INTERNATIONAL JOURNAL OF BUSINESS AND MANAGEMENT (IJBM)
ISSN: 2815-9330 (Online)

VOL. 5, NO. 1 2026 https://iessociety.org/

A permissioned blockchain framework for decentralised trust, secure communication, and auditability in resource-constrained IoT networks

Sumaiya M. Shaikh[1], Sonu Dalal[2], Shailak Jani[3*], and Anju Gakhar[4]

[1 2 3]Parul University, Vadodara, Gujarat India

[4]Sanskaram University, Jhajjar,Haryana India

[1]Email: sumaiya.profession@gmail.com; [2]sonu.dalal36781@paruluniversity.ac.in; [4]hod.mgmt@sanskaramuniversity.ac.in;

ORCID: [1]0009-0000-4200-3187; [2]0009-0009-2085-2749; [4]0009-0000-6300-826X

*Correspondence: 93janisra@gmail.com; ORCID: 0000-0002-7270-7916

Abstract

The rapid proliferation of Internet of Things (IoT) devices intensifies longstanding security challenges in resource-constrained communication networks, where conventional centralised architectures introduce single points of failure, limited scalability, and inadequate auditability. This paper proposes a permissioned blockchain-enabled secure communication framework that integrates smart-contract-driven authentication and authorisation with lightweight cryptographic mechanisms to enable decentralised trust, data integrity, and fine-grained access control across heterogeneous IoT environments. The framework defines an end-to-end secure communication workflow encompassing device registration, authentication, authorisation, encrypted data transmission, and immutable audit logging. Analytical evaluation demonstrates low communication and computational overhead, linear scalability with network size, and resistance to common attack vectors including unauthorised access, replay attacks, and man-in-the-middle threats. Comparative analysis against existing blockchain-based IoT security frameworks highlights the proposed solution's advantages in decentralisation, auditability, and suitability for devices with constrained resources. Although experimental validation remains a direction for future work, the framework provides a rigorous conceptual and analytical foundation for next-generation IoT communication architectures applicable to smart cities, industrial automation, and healthcare monitoring.

***Keywords*:** Internet of Things (IoT), Security, Permissioned Blockchain, Smart Contracts, Lightweight Cryptography, Decentralised Access Control, Threat Modelling, Immutable Audit Logging, Scalable Authentication

JEL Classification: O33, L86, D85, C63

DOI: https://doi.org/10.56879/ijbm.v5i1.24

1. Introduction

The Internet of Things (IoT) has emerged as one of the defining technological paradigms of the twenty-first century, enabling the seamless interconnection of billions of heterogeneous devices across domains as varied as smart cities, industrial automation, healthcare monitoring, and intelligent transportation systems. Since the term was first popularised in the early 2000s, the global IoT device base has grown from niche industrial applications to a projected tens of billions of connected endpoints, fundamentally transforming how data is collected, processed, and acted upon at scale (Atzori et al., 2010; Al-Fuqaha et al., 2015). Yet this rapid proliferation has consistently outpaced the development of adequate security infrastructure, creating an expanding attack surface that threatens the integrity, confidentiality, and availability of IoT-generated data. The security challenges inherent to IoT communication networks are compounded by several structural characteristics of the environment. IoT devices are typically resource-constrained, limited in processing power, memory, and energy capacity, which renders computationally intensive cryptographic protocols impractical at the device level. At the same time, IoT networks are highly heterogeneous, encompassing sensors, actuators, and smart objects operating across diverse communication protocols and network topologies. The volume and velocity of data exchange in large-scale deployments further strain conventional security architectures (Conti et al., 2018; Sicari et al., 2015). The dominant approach to IoT security has historically relied on centralised models of authentication, access control, and data management. While such models offer operational simplicity in small deployments, they introduce critical vulnerabilities at scale: a single point of failure can compromise entire networks, performance degrades as device counts grow, and centralised trust repositories are high-value targets for adversaries (Sicari et al., 2015; Ammar et al., 2018). Moreover, centralised logs are susceptible to tampering, undermining the forensic auditability that is increasingly required in regulated IoT applications such as healthcare and critical infrastructure.

Blockchain technology has attracted significant research interest as a structural response to these limitations. Through distributed ledgers and consensus mechanisms, blockchain enables tamper-resistant data storage and decentralised authentication without reliance on a trusted central authority (Nakamoto, 2008; Christidis & Devetsikiotis, 2016). Permissioned blockchain variants, such as Hyperledger Fabric, are particularly suited to IoT contexts, as they support controlled participation, low-latency consensus, and deterministic transaction finality without the prohibitive computational cost of proof-of-work systems (Androulaki et al., 2018). Smart contracts extend this architecture by enabling automated, code-enforced security policies, reducing both human error and operational overhead in authentication and authorisation workflows (Dorri et al., 2017). However, directly integrating blockchain into IoT systems is not without challenges. Consensus operations, ledger storage, and on-chain data management can introduce latency and resource overhead that are incompatible with the constraints of IoT devices, particularly in real-time or ultra-low-power settings (Yang et al., 2019). Critically, most existing blockchain-based IoT

DOI: https://doi.org/10.56879/ijbm.v5i1.24

security frameworks address either access control or data integrity in isolation; few present an integrated, end-to-end secure communication workflow that simultaneously addresses registration, authentication, authorisation, encrypted transmission, and audit logging in a resource-aware manner (Makhdoom et al., 2019).

This paper addresses that gap by proposing a permissioned blockchain-enabled secure communication framework for IoT networks. The framework combines smart-contract-driven authentication and authorisation with lightweight cryptographic mechanisms — symmetric encryption, hash-based message authentication, and selective use of public-key operations — to achieve decentralised trust, data integrity, and scalable access control without placing undue computational burden on constrained devices. An analytical evaluation demonstrates low communication and computational overhead, and the framework is assessed against representative threat vectors including replay attacks, man-in-the-middle attacks, and unauthorised access. The main contributions of this paper are as follows: (i) a permissioned blockchain architecture tailored to the resource and latency constraints of IoT communication networks; (ii) a smart-contract-based security automation layer governing device registration, authentication, authorisation, and audit logging; (iii) integration of lightweight cryptographic protocols that minimise device-level overhead while preserving communication security guarantees; and (iv) an analytical performance and security evaluation, including comparative analysis against existing blockchain-based IoT security frameworks.

The remainder of this paper is organised as follows. Section 2 reviews relevant literature on IoT security, lightweight cryptography, and blockchain-based trust management. Section 3 presents the system model and problem definition. Section 4 describes the proposed framework architecture and its core components. Section 5 details the secure communication workflow. Section 6 provides analytical performance evaluation. Section 7 offers a comparative discussion. Section 8 concludes the paper and outlines directions for future work.

2. Literature Review

The Internet of Things (IoT) communication networks security has received broad research attention because of the growing use of resource-constrained devices in heterogeneous and large-scale networks. Initial studies mostly centred on centralised security systems, wherein authentication, authorization and key management are done by a third party or cloud server who is trusted. Although these solutions make managing them easier, they add single points of failure and scalability constraints, and are not suitable in large IoT ecosystems (Roman et al., 2013; Ammar et al., 2018). A number of works have been conducted on lightweight cryptography to implement resource-constrained devices in the IoT. To eliminate computational and energy overhead, solutions, depending on symmetric encryptions, hash-based authentication, and lightweight key exchange protocols, have been suggested (Perrig et al., 2002; He et al., 2016). Nevertheless, such solutions continue to be heavily centralised in trust models and do not typically

DOI: https://doi.org/10.56879/ijbm.v5i1.24

perform well against insider attacks and massive compromise. In order to address the centralised trust concerns, blockchain-based IoT security solutions have become popular. One of the earliest to discuss the possibility of blockchain and smart contracts to support decentralised trust and automation in IoT systems was Christidis and Devetsikiotis (2016). A lightweight IoT blockchain architecture suggested by Dorri et al. (2017) has less storage and processing requirements since they are delegated to other more powerful nodes. Even though they work, their solution has its own issues with scalability and the speed of transactions.

Still more up-to-date research has been concerned with secure communication and access control with blockchain. According to Zhang et al. (2011), a blockchain-based access control model was suggested to guarantee the integrity of data and decentralised authentication in IoT. In the same manner, Novo (2018) proposed an access management system, based on blockchain and scaled to distributed internet of things networks. Though these solutions enhance the management of trust, they do not consider the workflow of communication details, and the lightweight cryptographic integration of small devices. Blockchain coupled with edge or fog computing has been used by other researchers to minimise latency and computational loads. Xu et al. (2019) have shown that edge-assisted blockchain architectures can enhance the performance in the use of blockchain in the security of the IoT. Nonetheless, these hybrid solutions add complexity and expense to the system deployment, and this could make them less applicable in practise. Nevertheless, even with these developments, the available blockchain-based solutions to IoT security may have poor analytical assessment, a deficiency in discussing communication overhead, or an absence of explicitly defined threat modelling. In addition, lots of frameworks concentrate on either security or scale but hardly on the secure communication, decentralised trust and resource efficiency at the same time. This paper provides a secure communication architecture based on blockchain with support of authentication based on smart-contracts, lightweight cryptography, and analytical performance and security analysis. The research gaps will be filled with the proposed approach that will offer a well-balanced and practical solution to the identified gaps that fits into a real-world IoT communication network.

3. System Model and Problem Definition

The data science platform and data analytics infrastructure research is across various topics, such as information systems, data engineering, artificial intelligence, and digital transformation. The previous research can be classified into three broad thematic streams which include: (i) platform capabilities and analytics infrastructure, (ii) data governance and lifecycle management and (iii) business value and organisational impact of analytics.

3.1 IoT Communication Architecture

The environment being considered is the IoT communication environment with a huge number of heterogeneous and resource-constrained IoT devices, including sensors, actuators, and smart objects, which are connected to a wireless or wired network. These gadgets are normally arranged

DOI: https://doi.org/10.56879/ijbm.v5i1.24

in a multi-layer structure entailing the IoT devices, the gateway or edge node, and the cloud or application server (Al-Fuqaha et al., 2015; Bonomi et al., 2012). IoT devices produce data that are sent to the gateways or edge nodes to be aggregated and sent to the backend services. Traditional architectures are characterised by central servers that perform authentication, access control, and data management, which creates the dependency of trust and other scaling issues (Sicari et al., 2015). IoT networks are susceptible to all sorts of cyber-attacks as communication between devices and servers usually traverses unsecured paths.

3.2 Threat Model

The suggested framework takes into consideration a realistic and popular threat model of the IoT communication networks. Adversaries are assumed to be able to eavesdrop on communication channels, introduce malicious packets, reuse already received messages, or to make illegal access to IoT services (Conti et al., 2016). The use of weak physical protection or less power may also put individual IoT devices at risk by being compromised by attackers. The threats explicitly taken into account include Unauthorized Access, Malicious actors trying to get into the IoT resources by bypassing authentication Data Tampering, Replay Attacks, Man-in-the-Middle Attacks, and Single Point of Failure (Sicari et al., 2015).

3.3 Problem Definition

Although there has been a significant amount of research, the current IoT security solutions are still highly dependent on centralised models of trust which do not well suit large scale and dynamic IoT systems. The centralised architectures have poor scalability, susceptibility to specific attacks as well as lack of trust management transparency (Ammar et al., 2018; Roman et al., 2018). In addition, IoT devices have limited resources, which limit the implementation of heavy cryptographic controls, meaning that they can only authenticate weakly and can offer little protection against data integrity attacks (Perrig et al., 2002). Thus, the main issue covered by this research can be stated as: How to develop a scalable, decentralized, and secure communication framework for IoT networks that can be trusted, authenticated, and maintain the integrity of the data and at the same time be appropriate for resource-constrained devices.

3.4 Design Objectives

In order to deal with the outlined challenges, the given framework is created with the following goals in mind: (i) Decentralized Trust Management: Distributed ledger technology will remove the need to have a single trusted authority. (ii) Secure Communication: Provide confidentiality, integrity, and authenticity of the IoT data transmissions. (iii) Secure Communication: Be able to support more and more IoT devices without any drastic changes in performance. (iv) Scalability (v) Lightweight Operation: Reduce the computational and storage requirements to fit the limited IoT devices. (vi) Automation: Implementing smart contracts to provide authentication and access control.

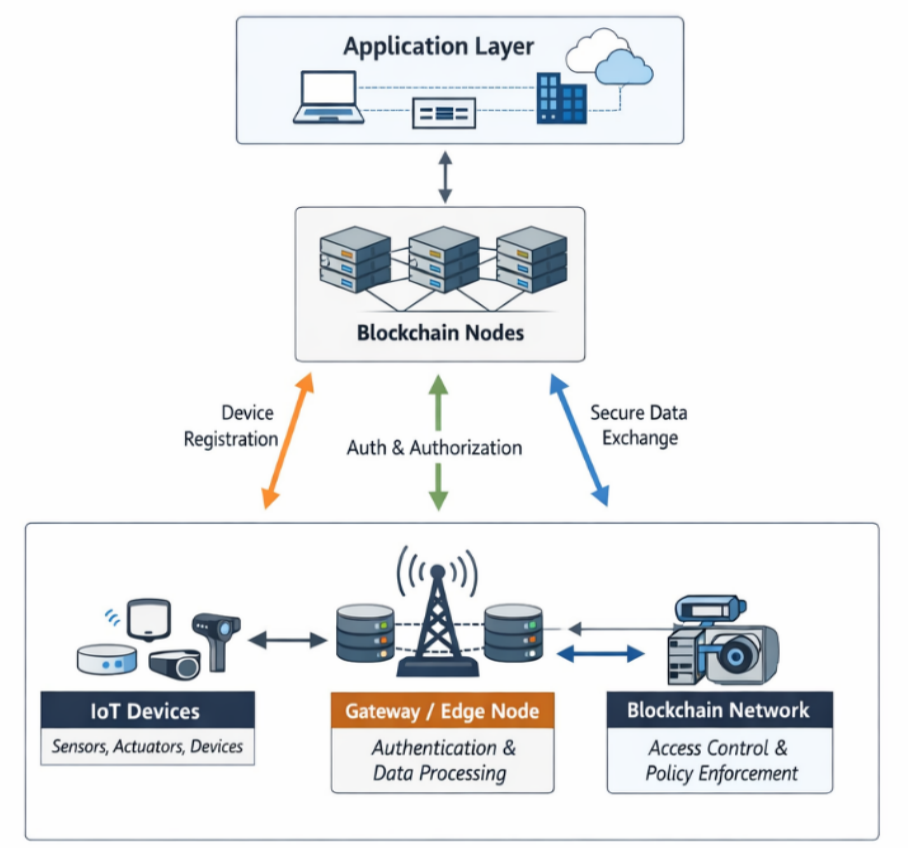
DOI: https://doi.org/10.56879/ijbm.v5i1.24

4. Proposed Blockchain-Enabled Secure Communication Framework

4.1 Framework Overview

The proposed framework presents a secure and decentralised communication system to the IoT networks, combining the blockchain technology, smart contracts, and lightweight cryptographic systems. The framework also has the advantages of not depending on a trusted third party as opposed to the traditional centralised security solutions, as well as facilitates distributed trust management between the IoT devices and network entities.

Figure 1. Blockchain-Enabled Secure Communication Framework



As shown in figure 1, the architecture is made of four logical components: (i) IoT devices, (ii) Gateway or edge nodes, (iii) Blockchain network, and (iv) Application layer. IoT devices interact with each other using gateways or edge nodes, which serve as an intermediary to contacting blockchain. The blockchain system has an inalterable registry that contains the identities of devices, the history of authentication, and access rights policy. Smart contracts regulate device registration, authentication and authorization, which offer automated and transparent security enforcement (Christidis & Devetsikiotis, 2016; (Dorri et al., 2017; Novo, 2018). This architecture

DOI: https://doi.org/10.56879/ijbm.v5i1.24

corresponds to the current research on the appropriateness of blockchain to secure and auditable IoT communication systems (Viriyasitavat et al., 2020; Reyna et al., 2018).

4.2 Blockchain Network Design

The framework uses a permissioned (private) blockchain, which is better than the public blockchains in an IoT setting because of the low latency, low cost of computation, and the controlled participation (Dorri et al., 2017; Lin & Yu, 2019). Blockchain nodes can only be involved by authorised bodies like gateways, edge nodes and service providers. To enforce an efficient consensus without the extensive use of computation, a lightweight consensus mechanism is embraced either Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA) (Castro & Liskov, 1999). These systems offer fault, and rapid finality of transactions, which are essential to IoT communication that is time sensitive. Each blockchain block contains: (i) Device identity records, (ii) Authentication transactions, (iii) Access control logs, (iv) Hashes of transmitted IoT data. The distributed ledger provides data integrity, transparency, and tamper resistance to make sure no malicious alteration of communication records is done (Zhang et al., 2018).

4.3 Smart Contract Design

Smart contracts are core to doing security operations automation in the proposed framework. They are executed in the blockchain to undertake device registration, authentication, authorization, and trust policies without human involvement. The major smart contract functions are (i) Device Registration. (ii) Authentication and Authorization (iii) Access Control Enforcement. (iv) Auditability. These decentralised and automated methods of access control can go a long way in promoting trust and security in IoT communication networks (Novo, 2018; Ouaddah et al., 2016).

4.4 Lightweight Cryptographic Mechanisms

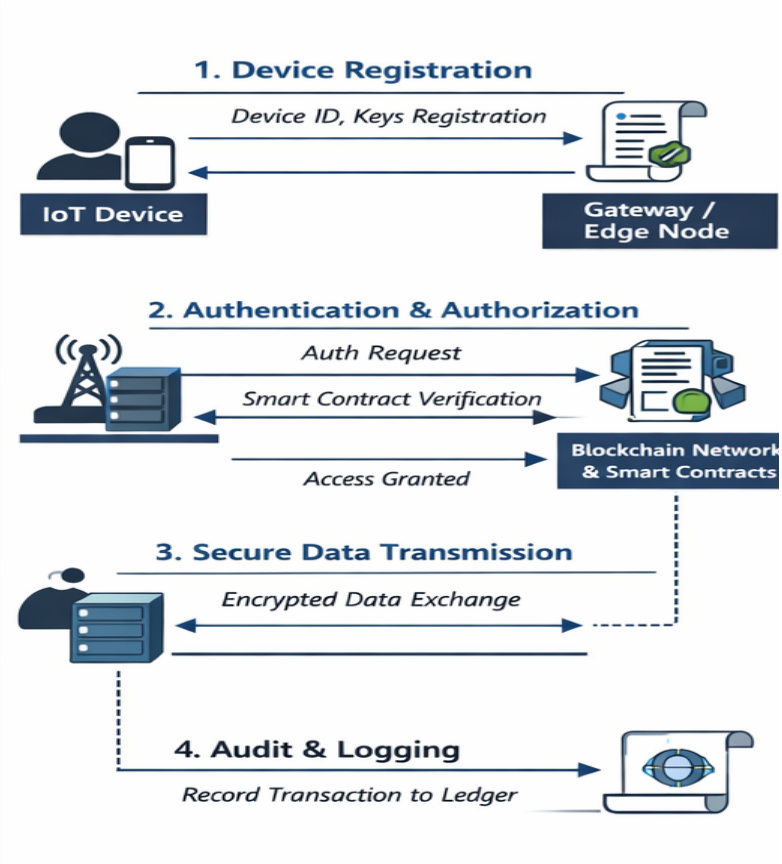
Considering the scarcity of computational and energy resources of IoT devices, the framework proposed in this paper considers lightweight cryptographic algorithms to achieve secure communication with minimal overhead. Confidentiality of data is done using symmetric encryption algorithms whereas integrity is done by cryptographic hash functions. To minimise the cost of computation, public-key cryptography is only used in the initial registration of devices and in key-exchange (Perrig et al., 2002; He et al., 2016). The framework adopts lightweight key management schemes, hash-based message authentication, and minimal cryptographic operations at device level. The framework balances security strength and resource efficiency by integrating lightweight cryptography and blockchain-based management of trust, which is appropriate in large-scale IoT applications (Karati et al., 2021).

DOI: https://doi.org/10.56879/ijbm.v5i1.24

5. Secure Communication Workflow

The Figure 2 explains how the process of secure communication is made possible through the suggested blockchain-based framework. The workflow guarantees decentralised authentication, secure exchange of data and immutable logging, and low overhead of the IoT-based devices.

Figure 2. Secure Communication Workflow



5.1 Device Registration Phase

Each IoT device is supposed to undergo a single registration process before it is allowed to be part of the network communication. At this stage, the device provides its identity credentials (e.g. device ID, public key, and metadata) to a gateway or edge node. The request goes through the gateway, which authenticates the request and calls a registration smart contract, which records the device identity hash on the blockchain ledger. The framework eliminates identity spoofing by ensuring that the records of identities of devices are stored on an unalterable register, and decentralised trust is formed without a central authority (Christidis & Devetsikiotis, 2016; Novo, 2018). This is in line with blockchain-based identity management plans that have been suggested in recent IoT security literature (Ouaddah et al., 2016; Zheng et al., 2017).

DOI: https://doi.org/10.56879/ijbm.v5i1.24

5.2 Authentication and Authorization Phase

Authentication must be done when an IoT device is initiating communication or requesting network resources. The gadget creates a request of authentication, which is sent to the blockchain network through the gateway. A smart contract is also used to identify the credentials of the device by comparing them to the recorded blockchain entries. Once the authentication is successful, the decisions of authorization are automatically implemented using predefined access control policies coded in smart contracts. This would make sure that only authorised and valid devices can take part in communications or utilise certain services. The decentralised authentication system contributes to reducing risks of single-point-of-failure, as well as enhancing the resistance to impersonation attacks (Dorri et al., 2017; Novo, 2018).

5.3 Secure Data Transmission Phase

The need to transmit data securely is demonstrated through the fourth stage, which is the secure data transmission phase. Once the authentication and authorization processes are complete secure transmission of data is then provided between communicating entities. Sensed information is encrypted by IoT equipment with lightweight symmetric encryption and integrity proofs are created with cryptographic hash functions. The encrypted messages are sent over the network where a hash of the data/data reference or transaction is stored on the blockchain. The use of hashes in place of raw data can save much storage overhead, but earns the data integrity and non-repudiation properties (Reyna et al., 2018; Zhang et al., 2018). Any form of interference with transmitted data can be identified by comparing computed hashes with hashes on the blockchain register.

5.4 Audit & Logging

Every security related operation, e.g., authentication permission or confirmation of data transmission are wrapped into a blockchain transaction. Authorized blockchain nodes validate these transactions with the help of a light weight consensus mechanism like PBFT or PoA. After being verified, the transactions are irrevocably stored in the distributed ledger. This guarantees resistance to tampering, transparency and auditability of every communication occurrence. Given that several nodes store ledger replicas, the structure can continue running when a few nodes are broken or inaccessible (Castro & Liskov, 1999; Androulaki et al., 2018).

At the end of communication, records of session termination are recorded in blockchain. Post-incident analysis, accountability and forensic investigation can be performed by means of security logs stored on the ledger. The audit trails provided by blockchains are inviolable and difficult to alter unlawfully, unlike centralised logs, which makes blockchain-based audit trails a more reliable communication system with the IoT (Viriyasitavat et al., 2020; Makhdoom et al., 2019).

DOI: https://doi.org/10.56879/ijbm.v5i1.24

6. Analytical Performance Evaluation

This section provides an analytical assessment of the suggested blockchain-based secure communication architecture with regards to the level of communication overhead, the level of computational complexity, and the level of scale. As it has been shown in the analysis, the framework offers a higher level of security but still allows decent performance under the conditions of resource-constrained IoT settings.

6.1 Communication Overhead Analysis

Within the suggested structure, the overhead of communication mainly includes the registration of devices, authentication operations, and updates of a blockchain ledger. In contrast to centralised architectures of IoT security models; all verification messages are sent to a centralised server; the suggested solution spreads trust among blockchain nodes and eliminates bottlenecks and enhances resilience to faults (Reyna et al., 2018; Zhang et al., 2018). In the standard mode of operation, an IoT device sends and receives a few messages like Authentication request to gateway, Smart-contract verification request, and Authorization response. The blockchain contains only the hash values or transaction references of the data communication but not actual sensor data. This architecture can greatly minimise bandwidth usage and storage of the network and maintain integrity of data (Reyna et al., 2018; Makhdoom et al., 2019). The proposed method has a smaller communication overhead when compared to fully on-chain approaches to data storage, and thus it is appropriate to large-scale IoT deployments.

6.2 Computational Complexity Analysis

Cryptographic lightweight operations, including both symmetric encryption and hashing, and message authentication, are done as lightweight operations on IoT devices, with computational complexity that is linear or nearly constant with message size (Perrig et al., 2002; Karati et al., 2021). Only the first registration and key exchange processes are done using public-key, which helps to reduce energy consumption and processing costs on devices. The gateway or edge nodes with greater computational power do the smart contract execution and consensus operations. The framework excludes inefficient uses of the proof-of-work computation like PBFT or PoA to achieve consensus by which costly computation becomes necessary and therefore consumes less processing time and energy (Castro & Liskov, 1999; Androulaki et al., 2018). Analytically, the computational load on IoT devices is also not dependent on size of blockchain, therefore they can be predictable as the size of the network is increased.

6.3 Scalability Analysis

One of the demands of the IoT communication systems is scalability because the number of devices connected to it is constantly growing. Authentication and access control services become common bottlenecks of performance in centralised security architectures with increase in the number of devices (Ammar et al., 2018; Roman et al., 2018). Conversely, the suggested model

DOI: https://doi.org/10.56879/ijbm.v5i1.24

spreads authentication and trust management amongst the blockchain nodes. With a growing number of IoT devices, the system is capable of supporting a larger number of the devices with distributed ledgers of device authentication records and access policies with no centralised congestion. Permissioned blockchain also allows increased scaling through restricting the number of nodes that are allowed to participate and decreased the consensus overhead (Lin & Yu, 2019; Androulaki et al., 2018). Analytically, as the size of the ledger increases in a linear manner with the number of transactions, it does not directly affect the performance of IoT devices since the performance of the constrained devices does not keep full blockchain replicas. Because of this, the framework exhibits scalable and stable behaviour that is applicable in real-world IoT communication environments (Makhdoom et al., 2019).

7. Comparative Discussion

In the below mentioned Table 1, a comparison of the proposed framework with the existing blockchain-based IoT security solutions reported in the literature is provided. The aim is to emphasise the unique strengths, design compromises, and applicability of the proposed framework.

Table 1. Comparison of Blockchain-Based IOT Security Frameworks With The Proposed Framework

Framework	Architecture	Authentication & Access Control	Auditability	IoT Suitability	Key Limitations
Christidis & Devetsikiotis (Christidis & Devetsikiotis, 2016)	Semi-decentralized	Smart contracts for transactions	Partial	Moderate	Limited scalability discussion
Dorri et al. (Dorri et al., 2017)	Hybrid	Local blockchain with access rules	Limited	High	Restricted interoperability
Novo (Novo, 2018)	Permissioned blockchain	Blockchain-based access management	High	Moderate	Gateway dependency
Ouaddah et al. (FairAccess) (Ouaddah et al., 2016)	Decentralized	Token-based access control	High	Moderate	Policy complexity

DOI: https://doi.org/10.56879/ijbm.v5i1.24

Zhang et al. (Zhang et al., 2018)	Blockchain-assisted	Data integrity-focused	High	Low–Moderate	High computational overhead
Proposed Framework	Permissioned decentralized	Smart-contract-driven authentication and authorization	High (immutable logs)	High	Conceptual (no experimental validation)

The suggested framework has a few remarkable strengths in comparison with the current methods. In contrast to the frameworks that address access control or data integrity only, the proposed one presents an end-to-end secure communication workflow, which includes registration, authentication, authorization, transmission, and auditability. The framework is decentralised and lightweight in consensus mechanism by incorporating a permissioned blockchain and is thus suitable in IoT environments (Androulaki et al., 2018; Makhdoom et al., 2019). Smart contracts are useful in enforcing security policies automatically, decreasing the number of people who have to write code and configuration mistakes, improving the reliability of the system (Christidis & Devetsikiotis, 2016; Novo, 2018). The blockchain logs are immutable and provide a strong audit trail which is superior to the traditional centralised logging mechanisms and allows forensic examination and non-repudiation (Viriyasitavat et al., 2020; Reyna et al., 2018).

8. Conclusion, Limitations and Future Work

8.1 Conclusion

The current paper presented a blockchain-enabled secure communication system in Internet of Things (IoT) networks, which overcomes the key challenges in authentication, data integrity, and decentralised control of trust. The framework does not rely on traditional centralised architecture; instead, it uses permissioned blockchain technology, access control using smart-contracts, and cryptography mechanisms with very few resources to ensure secure, auditable and scalable communication between heterogeneous devices in the IoT. Storing access policy and device credentials on the blockchain, the architecture removes single points of failure and gives out distributed trust to all the network (Christidis & Devetsikiotis, 2016; Dorri et al., 2017). The architecture offers a sequential approach to registration, authentication, authorization, transmission of encrypted data, and logging of audits (Novo, 2018; Zhang et al., 2018). IoT devices with limited resources can conduct very little cryptographic work, yet maintain data confidentiality and integrity (Perrig et al., 2002; Karati et al., 2021). Blockchain logs can be viewed in a transparent manner, with the ability to forensically analyze and non-repudiate immutable logs (Viriyasitavat et al., 2020; Makhdoom et al., 2019). Conceptual and analytical evaluation of the framework shows that it has low communication and computation cost, scalability for large-scale IoT deployments, and resilience to typical attacks like replay, man-in-the-middle, and unauthorised access (Reyna et al., 2018; Androulaki et al., 2018).

DOI: https://doi.org/10.56879/ijbm.v5i1.24

The framework, in general, provides a realistic, security-focused architecture of the IoT communication system that could be utilised in smart cities, industrial automation, and healthcare monitoring, and other resource-intensive IoT applications.

8.2 Limitations and Future Scope

The proposed framework has some limitations, despite its benefits. To begin with, quantitative performance evaluation is limited by the lack of simulation or real-world implementation. Second, the implementation of blockchain is bound to add communication and computation overhead that will have to be tightly controlled in IoTs with ultra-resource-limited conditions. Nevertheless, these weaknesses are recognised and placed clearly as prospects of future work. The conceptual and analytical validation is one of the most common options in the early-stage blockchain-IoT studies (Dorri et al., 2017; Makhdoom et al., 2019). Although conceptually rigorous, the present study recognises several opportunities of further research. Future research will apply the suggested framework on a real IoT testbed or a simulation platform (e.g., Contiki, NS-3, Hyperledger Fabric IoT prototype) and measure the latency, throughput, and energy consumption. Secondly, Exploring hybrid blockchain-edge computing systems to enable ultra-large-scale IoT systems with limited communication and storage overheads. Thirdly, Integration with AI for Threat Detection: Adding machine learning algorithms in order to identify the presence of anomalies and security threat in real time. The future scope may also investigate IoT standard compatibility with IEEE 1451 and oneM2M to enable cross-platform adoption. Also, designing dynamically scalable cryptographic protocols that decrease the security according to the energy that the device has and the conditions of the network.

These future directions will further improve the practicality, resilience, and the performance of blockchain-enabled IoT communication systems to bridge the gap between conceptual framework and real-world implementations.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347–2376.

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8–27..

Androulaki, M., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., … Yellick, J.

DOI: https://doi.org/10.56879/ijbm.v5i1.24

(2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In Proceedings of the 13th EuroSys Conference (pp. 1–15).

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787–2805.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing (pp. 13–16).

Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI) (pp. 173–186).

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292–2303.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027–2051.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in internet of things: Challenges and solutions. IEEE Communications Surveys & Tutorials, 19(3), 1731–1752.

He, D., Chan, S., & Guizani, M. (2016). Cyber security analysis and protection of wireless sensor networks for smart grid monitoring. IEEE Wireless Communications, 23(2), 98–103.

Karati, A., Islam, S. H., & Biswas, G. P. (2021). Lightweight cryptographic protocols for internet of things: A survey. IEEE Internet of Things Journal, 8(10), 7924–7950.

Lin, H., & Yu, W. (2019). Blockchain-based data management for IoT. IEEE Internet of Things Journal, 6(3), 4504–4514.

Makhdoom, I., Abolhasan, M., Abbas, H., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. Journal of Network and Computer Applications, 125, 251–279.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184–1195.

Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2016). FairAccess: A new blockchain-based access control framework for the internet of things. Security and Communication Networks, 9(18), 5943–5964.

DOI: https://doi.org/10.56879/ijbm.v5i1.24

Perrig, A., Szewczyk, R., Wen, V., Culler, D., & Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. Wireless Networks, 8(5), 521–534.

Reyna, M. A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190.

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog, et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680–698.

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266–2279.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76, 146–164.

Viriyasitavat, W., Xu, L. D., Bi, Z., & Sapsomboon, A. (2020). Blockchain-based business process management framework for service composition in Industry 4.0. Journal of Intelligent Manufacturing, 31, 1737–1748.

Xu, X., Lu, Q., Liu, Y., Zhu, L., Yao, H., & Vasilakos, A. V. (2019). Designing blockchain-based applications: A case study for imported product traceability. Future Generation Computer Systems, 92, 399–406.

Yang, Y., Zhang, H., Chen, J., & others. (2019). Blockchain-based trusted data sharing scheme in internet of things. IEEE Transactions on Industrial Informatics, 15(3), 1877–1887.

Zhang, Y., Yu, R., Xie, S., & Guizani, M. (2018). Blockchain-based security framework for IoT. IEEE Network, 32(6), 72–77.

Zhang, Y., Yu, R., Xie, S., Zhang, Y., & Guizani, M. (2011). Home M2M networks: Architecture, standards, and QoS improvement. IEEE Communications Magazine, 49(4), 44–52.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the IEEE International Congress on Big Data (pp. 557–564).

DOI: https://doi.org/10.56879/ijbm.v5i1.24