inspection Node), FN (Forwarding Node), BSS (Blockchain Security Service), and SDD (Sensor Data Destination). These variables are used in subsequent sections for conceptual and expert-driven performance evaluation.

The integration of these components, their distinct roles, and their interconnections through blockchain constructs form the core contribution of the proposed framework, bridging the gap between theoretical design and applied security infrastructure in IoT networks.

Within the architectural framework, the Blockchain Security Service (BSS) plays a dual role. From a system design perspective, it functions as an independent architectural unit, responsible for access control, hashing, consensus validation, and immutability enforcement. However, from a performance flow standpoint, BSS also operates downstream, relying on the outputs of earlier components such as the Forwarding Node and Inspection Node. Therefore, while BSS is evaluated independently in terms of its effectiveness, it is also positionally dependent in the data flow sequence. This layered dependency is reflected in the architectural model (Fig. 1).

The proposed architectural variables

The proposed research variables are: "IoT Sensor Data Source", "IoT Sensor Data Destination". "Data Transmission Pattern", "Transmission Node", "Inspection Node", "Forwarding Node", and "Blockchain Security Service". These variables are obtained from the scenario in which data needs to be transmitted from the source sensor to the destination sensor. The landscape of IoT data security and management is characterized by several elements that are crucial for guaranteeing effective operations, data integrity, and network resilience. Each variable is specifically designed to serve its purpose within the transmission session, as part of the Internet of Things architecture that utilizes blockchain technology.

IoT sensor data source The operational definition of this variable is directly expressing a particular location or point of origin from which data is generated by Internet of Things sensors. It is referred to as the IoT Sensor Data Source. Includes a wide range of sensors, including temperature sensors, motion sensors, cameras, and others, that are distributed throughout Internet of Things devices. Obtains raw data from the tangible world or from devices that are part of the Internet of Things ecosystem. consists of the fundamental input that is used for subsequent processing, analysis, and use inside the Internet of Things network.

The justification of using this as the research variable lies with The Internet of Things (IoT) depends on sensors to provide data for different IoT services. There is an issue associated with reading of sensor in that an error and other signal interference can lead to a fluctuations of data reading. This will affect the efficiency of the entire system[30]. The research can critically be situated towards leading to an increase in impact secure IoT. Even though the method associated to IoT security can be directly dependent on the resource's computational capabilities[31]. That raised a concern that each microcontroller unit in IoT system requires a specific security operation. Hence integrating a blockchain covers that option and then enhances a security operation since blockchain will provide any sensor data a hash and an associated link to that hash. For that reason, efficient security of data in transmission and at storage has been identified[32]. Encrypting the gathered data is crucial in wireless sensor networks to mitigate security vulnerabilities. An innovative method incorporates homomorphic encryption algorithms into sensor equipment, enabling the transmission of encrypted data and performing computations on the encrypted data[33]. Finally, an evaluation is conducted on the utilization of biometric data from IoT devices for generating randomness. The study concludes that human gait is not a good source of randomness. However, the use of data from several sensors does marginally enhance the level of randomness[34]– [35].

IoT sensor data destination The operational definition of "Data Destination for Internet of Things Sensors" is the endpoint or location that has been designated for the purpose of sending, storing, or processing data generated by Internet of Things sensors. It serves as a representation of databases, cloud servers, analytics platforms, or certain Internet of Things devices. The efficient handling of sensor data guarantees that it is sent to the intended destinations within the Internet of Things architecture for the purposes of analysis, decision-making, or storage.

The rationale for utilizing this as a study variable is based on the capability of IoT sensors to communicate data to a remote server for analysis and storage[33]. In the field of wireless sensor networks, the collected data is encrypted using homomorphic encryption algorithms before being transferred[36]. This allows the server to do computations on the encrypted data without decrypting it, ensuring the data's security[37]. To detect irregularities in sensor data for monitoring grain in large horizontal grain bins, typical machine learning methods like Location Factor, Isolation Forest, and One-class Support Vector Machine can be utilized[38].

Data transmission pattern The operational definition of the "Data Transmission Pattern" describe the structure or arrangement that defines the flow and method of transporting data from Internet of Things devices to their intended destinations. This is also associated to the sequence, frequency, for-mat, and protocols that are utilized for the transmission of data created. Furthermore, the delay of data, the usage of bandwidth, and the overall effectiveness of the network are all affected by the various transmission patterns. There is a reduction in congestion and an improvement in the overall performance of Internet of Things networks as a result of optimized data transmission patterns, which enable timely and reliable delivery of information.

The justification of using this variable for this study lies with the fact that "Data trans-mission patterns play" a crucial role in a range of technologies, including IoT monitoring services and 5G communication systems. A data accuracy pattern-based transmission period control technique is suggested in IoT monitoring to minimize energy usage while guaranteeing precise data restoration[39]. Pattern exclusive codes (PECs) are developed in the context of 5G communications to combine information from many sources and facilitate da-ta transmission without the need for packets[40].

Transmission node The operational definition of "Transmission node" describes a scenario where a transmission of data between Internet of Things devices and the larger network or blockchain infrastructure operate. That is, a transmission node is a component of the network that is responsible for transfer between nodes within the network. Effective transmission nodes contribute to the management of data flow, which in turn ensures that Internet of Things devices and the blockchain-based system work together without any hiccups. When it comes to Internet of Things environments, having transmission nodes that are reliable helps to reduce latency, improve network stability, and bring about an increase in data throughput.

The justification of this lies with the fact that "a transmission node is tasked with sending data to other nodes within the network. The system has the capability to choose a transmission strategy from a variety of available options and send data to communication nodes[41]. If the main link connected to a reception node has a poor communication environment, the transmission node might choose to use an auxiliary transmission node. In this case, the transmission node will send a signal to the reception node through the main connection during a specific time period called the initial transmission period[42]. In certain transmission session associated to relay, that particular transmission source note, being the initiator of the transmission, link direct to the next directed node, similar to blockchain approach, hence even before the introduction of the blockchan, in a network transmission session, the pattern is the same[43]. When relating this to a wireless communication system, introducing a blockchain will effectively search as a secure transmission and prevention of data.

Inspection node This study formulated the notion of a "Inspection node" and provided a clear definition of its function within the blockchain-based system. The Inspection Node is a crucial component tasked with verifying the authenticity and reliability of the data transmitted via the Internet of Things (IoT). Prior to gaining access to the blockchain network, data packets undergo scrutiny to verify their compliance with the established criteria. Ensures data integrity by avoiding the introduction of incorrect or malicious data into the network environment. Utilizing safe inspection nodes guarantees the integrity of the data stored in the blockchain, hence enhancing the overall security and reliability of the system.

The rationale for choosing the term "Inspection node" as a variable is based on the fact that data packet inspection is a method used to analyses the behavior of network subscribers and predict their service category[44]. The procedure involves analyzing deep packet inspection (DPI) data, which displays the network usage of subscribers and the types of services they are using[45]. By employing ensemble learning techniques on the DPI dataset, it is feasible to efficiently address the classification and prediction problem with a significant degree of accuracy[46]. This technique allows for a more thorough understanding of subscribers' individual behavior, detection of network abnormalities, and development of advanced Deep Packet Inspection (DPI) technologies[47]. Furthermore, the implementation of data packet transmission techniques can improve the reliability of data transfer and ensure optimal network throughput[48]. These strategies include the sending and resending of data packets at predetermined time intervals. Data packet inspection and transmission algorithms are crucial for assessing network behavior, predicting service categories, and optimizing data delivery.

Forwarding node The operational definition of "A forwarding node" is a component of a network that is accountable for the routing and direction of data packets generated by the Internet of Things (IoT) through the blockchain infrastructure. Allows data packets to be routed according to predetermined rules or protocols, thereby optimizing their delivery to the destinations that have been chosen. To ensure that data flows and is delivered correctly throughout the network, efficient forwarding nodes are essential. The presence of efficient forwarding nodes in Internet of Things environments contributes to the reduction of data congestion, the improvement of data delivery, and the enhancement of network performance.

The justification of selecting "forwarding node" lies with the fact that a forwarding node is a network node that directly transmits messages or data sent by other nodes. It enhances the efficiency of a networking system[49]. In this case, a forwarding node is a P node that calculates the time delay for forwarding between two endpoints of a test system[50]. In the context of an aggregating server, a forwarding node is a secondary proxy node that transfers data from a first node to a second node in a remote address space based on an in-put/output connection[51]. In the context of determining the path for message forwarding, a forwarding node is a network node that must be included in the message forwarding path in order to guarantee network security[52]. In the context of a packet forwarding mechanism, a forwarding node is a node that removes the segment routing header before passing the IPv6 packet[53].

Blockchain security service In the context of the blockchain architecture, Blockchain Security Service refers to specialized methods and protocols that are designed to protect data created by the Internet of Things (IoT). The data that is stored on the blockchain is protected through the utilization of crypto-graphic techniques, consensus procedures, and access control systems. It guarantees the immutability, integrity, and confidentiality of the Internet of Things data that is stored on the blockchain. The overall security posture of Internet of Things ecosystems is improved by robust blockchain security services, which provide a basis for trust, privacy, and resistance against cyber threats.

The justification of using "Blockchain security service" lies with the fact that the utilization of blockchain technology aims to improve data integrity and minimize vulnerability across many domains. An example of such utilization is in cloud-based data storage, where encryption and data verification methods are employed to guarantee the security and reliability of client data[54,55]. Blockchain is also being utilized in the administration of electronic health records, providing enhanced data accessibility, security, and privacy[56]. Healthcare practitioners can enhance their ability to forecast and assist in diagnosis by leveraging blockchain technology in conjunction with machine learning and artificial intelligence[57]. In general, blockchain-based solutions offer a very secure and dependable method for managing data, rendering it extremely difficult to hack or disclose information without authorization[58]. The progress made in blockchain technology has the capacity to trans-form multiple industries and enhance the precision, cost-efficiency, and security of data management systems.

The conceptual framework

The study's architectural framework (see Fig. 1) involves the transmission of sensors from the source to the target. The data will pass via a Blockchain-based system to ensure data protection and management before reaching the destination. The purpose of data security and management prior to reaching its destination is to establish. For that reason, the variables conceptualized are:

S = IoT Sensor Data Source.
D = IoT Sensor Data Destination.
P = Data Transmission Pattern.
TN = Transmission Node.
IN = Inspection Node.
FN = Forwarding Node.
BSS = Blockchain Security Service.
Based on this, the data transmission process is defined as follows:

$$S \xrightarrow{P} TN \xrightarrow{IN} FN \xrightarrow{BSS} TN \tag{1}$$

Equation (1) illustrates the flow of data from the IoT Sensor Data Source (S) through the Data Transmission Pattern (P), Transmission Node (TN), Inspection Node (IN), Forwarding Node (FN), and finally reaching the IoT Sensor Data Destination (D).

1. Data transmission pattern: The data transmission pattern refers to the process of handling data from sensors associated with a specific transmission session. This involves various activities at the transmission, inspection, and forwarding nodes as the data travels from the source to the destination. Giving that:

$$S(t) - a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0$$

where *S(t)* represents the sensor data at time *t*, and $a_n, \ a_{n-1} \ \ldots \ a_0$ are coefficients.

a. The transmission node activities consist of maintaining a record of the "Data" during transmission. Each data in transmission between one sensor to the other is provided with a header information. When transferring sensor data, it is crucial to include a header in the data packet format. Typically, it comprises data that assists in the identification, organization, and interpretation of the sent information. The IEEE (Institute of Electrical and Electronics Engineers) does not require a specific format for sensor data headers. Instead, it develops standardized communication protocols and data formats used across several areas of electronics and electrical engineering. However, specific protocols or industries may utilize or reference IEEE standards for the transmission of sensor data. IEEE 1451 sets forth standards for intelligent transducer interfaces, which involve the transmission of data from sensors. Nevertheless, even when following these guidelines, the exact arrangement of the header may vary based on the specific implementation and protocol used. In this instance, the ongoing research is conceiving the acquired data to be systematically organized with a unique identifier at the start of each transmission session at every "transmission node.".
b. The inspection node involves deep inspections of every header field of each series of the data in transmission from which the header details involving:

   i. Preamble: a field that content series of bits used to synchronize the receiver's clock and prepare for data reception.
   ii. Start Delimiter: a field that content marks for which it indicates the start of the packet/frame.
   iii. Control: a field that controls certain aspects of the frame, such as addressing and data type.
   iv. Address: a field that specifies the address of the source and destination for which the data will be used for the transmission.
   v. Payload Length: a field that indicates the size of the data in transmission with associated headers data.
   vi. Payload: a field that indicates the actual sensor data being transmitted.
   vii. CRC (Cyclic Redundancy Check): a field that indicates a calculated value used for error checking to ensure data integrity.
   viii. End Delimiter: a field that marks the end of the packet/frame.

An inspection of the entire field will be conducted, with each data in the transmission session being examined based on its serial number. The purpose of the inspection is to verify the existence of the data transmitted from the source sensor node.

#	Items	11	12	13	44	15
11	How does the blockchain-based system guarantee the secure and dependable transmission of data to the specified destination for IoT services?					
22	Could you provide more details regarding the techniques employed to manage diverse IoT service data and effectively direct them to their designated destinations utilizing blockchain technology?					
33	How does this system ensure that data integrity and accuracy are given priority when transferring IoT service data to various destinations?					
43	Could you elaborate on the scalability issues faced while handling IoT service data destinations in the blockchain architecture and how they were resolved?					
55	What steps are taken to guarantee compatibility between IoT devices and their assigned data destinations in the blockchain network, particularly in light of different communication protocols and data formats?					
66	How does the blockchain-based system handle latency and enhance data delivery to the IoT service data destination, particularly while managing substantial amounts of real-time data streams from many sources?					

Table 1. IoT sensor data source and destination Items.

#	Items	11	12	13	44	15
11	Could you elucidate the precise data transmission patterns employed in the blockchain-based system for transferring information from IoT devices to their intended destinations?					
22	How are transmission nodes engineered and employed in this system to guarantee the efficient and secure flow of IoT-generated data over the blockchain network?					
33	Could you provide more details about how inspection nodes contribute to checking the integrity and authenticity of transmitted IoT data within the blockchain infrastructure?					
44	What tactics or protocols are used at the forwarding nodes to enhance the routing and delivery of IoT data within the blockchain network?					
55	How does the blockchain-based system manage data redundancy and packet loss when transmitting from IoT devices to their destinations?					
66	How does the system efficiently allocate and control data traffic across different transmission nodes while handling different types of IoT-generated data within the blockchain network?					

Table 2. Data transmission pattern Items.

#	Items	11	12	13	44	15
11	Please elucidate the central function of transmission nodes in the blockchain-based system for managing IoT data and how they enable the flow of data between IoT devices and the blockchain network.					
22	What specific protocols or processes are used in transmission nodes to guarantee the secure and dependable transmission of data from IoT devices to the blockchain network?					
33	Can you elaborate on the difficulties faced while establishing connectivity between IoT devices and transmission nodes inside the blockchain architecture, and explain the strategies employed to overcome these challenges?					
44	How does the system manage potential bottlenecks or congestion at transmission nodes, particularly during periods of high data traffic from several IoT devices?					
55	What strategies are implemented in transmission nodes to enhance data throughput and reduce latency while transmitting various types of IoT-generated data across the blockchain network?					
66	The technology ensures the integrity and validity of data packets transmitted by IoT devices through the transmission nodes in order to maintain a secure and tamper-proof data flow inside the blockchain network.					

Table 3. Transmission node Items.

c. Right after the inspection, once it is confirmed that the header details are still intact, the series of data will be sent to the "forwarding node". At this node, every series will be allocated to a "Block" of a blockchain and directed to the "node security services" which encompass the process of hashing the block. This implies that two distinct concurrent operations were scheduled to be executed, and now both of these activities will be transmitted to the "Blockchain Security Service".

2. At the "Blockchain Security Service," which is a point in the conceptualization of the architecture, it is the point at which typical features like device authentication, data encryption, access controls, and monitoring will be carried out in order to guarantee that security is of the utmost importance in every facet of the Internet of Things architecture. Consequently, this layer is regarded as the specialist security layer because of this reason. It protects the privacy and security of data collected by the Internet of Things, thereby decreasing the risks that are associated with a system that is heavily interconnected.

Development of research items

The process of constructing research questionnaires entails a methodical strategy to guarantee the reliability and excellence of survey research[59]. This current study questions are formulated by considering the latest trends, state-of-the-art studies, and technological advancements in the study domain, which is the view from many studies[60,61]. The text in the questions is already straightforward and precise. The entire questions are pretested, validated and pilot tested. Hence the final questions for each variable (see Tables 1, 2, 3, 4, 5 and 6), after

#	Items	11	12	13	44	15
11	What are the primary purposes and duties of inspection nodes in a blockchain-based system for managing IoT data, specifically in relation to data validation and verification?					
22	Can you clarify the verification process conducted by inspection nodes to guarantee the integrity and validity of IoT-generated data that enters the blockchain network?					
33	How does the system address discrepancies or inconsistencies identified by inspection nodes throughout the verification process, particularly when handling possibly hacked IoT data?					
44	What procedures or algorithms are used in inspection nodes to identify and prohibit the inclusion of harmful or fraudulent data entries in the blockchain ledger that originate from IoT devices?					
55	Can you elaborate on the scalability considerations pertaining to inspection nodes in the context of managing a substantial quantity of IoT devices and the consequent effect on the overall efficiency of the blockchain-based system?					
66	How does the system ensure privacy when inspection nodes check and process IoT-generated data within the blockchain network, particularly when handling sensitive information?					

Table 4. Inspection node Items.

#	Items	11	12	13	44	15
11	The fundamental function of forwarding nodes in the blockchain-based system for IoT data management is to facilitate the routing and distribution of data within the network.					
22	How do forwarding nodes effectively route IoT-generated data packets to their assigned destinations inside the blockchain architecture, while also assuring security and reliability?					
33	Could you provide more details regarding the decision-making methods or algorithms employed by forwarding nodes to enhance data routing patterns for various categories of IoT-generated data within the blockchain network?					
44	What measures or safeguards are implemented in forwarding nodes to manage network disruptions or node failures and ensure uninterrupted data transmission and delivery in the blockchain infrastructure?					
55	The system manages the trade-offs between speed and accuracy by effectively routing different IoT-generated data across the blockchain network to their designated destinations.					
66	How does the blockchain-based system handle load balancing and prioritize data flow at forwarding nodes, particularly during high-demand periods or abrupt increases in data transmission from IoT devices?					

Table 5. Forwarding node Items.

#	Items	11	12	13	44	15
1	What are the main security measures used in the blockchain architecture to protect IoT-generated data during transmission and storage?					
2	How can the system guarantee the confidentiality, integrity, and authenticity of data by utilizing blockchain-based security services in an Internet of Things (IoT) setting?					
3	Could you elaborate on the encryption or hashing mechanisms employed to bolster data security in blockchain-based IoT data management?					
4	The system employs robust mechanisms for identity verification and access control to regulate the participation of devices in the blockchain network, thereby ensuring that only authorized organizations are able to engage.					
5	How can the blockchain-based security solution safeguard against potential cyber dangers, such as DDoS assaults or tampering efforts, particularly in a distributed IoT environment?					
6	Can you provide more details on the techniques implemented to regularly upgrade and uphold the security protocols within the blockchain framework, ensuring ongoing protection against emerging security risks in the management of IoT data?					

Table 6. Blockchain security service items.

undergoing pre-evaluation are found to be focused, explicit, and succinct, and provide a clear foundation for generating precise response in both qualitative and quantitative direction.

There are six items for the variable "IoT Sensor Data Source and Destination" designed to assess the influence of data measurement on security and blockchain at both the source and the destination. Each question is anticipated to receive two responses. The assessment includes both open-ended responses and a score system ranging from 1 to 5, which is dependent on the submitted answers. This particular questionnaire aims to collect valuable insights and information regarding the efficiency and capabilities of the blockchain-based system in dealing with crucial concerns pertaining to the secure transmission, management, integrity, scalability, compatibility, and real-time delivery of IoT sensor data. The responses will offer a thorough comprehension of the system's capabilities and potential obstacles in fulfilling the demands of IoT services, together with the extent of their influence. This information is essential for enhancing the system, guaranteeing its dependability, and guiding decision-making processes concerning IoT data management.

Similarly, there are six elements for the variable "Data Transmission Pattern Items" (see to Table 2) that were designed to assess the influence of the variable on both security and blockchain. Each question is intended to have the same two responses. The assessment includes both open-ended responses and a score system ranging from 1 to 5, which is dependent on the follow up open-end question answers.

Table 3 contains six factors for the variable "Transmission Node" that were specifically created to evaluate its impact on both security and blockchain. Every question is designed to elicit the same two answers. The assessment comprises of both open-ended responses and a scoring system that ranges from 1 to 5. The scoring is determined based on the answers to the subsequent open-ended questions.

Additionally, Table 4 presents six factors pertaining to the variable "Inspection Node" that were specifically devised to evaluate its impact on both security and blockchain. Every question is designed to elicit the same two answers. The assessment comprises of both open-ended responses and a scoring system that ranges from 1 to 5. The scoring is contingent upon the answers provided in the subsequent open-ended questions.

In a similar vein, the variable "Forwarding Node Items" (see to Table 5) has six components meant to evaluate the variable's impact on blockchain and security. There should be two possible answers for every question. The assessment uses a scoring system that is dependent on the answers to the follow-up open-ended questions and a system that contains both closed- and open-ended questions.

The "Blockchain Security Service" variable also has six values. in order to determine the impact of the variable on Internet of Things (IoT) security (refer to Table 6). There should be two possible answers for every question. The assessment uses a scoring system that is dependent on the answers to the follow-up open-ended questions and a system that contains both closed- and open-ended questions.

Research population, and sampling

Research Population: The research population encompasses the entirety of the group that is the focus of the investigation. The population in question is expected to consist of persons, organizations, or entities who are engaged in or possess expertise in the field of blockchain-based systems for the management of IoT sensor data. The population of this current study comprise of "Developers and engineers who are engaged in the process of conceptualizing, creating, and executing blockchain-driven systems for the Internet of Things (IoT)". The other groups are "System Administrators who are professionals who are accountable for the upkeep and functioning of the blockchain-based system". The other group are "IoT Service Providers who are involve in organizations that offer services related to the Internet of Things (IoT) and make use of blockchain technology". Finally, "Researchers and academics who are individuals who contribute to the scholarly and scientific aspects of integrating blockchain with IoT".

Purposive sampling technique was selected in order to cover the wide range of individuals described above who are within the research population. This involves selectively choosing participants based on their proficiency in blockchain technology or their familiarity with IoT services. The process of determining the suitable sample size in purposive sampling requires finding a compromise between attaining a comprehensive understanding and taking into account practical factors[62]. Purposive sampling, in contrast to random sampling, does not rely on a precise statistical formula to determine the sample size. Instead, it is based on the researcher's judgment and seeks to select situations that provide rich and informative data[63].

Purposive sampling is commonly employed in qualitative research, wherein investigators deliberately choose participants based on the specific objectives of the study, with the anticipation that each individual will contribute distinct and useful insights. In this sampling strategy, the sample size is decided based on data saturation rather than statistical power analysis[63]. The objective is to attain a state of informational redundancy or theoretical saturation, guaranteeing that a sufficient amount of evidence is gathered to substantiate the study assertions. Determining the sample size in qualitative research involves making decisions based on judgment and experience, taking into account the research technique, purposeful sampling strategy, and intended study outcome. As a result, this research was able to come up with 32 respondents. This study employed purposive sampling to select 32 respondents who possess direct expertise in blockchain, IoT architecture, cybersecurity, or system administration. The selection was guided by the objective of obtaining domain-relevant insights rather than statistical generalizability.

Respondents were intentionally drawn from four stakeholder groups: (i) software developers and engineers, (ii) system/network administrators, (iii) IoT service providers, and (iv) academic researchers specializing in cybersecurity and blockchain. The sample size of 32 is consistent with methodological recommendations for expert-based evaluations, particularly in mixed-method studies involving structured surveys and architectural validation. Prior literature supports that 20–30 domain experts are sufficient to reach informational adequacy and generate meaningful trends for exploratory or formative assessments[62,63]. The representativeness in this context is ensured not through probabilistic sampling, but by ensuring heterogeneous expertise across roles that are operationally relevant to the framework being evaluated.

Data collection

Data collection is an essential stage in the research process when researchers acquire information to address their study questions or aims. The selection of data collection methods is contingent upon the research design, the characteristics of the study, and the specific type of data needed. The following activities were conducted during the process of data gathering.

1. Extensive dialogues between the researcher and the participant(s) to acquire comprehensive information.
2. Interview on open-ended questions to obtain extensive qualitative data.
3. The participant(s) evaluate their answers.

Presentation of the analytical results and discussion

The section presents the analytical results of the research. The solution includes an intermediary translation layer that functions as a protocol converter, facilitating smooth connection between various IoT devices and standardizing data formats prior to transmission via the blockchain network. In addition, smart contracts have

SD	*P*	TN	IN	FN	BS
4.0463	4.0815	4.6863	4.1320	4.3720	4.3891
4.0634	4.0987	4.7034	3.9720	3.9020	4.4063
4.0806	4.1158	4.7206	3.8120	3.4320	4.1149
4.0977	4.0080	4.7377	3.6520	4.2120	4.1320
3.9190	3.5380	3.9020	3.4920	4.0520	4.1491
3.4490	4.3180	3.4320	3.3320	4.0120	4.1663

Table 7. The blockchain-based system assessment.

SD	*P*	TN	IN	FN	BS
4.3901	4.6691	4.3890	4.4780	4.3720	4.0720
4.6691	4.6691	4.6691	4.6691	6.8070	4.0720
4.7160	6.1747	3.2520	2.2120	4.0120	4.6691
4.8390	6.4847	3.0920	4.6691	4.6691	4.6691
3.902	3.9201	4.542	3.919	4.008	3.902
3.432	3.4501	4.072	3.449	3.538	3.432

Table 8. Level of ensuring data integrity and accuracy.

the ability to dynamically understand and convert data in order to conform to the necessary formats at their intended destinations. The system employs middleware adapters to convert incoming data from various devices into a uniform format that is universally recognized by the blockchain network. Intelligent oracles verify the compliance of data, guaranteeing its compatibility with specified data destinations. In order to reduce latency, the system employs a hierarchical data processing strategy. First, edge computing performs filtration and preprocessing of incoming data in a local manner, hence decreasing the amount of data transmitted to the blockchain network. Simultaneously, load balancing algorithms in the blockchain efficiently distribute processed data, maximizing its delivery to destinations.

Table 7 display the result associated to the blockchain-based system Guarantees Internet of Things (IoT) Sensor Data Source Destination (SD): The mean values for IoT Sensor Data Source Destination constantly fall within the range of 3.4490 and 4.0977, suggesting an overall positive view of the dependability and safety of IoT sensor data sources and destinations. The Data Transmission Pattern (P) frequently exhibits high mean values ranging from 4.0080 to 4.3180, indicating a favorable perception of the techniques and patterns utilized for data transmission inside the Internet of Things (IoT) and blockchain framework.

The Transmission Node (TN) frequently demonstrates elevated mean values, ranging from 3.4320 to 4.7377, which suggests a favorable opinion of the transmission nodes' role and operation inside the blockchain-based system. The mean values of the Inspection Node (IN) range from 3.3320 to 4.1320. Although there may be some variation, respondents typically have a positive perception of inspection nodes when it comes to the integration of IoT and blockchain. Similarly, a value of within 3.9020 to 4.3720 on the transmission toward 4.1149 to 4.4063 was received.

The solution utilizes a hierarchical data aggregation approach to prioritize crucial data streams and implements parallel processing within the blockchain network. In addition, caching algorithms are employed at intermediary nodes to efficiently store and retrieve frequently accessed data, hence reducing latency for real-time data streams. The system predominantly uses a Publish-Subscribe paradigm for transmitting data. Internet of Things (IoT) devices transmit data to designated topics and subscribing nodes within the blockchain network receive pertinent information according to their subscriptions, guaranteeing precise data distribution. By utilizing a Mesh network design, Internet of Things (IoT) devices establish direct communication with neighboring nodes, creating several pathways for data transmission. The data is disseminated over the network using a flood-based methodology, guaranteeing duplication and dependability.

Table 8 presents the result on ensuring data integrity and accuracy. The standard deviation figures offer insights into the extent of variation in responses. Typically, the values remain constant in all observations, suggesting a moderate level of consensus among respondents. The probability (P) regularly exhibits high mean values, ranging from 3.4501 to 6.4847. The elevated results, particularly in observations 3 and 4, may suggest diverse interpretations or a dearth of agreement among the participants. The values of the Transmission Node (TN) range from 3.0920 to 4.6691. The variety indicates divergent viewpoints regarding the efficacy of transmission nodes in guaranteeing data integrity and accuracy.

The Inspection Node (IN) values span from 2.2120 to 4.6691. Observation 3 exhibits a significantly diminished value, suggesting a possible area of concern or divergent viewpoints regarding the function of inspection nodes. The values of the Forwarding Node (FN) demonstrate considerable variety, with observation 2 displaying a substantially higher value of 6.8070. This disparity indicates possible divergence among responders concerning the function of forwarding nodes.

SD	*P*	TN	IN	FN	BS
4.2015	4.8234	5.4540	7.7247	2.2920	4.7247
4.2187	4.8406	5.5770	8.0347	2.1320	5.0347
4.2358	4.8577	5.7000	8.3447	1.9720	5.3447
4.2530	4.8749	5.8230	8.6547	1.8120	5.6547
4.2701	4.8920	5.9460	8.9647	1.6520	5.9647
3.7601	4.3820	3.7590	3.8480	3.7420	4.3387

Table 9. Level of maintaining security protocols within the blockchain.

SD	*P*	TN	IN	FN	BS
4.2872	4.9091	6.0690	4.4147	1.4920	1.4147
4.3044	4.9263	6.1920	4.7247	1.3320	1.7247
4.3215	4.9434	6.3150	5.0347	1.1720	2.0347
4.3387	4.9606	6.4380	3.7420	1.0120	4.4147
4.3558	4.9777	6.5610	4.3720	0.8520	4.7247
4.3730	4.9949	6.6840	3.9020	0.6920	5.0347
4.3901	5.0120	6.8070	3.4320	0.5320	3.7420

Table 10. Blockchain architecture to safeguard IoT-generated data.

The range of values for the Blockchain Security Service (BS) is between 3.4320 and 4.6691. Like other variables, there is variability, indicating a range of perspectives regarding the efficacy of blockchain security services. The data indicates that respondents had various opinions on how helpful certain components are in maintaining the integrity and authenticity of data. The elevated probabilities observed in observations 3 and 4, along with the significant variability in other variables, emphasize the possibility of disagreement or divergent viewpoints among respondents.

Inspection nodes have a crucial function in data validation as they perform cryptographic checks and consensus verifications. The data hashes and timestamps are scrutinized to verify their adherence to specified rules established by smart contracts, thereby guaranteeing the integrity and authenticity of the blockchain.

Table 9 presented the finding associated to maintaining security protocols within the Blockchain. Standard Deviation numbers quantify the extent of variation in responses. The values exhibit uniformity among observations, indicating a moderate degree of concurrence among respondents. The probability (P) regularly exhibits high mean values, ranging from 4.3820 to 4.8920. These numbers indicate a favorable opinion of the likelihood factors related to upholding security procedures within the blockchain. The values of the Transmission Node (TN) continually grow, ranging from 3.7590 to 5.9460. The pattern indicates a growing favorable view of the efficacy of transmission nodes in upholding security procedures.

These findings suggest a favorable shift in respondents' perceptions of the efficacy of transmission nodes within the framework of blockchain architecture for protecting data created by the Internet of Things (IoT). The values of the Inspection Node (IN) continually increase, ranging from 3.4320 to 5.0347. This indicates a growing favorable view of the need of inspection nodes in protecting data generated by the Internet of Things (IoT) through the use of blockchain architecture. The values of the Forwarding Node (FN) continually decline, ranging from 0.5320 to 1.4920. Smaller numbers indicate a declining favorable impression of the function of forwarding nodes in protecting IoT-generated data through blockchain architecture. The Blockchain Security Service (BS) experiences a steady appreciation in value, fluctuating between 1.4147 and 5.0347 (see Table 10). This suggests a growing favorable view regarding the efficacy of blockchain security services in protecting data created by the Internet of Things (IoT). The research indicates a predominantly favorable impression of utilizing blockchain architecture to protect data created by the Internet of Things (IoT). The rising numbers for transmission nodes, inspection nodes, and blockchain security services suggest a favorable trend in respondents' perceptions of the efficacy of these elements. Nevertheless, the declining pattern in forwarding nodes indicates a possible area of worry or divergent viewpoints regarding their function in protecting data created by the Internet of Things (IoT).

The solution employs the method of data replication, whereby essential IoT data is repeated across numerous nodes inside the blockchain network. This redundancy guarantees that in the event of packet loss during transmission, the data can be recovered from alternate nodes, thereby minimizing the consequences of the loss. The system employs error correction codes and forward error correction algorithms to mitigate packet loss that may occur during transmission. Parity bits, also known as redundant information, are included in the data packets to enable automatic identification and rectification of errors upon receiving.

Table 11 indicates the finding indicate that privacy concerns while inspecting nodes verify. The standard seviation (SD) values exhibit a somewhat uniform pattern across observations, indicating a modest degree of concurrence among respondents. The range of probability (P) values is from 3.4501 to 4.2301. The findings suggest a moderate consensus among respondents considering the likelihood factors linked to privacy concerns during the examination of nodes for verification. The values of the Transmission Node (TN) range from 4.0720

SD	*P*	TN	IN	FN	BS
4.3720	3.9201	5.0120	5.0347	3.4847	4.2691
3.9020	3.4501	4.5420	5.3447	3.7947	4.2863
3.4320	4.2301	4.0720	5.6547	4.1047	4.3034
4.2120	4.0701	4.8520	5.9647	4.4147	4.3206
4.0520	4.0301	4.6920	4.6120	4.7247	4.3377
4.0120	4.0472	4.6520	4.4520	5.0347	4.3549
4.0291	4.0644	4.6691	4.2920	3.7420	4.3720

Table 11. Privacy concerns while inspecting nodes verify.

SD	*P*	TN	IN	FN	BS
4.2290	4.1580	4.2120	3.1720	3.7420	4.1834
4.0690	4.6247	4.0520	3.0120	4.3720	4.2006
4.2240	4.9347	3.8920	2.8520	3.9020	4.2177
4.3470	5.2447	3.7320	2.6920	3.4320	4.2349
4.4700	5.5547	3.5720	2.5320	4.2120	4.2520
4.5930	5.8647	3.4120	2.3720	4.0520	3.7420

Table 12. Handle discrepancies or inconsistencies.

to 5.0120. This indicates a moderate consensus among participants regarding the efficacy of transmission nodes in addressing privacy issues during the verification procedure. The values of the Inspection Node (IN) constantly grow, ranging from 4.2920 to 5.9647. There is a growing consensus among respondents about privacy concerns when examining nodes for verification.

The values of the Forwarding Node (FN) range from 3.4847 to 5.0347. This indicates a moderate consensus among participants regarding the involvement of forwarding nodes in addressing privacy issues throughout the verification procedure. The range of values for the Blockchain Security Service (BS) is from 4.2691 to 4.3720. The values suggest a moderate consensus among respondents regarding the efficacy of blockchain security services in addressing privacy concerns during the verification process. The data indicates a moderate amount of consensus among respondents considering privacy concerns while examining nodes for verification. The rising numbers for inspection nodes signify a greater consensus on the significance of this element in addressing privacy concerns during the verification process.

The prioritization is based on the type of data, its urgency, and the conditions of the network, which allows for effective management of data traffic among transmission nodes. Table 12 indicate the finding associated to handling discrepancies or inconsistencies. The standard seviation (SD) values exhibit a pretty uniform pattern across observations, indicating a reasonable degree of consensus among responders. The range of probability (P) values is from 4.1580 to 5.8647. The results suggest a substantial consensus among respondents regarding the likelihood factors related to managing discrepancies or inconsistencies. Overall Perception: The average scores suggest a moderate to high level of perception across many factors associated with IoT and blockchain.

The data transmission pattern is perceived to be higher by respondents compared to other characteristics. The mean values of IoT Sensor Data Source (S), Forwarding Node (FN), and Blockchain Security Service (BSS) are similar, indicating a consistent view across these elements. This implies a rather good attitude, indicating that respondents usually have a favorable assessment of the dependability and safety of data sources from IoT devices. IoT Sensor Data Destination (D): The average value for IoT sensor data destinations is 3.8602, which closely corresponds to the perception of data sources. Respondents consistently maintain a coherent perspective on both the origin and destination aspects of data created by the Internet of Things (IoT).

The data transmission pattern (P) has the greatest mean value of 4.452. Respondents have shown a relatively greater level of positive impression towards the methods and patterns used to transmit data within the IoT and blockchain framework. The mean values of the Transmission Node (TN) and Inspection Node (IN) are 3.859 and 3.948, respectively. These numbers indicate favorable perceptions, albeit they are not as elevated as the data transmission pattern. Respondents generally have a positive perception of the capabilities of transmission and inspection nodes. The Forwarding Node (FN) variable, with a mean value of 3.842, closely corresponds to the IoT sensor data source and destination, suggesting a consistent view across these features. Respondents consider forwarding nodes to be essential components in the architecture of the Internet of Things (IoT) and blockchain.

Blockchain Security Service (BSS): The average rating for blockchain security services is 3.842, reflecting the opinions of IoT sensor data sources and forwarding nodes (see Fig. 2). These findings indicate that the participants view blockchain security services as equally significant and dependable. The respondents usually have favorable attitudes of the integration of IoT and blockchain across many dimensions. A higher mean value for data transmission pattern signifies a specific inclination or assurance in the effectiveness and dependability of data transmission techniques. The uniformity in average values across all categories suggests a consistent and well-balanced understanding among respondents on the essential elements of IoT and blockchain systems. This

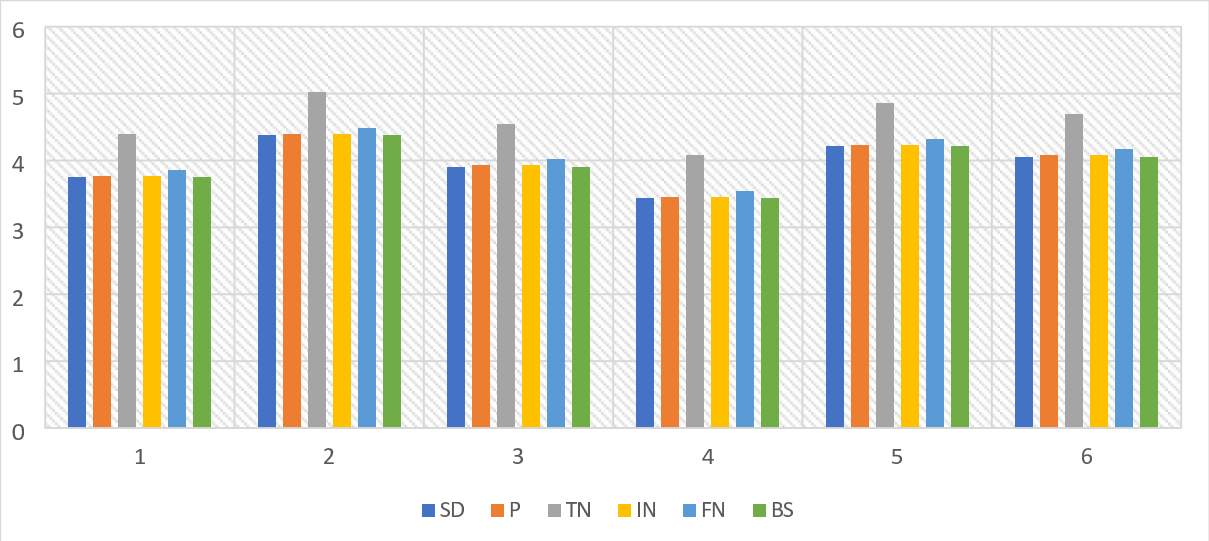

Fig. 2. The overall blockchain security service perceptions.

study offers useful insights into the diverse viewpoints of those who possess expertise in blockchain technology or have firsthand experience with IoT services. Subsequent studies should further investigate the precise aspects that contribute to these impressions and examine new avenues for enhancing the integration of IoT and blockchain technology.

Implication of the study findings

The study demonstrates that participants hold a favorable opinion regarding the security and dependability of the blockchain-based system for overseeing data generated by the Internet of Things (IoT). This indicates an increasing belief in the capability of blockchain technology to tackle security issues in IoT services. The declining trend in scores associated with Inspection Nodes suggests a potential topic of concern or divergent viewpoints among participants. Comprehending and resolving these difficulties are vital to guaranteeing the efficient incorporation of inspection nodes into the blockchain framework. Participants typically concur on the function of Forwarding Nodes in managing discrepancies or inconsistencies. This modest consensus indicates a certain degree of assurance in the efficacy of forwarding nodes in the blockchain-based system. The study highlights potential areas for enhancement in particular elements, such as Inspection Nodes. To improve the overall effectiveness of the system, it is important to address these areas by implementing specific interventions or enhancements based on participant feedback.

The favorable ratings for Blockchain Security Service suggest that it is considered very successful in protecting data created by the Internet of Things (IoT). This highlights the significance of strong security mechanisms in the blockchain framework to guarantee the reliability and privacy of data. The consequences necessitate additional research, such as conducting in-depth interviews or focus group discussions, to investigate the underlying factors contributing to differing impressions. It is advisable to provide focused interventions based on feedback from participants in order to address concerns and improve certain components. The findings obtained from this study establish a basis for future progress and enhancements in the incorporation of blockchain technology in IoT services. Continuing this discussion is essential for keeping up with rising difficulties and possibilities in this developing area. The study's findings emphasize the favorable perceptions and areas of enhancement in the blockchain-based system used to manage data created by the Internet of Things (IoT). Tackling these consequences can aid in the ongoing advancement and refinement of blockchain technology within the framework of Internet of Things applications.

The thorough examination of the survey responses from the participants yields significant information into multiple facets of the blockchain-based system for overseeing data created by the Internet of Things (IoT). The study examined key elements like IoT Sensor Data Source and Destination (SD), Data Transmission Pattern (P), Transmission Node (TN), Inspection Node (IN), Forwarding Node (FN), and Blockchain Security Service (BS). The participants' perceptions were assessed using a scale that ranged from 1 to 5 for these components. The participants consistently conveyed a favorable perspective on the probabilistic elements linked to the utilization of blockchain architecture, with average values ranging from 4.1580 to 5.8647. This indicates a strong level of assurance in the efficacy of blockchain technology.

The Transmission Node (TN) continuously obtained high scores, showing a positive opinion of its effectiveness. However, the Inspection Node (IN) exhibited a declining tendency. This indicates a possible area of concern or conflicting viewpoints regarding the function of inspection nodes inside the system. The respondents reached a consensus regarding the function of Forwarding Nodes (FN) in addressing discrepancies or inconsistencies, with average values ranging from 3.4320 to 4.3720. There appears to be a moderate level of agreement regarding the usefulness of forwarding nodes. The Blockchain Security Service (BS) earned predominantly favorable

ratings, suggesting a perceived efficacy in protecting data generated by the Internet of Things (IoT). The mean values varied between 3.7420 and 5.0347. The findings underscore the participants' assurance in the security and dependability of the system based on blockchain technology. Nevertheless, the differing viewpoints of some elements, namely Inspection Nodes, suggest the necessity for additional scrutiny and potential enhancements in these domains.

The thorough examination of the survey responses from the participants yields significant information into multiple facets of the blockchain-based system for overseeing data created by the Internet of Things (IoT). The study examined essential elements like IoT Sensor Data Source and Destination (SD), Data Transmission Pattern (P), Transmission Node (TN), Inspection Node (IN), Forwarding Node (FN), and Blockchain Security Service (BS). The participants' perceptions were assessed using a scale that ranged from 1 to 5 for these components. The participants consistently displayed a favorable perspective regarding the probability factors linked to the utilization of blockchain architecture, with mean values ranging from 4.1580 to 5.8647. This indicates a significant degree of assurance in the efficacy of blockchain technology.

The Transmission Node (TN) regularly obtained high scores, showing a positive opinion of its effectiveness. However, the Inspection Node (IN) displayed a declining trend. This indicates a possible issue or conflicting viewpoints regarding the function of inspection nodes in the system. The respondents reached a consensus regarding the function of Forwarding Nodes (FN) in addressing discrepancies or inconsistencies, with average values ranging from 3.4320 to 4.3720. This indicates a moderate degree of agreement regarding the efficacy of forwarding nodes. The Blockchain Security Service (BS) earned predominantly favorable ratings, suggesting a perceived efficacy in protecting data generated by the Internet of Things (IoT). The mean values varied between 3.7420 and 5.0347.

The results emphasize the participants' trust in the security and dependability of the system based on blockchain technology. Nevertheless, the divergent viewpoints regarding specific elements, namely Inspection Nodes, suggest the necessity for additional scrutiny and possible enhancements in these domains. To obtain qualitative insights and delve into participants' thoughts, particularly about Inspection Nodes, it is recommended to conduct thorough interviews or engage in focus group discussions. Execute focused interventions or improvements according to participant feedback to tackle concerns and boost the perceived efficacy of specific elements. Broaden the scope of the research to encompass a wider and more varied group of participants in order to guarantee a thorough comprehension of numerous viewpoints. While the purposive sampling of 32 domain experts provided rich and targeted insights into the architectural and performance aspects of the proposed framework, it also introduces a limitation in terms of generalizability. The findings reflect expert opinion within a specific context and do not represent the broader population of IoT or blockchain users. As such, the conclusions drawn are best interpreted as exploratory and formative. Future studies may consider using larger, probabilistically selected samples, or cross-sector evaluations, along with inferential statistical analysis to test relationships and generalize findings across wider operational contexts.

Conclusions

This study addressed the challenge of secure data transmission within Internet of Things (IoT) environments by proposing and evaluating a blockchain-based architectural framework. The framework comprises functional components such as Transmission Nodes, Inspection Nodes, Forwarding Nodes, and a Blockchain Security Service to ensure the authenticity, integrity, and confidentiality of sensor data across the IoT network. Through a mixed-method approach incorporating expert evaluations, we identified that while components like the Blockchain Security Service and Transmission Nodes were perceived as highly effective in securing and managing IoT data, elements such as Inspection Nodes showed variability in perception—highlighting opportunities for improvement. By integrating subjective evaluation, the study bridges the gap between theoretical blockchain-IoT models and real-world operational expectations. The contributions of this work lie in its architectural granularity, its case-based validation strategy, and its user-informed assessment model. This positions the research as a novel and practical advancement toward designing scalable, decentralized, and secure IoT transmission systems. Aligned with the title and abstract, this study contributes to the growing literature on blockchain-enabled IoT infrastructures and serves as a foundation for future improvements in transmission security, system design, and performance benchmarking in smart environments.

Data availability

The datasets generated and/or analysed during the current study are not publicly available due the fact that they are direct responses from respondents on Items from Tables 1, 2, 3, 4, 5 and 6, but are available from the corresponding author on reasonable request.

Received: 2 April 2025; Accepted: 4 September 2025
Published online: 29 September 2025

References

1. Javadpour, A. et al. Encryption as a service for iot: opportunities, challenges and solutions. *IEEE Internet Things J.* (2023).
2. Soori, M., Arezoo, B. & Dastres, R. Internet of things for smart factories in industry 4.0, a review. *Internet Things Cyber-Phys. Syst.* (2023).
3. Motlagh, N. H., Zaidan, M. A., Morabito, R., Nurmi, P. & Tarkoma, S. Towards large-scale IoT deployments in smart cities: Requirements and challenges. In *Learning Techniques for the Internet of Things*. (Springer, 2024).
4. Mannayee, V. & Ramanathan, T. An efficient SDFRM security system for blockchain based internet of things. *Intell. Autom. Soft Comput.* **35**(2). (2023).

5. Abdullah, A. et al. Data security in healthcare industrial internet of things with blockchain. *IEEE Sens. J.* https://doi.org/10.1109/jsen.2023.3273851 (2023).
6. Zhang, R., Xu, C. & Xie, M. Secure decentralized IoT service platform using consortium blockchain. *Sensors* **22** (21), 8186 (2022).
7. Kavitha, K. K. & Sathis, S. Healthcare internet of things (HIoT) data security enhancement using blockchain technology. *J. Intell. Fuzzy Syst.* https://doi.org/10.3233/jifs-220797 (2022).
8. Arvind, K. S. S. & Vanitha, K. S. Suganya pandemic management using internet of things and big data: A security and privacy perspective. (2022). https://doi.org/10.1201/9781003217404-8
9. Chunpeng, G., Zhe, L. & Fang, L. A blockchain based decentralized data security mechanism for the internet of things. *J. Parallel Distrib. Comput.* https://doi.org/10.1016/J.JPDC.2020.03.005 (2020).
10. Abdullah, A. Blockchain-based information sharing security for the internet of things. *Mathematics*. https://doi.org/10.3390/math11092157 (2023).
11. Jinghan, L. & Yang, Y. Communication mechanism of internet of things based on blockchain. https://doi.org/10.1117/12.2636584 (2022).
12. Huiting, Y., Bai, Y., Zhenwan, Z., Qiang, Z. & Bin, W. Research on data security sharing mechanism of power internet of things based on blockchain. https://doi.org/10.1109/ITAIC49862.2020.9338843 (2020).
13. Sureshkumar, M. Blockchain based security system for the devices in internet of things. https://doi.org/10.1109/ICCCI48352.2020.9104092 (2020).
14. Khan, A. A. et al. BDLT-IoMT: A novel architecture—SVM machine learning for robust and secure data processing in internet of medical things with blockchain cybersecurity. *J. Supercomput.* **81** (1), 1–22 (2025).
15. Khan, A. A. et al. BAIoT-EMS: consortium network for small-medium enterprises management system with blockchain and augmented intelligence of things. *Eng. Appl. Artif. Intell.* **141**, 109838 (2025).
16. Khan, A. A. et al. Artificial intelligence, internet of things, and blockchain empowering future vehicular developments: A comprehensive multi-hierarchical lifecycle review.(2025).
17. Khan, A. A., Laghari, A. A., Inam, S. A., Ullah, S. & Nadeem, L. A review on artificial intelligence thermal fluids and the integration of energy conservation with blockchain technology. *Discov. Sustain.* **6** (1), 1–18 (2025).
18. Khan, A. A. et al. B-LPoET: A middleware lightweight Proof-of-Elapsed time (PoET) for efficient distributed transaction execution and security on blockchain using multithreading technology. *Comput. Electr. Eng.* **118**, 109343 (2024).
19. Khan, A. A. et al. Secure remote sensing data with blockchain distributed Ledger technology: A solution for smart cities. *IEEE Access.* (2024).
20. Khan, A. A. et al. ORAN-B5G: A next generation open radio access network architecture with machine learning for beyond 5G in industrial 5.0. *IEEE Trans. Green. Commun. Netw.* (2024).
21. Luqman, M. & Faridi, A. R. Internet of things security: a blockchain perspective. In *Smart Trends in Computing and Communications: Proceedings of SmartCom*, 577–587 (Springer Nature Singapore, 2022).
22. Okegbile, S. D., Cai, J. & Alfa, A. S. Performance analysis of blockchain-enabled data-sharing scheme in cloud-edge computing-based IoT networks. *IEEE Internet Things J.* **9** (21), 21520–21536 (2022).
23. Xue, H., Chen, D., Zhang, N., Dai, H. N. & Yu, K. Integration of blockchain and edge computing in internet of things: A survey. *Future Gener. Comput. Syst.* **144**, 307–326 (2023).
24. Shang, J., Guan, R. & Tong, Y. Microgrid data security sharing method based on blockchain under internet of things architecture. *Wirel. Commun. Mob. Comput.* **2022**. (2022).
25. El Majdoubi, D., El Bakkali, H. & Sadki, S. SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework. *J. Healthc. Eng.* **2021** (2021).
26. Ngabo, D. et al. Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *Electronics*. **10** (17), 2110 (2021).
27. Abbas, A. et al. Blockchain-assisted secured data management framework for health information analysis based on internet of medical things. *Pers. Ubiq. Comput.* **19**, 1–4 (2021).
28. Dwivedi, S. K., Roy, P., Karda, C., Agrawal, S. & Amin, R. Blockchain-based internet of things and industrial iot: A comprehensive survey. *Secur. Commun. Netw.*. **2021**, 1–21 (2021).
29. Uppal, S., Kansekar, B., Meher, P., Mini, S. & Tosh, D. CareBlocks: A blockchain-based health information sharing framework for medical IoT. In *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)*, 928–933 (IEEE, 2021).
30. Wei, Z. & Wang, F. *Detecting Anomaly Data for IoT Sensor Networks* (Scientific Programming, 2022).
31. Rstoceanu, F., Rughini, R., Ciocrlan, D. & Enache, M. Sensor-based entropy source analysis and validation for use in IoT environments. *Electronics*. **10** (10), 1173 (2021).
32. Huang, S. Z. & Chen, R. Q. FPGA-based IoT sensor HUB. In *International Conference on Sensor Networks and Signal Processing (SNSP)*, 139–144 (IEEE, 2018).
33. Nguyen, T., Phan, Q. B. & Bui, N. T. High-secure data collection in IoT sensor networks using homomorphic encryption. In *Sensors and Systems for Space Applications XVI*, vol. 12546, 53–60 (SPIE, 2023).
34. Dinca, L. M. & Hancke, G. Behavioural sensor data as randomness source for IoT devices. In *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*, 2038–2043 (IEEE, 2017).
35. Nguyen, L. A., Kiet, P. T., Lee, S., Yeo, H. & Son, Y. Comprehensive survey of sensor data verification in internet of things. *IEEE Access.* (2023).
36. Zualkernan, I., Ahmed, N., Elmeligy, A., Abdelnaby, A. & Sheta, N. IoT sensor data consistency using deep learning. In *2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 198–203 (IEEE, 2022).
37. Krishnamurthi, R., Kumar, A., Gopinathan, D., Nayyar, A. & Qureshi, B. An overview of IoT sensor data processing, fusion, and analysis techniques. *Sensors* **20** (21), 6076 (2020).
38. Aparna, R., Mallick, A. K. & Sahay, U. Securing Sensor Data on Internet of Things (IoT) Devices. In *Proceedings of the International Conference on Cognitive and Intelligent Computing: ICCIC 2021*, vol. 1, 411–419 (Springer Nature Singapore, 2022).
39. Han, J., Lee, G. H., Park, H. & Choi, J. K. Data accuracy pattern-based transmission period control algorithm for IoT networks. In *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 668–673 (IEEE, 2023).
40. Chang, S. Y. & Wu, H. C. Packetless data transmission through pattern exclusive coding. *Phys. Commun.*. **41**, 101108 (2020).
41. Yang, N. Relay transmission method and relay node. European Patent Application published in accordance with Art. 153(4) EPC. (2020).
42. Zhang, N., Tian, L., Yuan, Z. & Cao, W. inventors; ZTE corp, assignee. Multiple access transmission configurations. United States patent application US 17/169,121 (2021).
43. Zomaya, A., Jeong, H. Y. & Obaidat, M. In *Frontier and Innovation in Future Computing and Communications*. 18 (eds Park, J. J.) (Springer, 2014).
44. Shukla, S., Hassan, M. F., Khan, M. K., Jung, L. T. & Awang, A. An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment. *PLoS One.* **14** (11), e0224934 (2019).
45. In-Seon, Y. O. inventor; Samsung SDS Co Ltd, assignee. Data packet transmission method, data packet authentication method, and server thereof. United States patent US 10,581,849. (2020).
46. Nkongolo, M., van Deventer, J. P. & Kasongo, S. M. Using deep packet inspection data to examine subscribers on the network. *Proc. Comput. Sci.* **215**, 182–191 (2022).

47. Ganesh, P. et al. Implementation of hidden node detection scheme for self-organization of data packet. *Wirel. Commun. Mob. Comput.* **2022**, 1–9 (2022).
48. Nkongolo, M., van Deventer, J. P., Kasongo, S. M. & van der Walt, W. Classifying social media using deep packet inspection data. In *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2022*, 543–557 (Springer Nature Singapore, 2022).
49. Mubarakali, A. et al. Fog-based delay-sensitive data transmission algorithm for data forwarding and storage in cloud environment for multimedia applications. *Big Data*. **11** (2), 128–136 (2023).
50. He, X. inventor; Huawei technologies Co ltd, assignee. Data or packet forwarding method, node, and system. United States patent application US 17/343,828 (2021).
51. Krossoy, F. & Braun, R. inventors; ABB Schweiz AG, assignee. Aggregating server and method for forwarding node data. United States patent application US 17/495,838 (2022).
52. Mahajan, S. & Malhotra, J. Energy efficient path determination in wireless sensor network using BFS approach. *Wirel. Sens. Netw.* **3** (11), 351 (2011).
53. Shaofu, P. E. & Feicai, J. I. inventors; ZTE corp, assignee. Message forwarding method and apparatus, and node. United States patent application US 17/106,066 (2021).
54. Geetha, S. K., Naveenkumaran, R., Selvaraju, K., Kishore, C. & Rathish, A. N. Blockchain based mechanism for cloud security. In *International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, 1287–1295 (IEEE, 2023).
55. Ahmmed, M. R. et al. Encryption process of Blockchain based online course curriculum education system. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, 1–7 (IEEE, 2023).
56. Alsudani, M. Q. et al. Blockchain-Based E-Medical record and data security service management based on IoMT resource. *Int. J. Pattern Recognit. Artif. Intell.* **37** (06), 2357001 (2023).
57. Pon, P. Blockchain based cloud service security architecture with distributed machine learning for smart device traffic record transaction. *Concurr. Comput. Pract. Exp*. **34** (3), e683 (2022).
58. Hewa, T., Braeken, A., Liyanage, M. & Ylianttila, M. Fog computing and blockchain-based security service architecture for 5G industrial IoT-enabled cloud manufacturing. *IEEE Trans. Industr. Inf.* **18** (10), 7174–7185 (2022).
59. Yusoff, M. S., Arifin, W. N. & Hadie, S. N. ABC of questionnaire development and validation for survey research. *Educ. Med. J.* ;**13**(1). (2021).
60. Barroga, E. & Matanguihan, G. J. A practical guide to writing quantitative and qualitative research questions and hypotheses in scholarly articles. *J. Korean Med. Sci.* **37**(16). (2022).
61. GonzÃ¡lez-Alzaga, B. et al. The questionnaire design process in the European human biomonitoring initiative (HBM4EU). *Environ. Int.* **160**, 107071 (2022).
62. Chatterjee, S. & Diaconis, P. The sample size required in importance sampling. *Ann. Appl. Probab.* **28** (2), 1099–1135 (2018).
63. Hirose, M. & Creswell, J. W. Applying core quality criteria of mixed methods research to an empirical study. *J. Mixed Methods Res.* **17** (1), 12–28 (2023).

Acknowledgements

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. (UJ-24-DR-20746-1). Therefore, the authors thank the University of Jeddah for its technical and financial support.

Author contributions

Conceptualization, A.A.; Data curation, A.I. and A.A.; Formal analysis, A.A. and A.A.; Funding acquisition, A.A.; Methodology, A.A.; Project administration, A.A.; Resources, A.I.; Software, A.A. and A.A.; Validation, A.A. and A.A.; Visualization, A.A.; Writing-original draft, A.A. and A.A.; Writing-review and editing, A.I.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to A.A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.