Blockchain Based Decentralized Identity Management System for Authentication and Authorization in IoT Networks

Kriti Patidar[1], Swapnil Jain[1], Mohammad Husain[2*], Mohd.Muqeem[3], Mohammad Nadeem Ahmed[4], Ahmad Neyaz Khan[5*], Mohammad Rashid Hussain[6], Arshad Ali[2], Nazneen Mushtaque[7]

[1]Department of Electrical and Electronics Engineering (EEE), Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, Madhya Pradesh, India

[2]Department of Computer Science, Faculty of Computer and Information systems, Islamic University of Madinah, Madinah-42351, KSA

[3]Department of Computer Science and Engineering, Sandip University, Nashik. Maharashtra, India

[4]Department of Computer Science, College of Computer Science, King Khalid University, Kingdom of Saudi Arabia, Abha-61421, KSA

[5]Department of CSE-Cybersecurity, Department of Computer Science, NIET, Greater Noida, UP, India

[6]Department of Business Informatics, College of Business, King Khalid University, Kingdom of Saudi Arabia, Abha-62217, KSA

[7]Department of Information Systems, Rijaal alma, King Khalid University, Kingdom of Saudi Arabia, KSA

E-mail: Kritipatidar09@gmail.com, swapnil4388@gmail.com, dr.husain@iu.edu.sa, muqeem.79@gmail.com, monaahmed@kku.edu.sa, ahmadnk500@gmail.com, humohammad@kku.edu.sa, a.ali@iu.edu.sa, nmshtag@kku.edu.sa

*Corresponding author

Keywords: decentralized identity management, authentication, IoT devices, distributed network, decentralized network

Received: May 8, 2025

As IoT-connected devices, sometimes referred to as the Internet of Things (IoT), continue to proliferate, existing centralized identity management systems struggle in the large scale due to issues with scalability, privacy and security. For these reasons, centralized identity management systems will not meet the requirements of large-scale IoT deployments. In this paper, we suggest a decentralized identity management system to authenticate and authorize IoT devices based on a hybrid blockchain and Zero-Knowledge Proof (ZKP) protocol. The proposed system utilizes decentralized identifiers (DIDs), verifiable credentials (VCs) and a hierarchical web-of-trust structure as part of the identity management process. The identity and credentials can be created and validated in a decentralized manner and locally, using smart contracts and lightweight consensus models such as Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT). The performance evaluation demonstrated the performance in respect of authentication latency businesses managed to get the latency to 250 ms, throughput reaching to 200 messages per second and energy efficiency improved to 300mW/device. Based on the baseline comparisons including PoW, OAuth and Hash-MAC based systems included, the proposed method is scalably better, provides greater security against DDoS and MITM attacks and used less memory. The proposed method yields a robust, fully decentralized identification system for managing IoT identities without requiring a centralized authority, allowing scalable and secure interactions across distributed networks.

Povzetek: Hibridni sistem za identitetno upravljanje v IoT združuje blockchain, DIDs, VCs in ZKP ter omogoča bolj kvalitetno avtentikacijo in avtorizacijo naprav kot centralizirani ali PoW pristopi.

1 Introduction

In recent years, the notion of the Internet of Things (IoT) has been popular due to the widespread use of high-speed networks that connect smartphones and other smart gadgets. These embedded or Internet of Things devices can also be accessed from a distance and can perform the necessary duties. They have connections to both public and private networks. Networking protocols are utilised by both public and private networks to facilitate data sharing and communication among devices that are part of the Internet of Things (IoT). The Internet of Things, sometimes known as IoT, provides numerous benefits to individuals. These encompass activities such as weather surveillance, medical gadgets aiding in treatments, animal identification using biochips, and car connectivity and tracking. The IoT servers collect data from these devices continuously, analyse it, and utilise the findings to improve the overall functioning of the system. There has been a significant increase worldwide in the number of devices connected to the Internet of Things (IoT). The Corps Information System Control officers (Cisco) have forecasted that by the conclusion of 2021, there would be a total of 40 billion interconnected gadgets [1]. Internet-connected gadgets not only consume a significant amount of energy, but they are also susceptible to hacking due to their inability to protect themselves against harmful attacks such as denial-of-service, masquerading, man-in-the-middle, and other similar attacks. This vulnerability grants unauthorised access to internet-connected devices, enabling individuals to do calculations according to their own preferences. Therefore, enhancing the security of Internet of Things devices is of utmost importance. In order to fulfil the goal of ensuring the entire security of Internet of Things devices, it is necessary to utilise appropriate user and device authentication mechanisms, together with computational transaction procedures. The system must ensure seamless communication between users and Internet of Things devices. The Internet of Things (IoT) employs networking protocols to establish connections between end users [2]. Any authentication technique for users and Internet of Things devices must recognise that these devices are appliances with restricted capabilities and are unable to perform substantial transactions or processing. Implementing secure user and device authentication techniques that are resistant to threats and attacks, can be easily expanded, and ensure authenticity is essential. Currently, there is a wide range of authentication approaches available, all designed to safeguard Internet of Things devices.

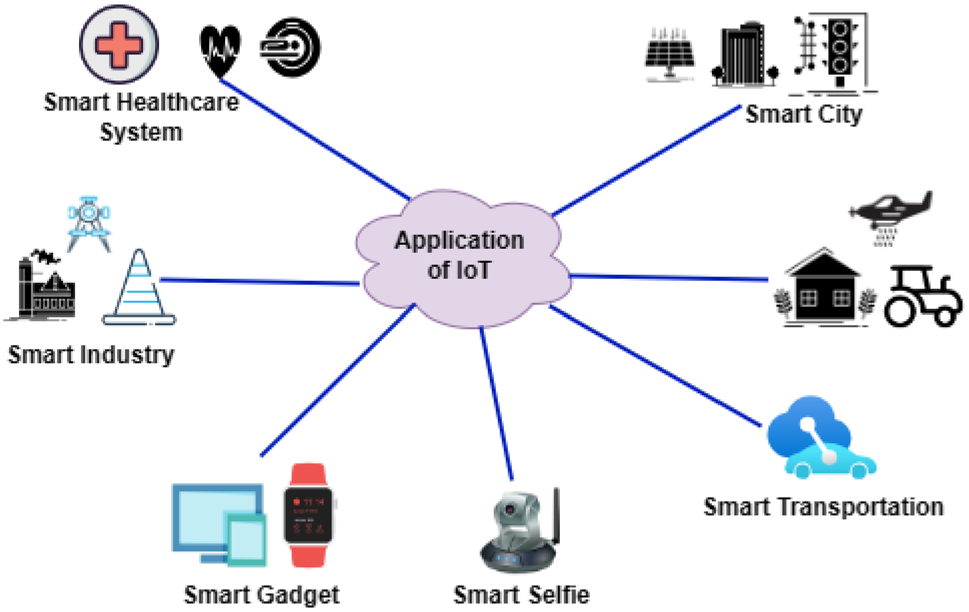

Figure 1: IoT device

However, the majority of existing solutions are constructed using a centralized design and rely on a governing entity, such as a centralized database or authentication server, which introduces bottlenecks and vulnerabilities. A centralised authority employs several encryption [3] approaches to authenticate end users, Internet of Things (IoT) devices within the system, and the communication logs between end users and IoT devices. Procedures encompassed by integrated authentication include mutual authentication, certificate-based authentication, and token-based authentication. These techniques are plagued by various problems, including exorbitant transaction processing expenses, dependence on centrally trusted third parties, vulnerability to hacking, lack of privacy, and other concerns. These strategies give rise to two distinct types of dependency problems as they depend on a reliable third party in this manner. Figure 1 provides an overview of key IoT application domains, such as smart healthcare and smart cities, which contextualize the diverse environments where secure and scalable identity management is critical.

This describes a technique for authentication of Internet of Things devices that addresses the limitations of centralised authentication by using a decentralised approach based on an algorithmic blockchain. The presented technique can be used to verify both individuals and Internet of Things-connected devices. In addition to offering security without requiring a centralised identity, the suggested [4] approach assists end-users in securely associating communication with Internet of Things devices. This research workaims to achieve security for end users, Internet of Things devices, and inter-device communication by implementing decentralised approaches. For a more precise illustration, we present a whole system consisting of end users, blockchain algorithms, and Internet of Things (IoT)-connected devices. These algorithms serve two purposes: they incorporate blockchain algorithmic logic into the public area network and fulfil authentication requirements.

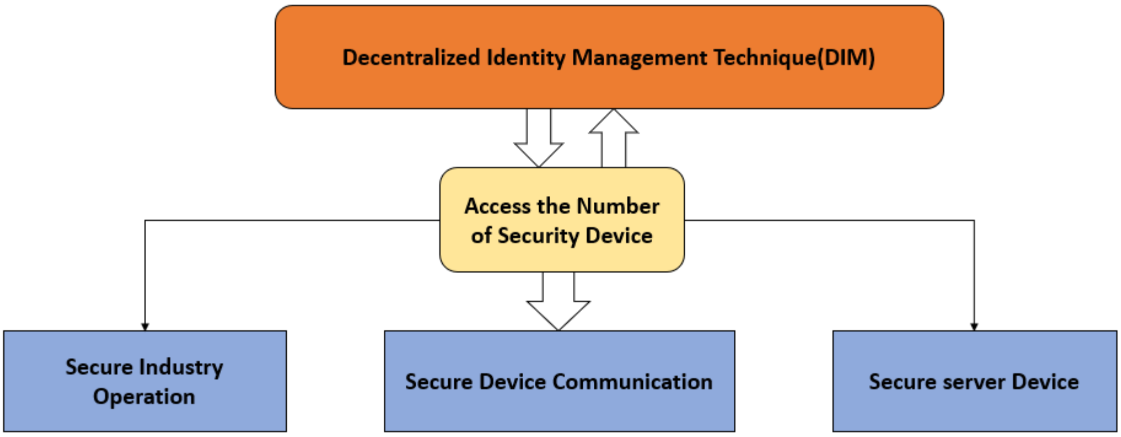
Decentralized Identity Management Technique(DIM)
Access the Number of Security Device
Secure Industry Operation
Secure Device Communication
Secure server Device

Figure 2: Trustworthy connections

Advancements in this field will enable the establishment of secure environments for the internet of things, leading to a more reliable and interconnected world.

- Evaluate the available identity management solutions in a decentralised Internet of Things environment. This will be beneficial for guiding future practices and evaluating present ones.
- Deliver a robust, efficient, and scalable decentralised identity management system with enhanced security measures. The strategy should not only tackle privacy and security concerns related to the Internet of Things, but also be very efficient for large-scale distributed networks.
- to determine the effectiveness of the new strategy. In order to accomplish this, a simulation of the technique will be conducted using a distributed network deployment. The evaluation will focus on assessing the robustness, scalability, and performance of the system.

The paper is organized in the following manner: Section 1 presents a related work, Section 3 proposed methodology; Section 4 simulation parameter and results section and a comparative analysis; and finally, Section 5 concludes the paper.

2 Research design

The rapidly evolving complexity and scale of IoT deployments require a reexamination of conventional identity management frameworks particularly with respect to decentralization, privacy, and to meet the performance requirements of those frameworks. This research was aimed at these challenges by developing and assessing a hybrid blockchain-based identity management framework with the use of ZKPs, DIDs, and smart contract-based authorization. In the interest of transparency and consistency in approach, this section presents the primary research questions guiding the study, the hypotheses that were assessed and the concrete design objectives that framed development and evaluation of the proposed identity management system. This study aims to answer the following primary questions:

- **RQ1:** Can a ZKP-enabled decentralized identity management system sustain low user authentication latency (≤ 300 ms) under large-scale user conditions (e.g., 5000+ IoT devices) when considering distributed network topologies?
- **RQ2:** Do energy-efficient consensus frameworks achieve a more significant impact than PoW in the system's scalability, energy efficiency, and real-time responsiveness within IoT ecosystems?
- **RQ3:** Are decentralized identity components (e.g. DIDs, VCs) in combination with smart contracts sufficiently secure and sufficiently private such that a central authority or trusted third party is not required?

By framing these questions this way, I am not only looking at the overall system performance but also to evaluate the ability of the complete system in terms of: (1) architectural independence, (2) resilience, and (3) applicability in resource-constrained, high-density, IoT environments. Given the existing limitations of centralized identity models and the prospective capabilities of blockchain and cryptographic technologies, we outlined the following hypotheses:

- **H1:** With the use of ZKPs to create a decentralized identity model, the system will be capable of achieving an average authentication latency of less than 300 ms across the authentication process, while the number of registered IoT nodes continues to increase and scale above 5000.

- **H2:** The use of PoS or PBFT consensus, in place of PoW, will lead to a minimum 30% reduction in energy consumption, while serving at least the same throughput, fault tolerance, and transaction finality.
- **H3:** Our use of DIDs and VCs, and smart contracts with immutability, will withstand known attacks (DDoS, MITM, replay), compared to commercial MAC-, OAuth-, and certificate-based systems, which are reliant on centralized trust anchors.

These hypotheses are examined through: simulation-based performance testing, comparative benchmarking, and security scenario modeling, as further developed in sections three and four respectively. In order to confirm the above hypotheses and respond to the research questions, a system level design principles were developed as follows:

- **G1**: Low Latency- The system must maintain an average end-to-end authentication latency of ≤ 300 ms across heterogenous network topologies including, during high-load scenarios for thousands of devices.
- **G2:** Full Decentralization- The identity management process must not depend on any central authority for key issuance, validation, or credential revocation.
- **G3:** Scale and Network Efficiency- The framework must support at least 5000 IoT devices concurrently active without significant decreases in throughput and consensus time. The throughput must be ≥ 150 TPS and latency must grow sublinear with respect to the node count, ideally no higher than another 1 ms of latency per node.
- **G4:** Security Assurance- They will demonstrate resistance to DoS, MITM, and replay attacks using cryptographic methods such as zkPs, and hashed key management, and tamper-proof distributed ledgers.
- **G5:** Resource Efficiency- The authentication mechanism must also work under a ≤ 300 mW power budget per device and must consume no more than 8MB of memory during peak authentication and authorization operations. Both of these must remain threshold levels to insure applicability to constrained IoT environments.

These design principles correspond to quantitative measures against which to evaluate the operational feasibility and successful deployment of the system. The results produced in simulation environments both positively confirm the hypotheses, and enable the evaluation of the transition to eventual real integration.

3 Related work

There is now a significant amount of research and development focused on exploring the possible applications of blockchain technology in the Internet of Things. Several methods have been developed to enable the seamless integration of blockchain technology with the Internet of Things. provides a comprehensive examination of the potential applications of blockchain technology in the Internet of Things. This concept aims to enhance the scalability and interoperability of the Internet of Things by introducing a new architecture that combines blockchain technology with the Internet of Things.

M. Adil et al. (2022) The aim of this work is to develop a lightweight mutual authentication method for Internet of Things (IoT)-based intelligent cyber-physical systems (CPS). The system uses a media access control (MAC) address and the hash function to verify network device authentication. The hash-MAC-DSDV routing protocol is the foundation of this authentication procedure. The simulation has proven to be successful in demonstrating the system's efficacy in terms of security and performance.

Cirani et al. (2015) This paper proposes an OAuth-based authorization service architecture for secure services in IoT scenarios. The architecture is designed to be lightweight and scalable, and it provides a number of security features, such as mutual authentication, authorization, and data integrity. The architecture is evaluated using simulation, and the results show that it is effective in terms of security and performance.

Condry, M. W., & Nelson, C. B. (2016) This study examines the capacity of intelligent edge Internet of Things devices to enhance control operations of the Internet of Things within a business. By utilising these devices, security measures are enhanced, and responses are expedited. The authors argue that by using smart edge Internet of Things devices, industrial Internet of Things networks can be enhanced in terms of trustworthiness and security. This article focuses on examining a chemical factory that has used a smart edge Internet of Things technology to enhance worker safety.

Chaudhry et al. (2020) This essay introduces a self-contained authentication method for future networks. This technique is specifically designed to be easily adaptable to different scales and to have a minimal impact on system resources. It includes features such as the ability to verify the identity of both parties involved, control access to resources, and ensure the accuracy and consistency of data. The simulation results demonstrate the efficacy and efficiency of the strategy.

Leithardt et al. (2020) This study discusses a pairing-free, lightweight, and unlinkable user access control system as a potential solution for distributed Internet of Things applications. The technique is efficient, safe, and scalable all at the same time. Simulation results demonstrate the strategy's benefits in terms of performance, security, and scalability.

In order to better compare the existing identity management and authentication methods for IoT settings, a complete tabular comparison across several core performance criteria, such as authentication delay, memory usage, scalability, and security features offered has been provided as Table 1 (a). This allows us to summarize not only the methods' strengths but also identify the critical gaps left unattended, leading to the rationale for our proposed approach.

Table 1: (A) Comparative analysis

Ref.	**Authors (Year)**	**Methodology**	**Auth Time (ms)**	**Memory Use**	**Scalability**	**Key Security Features**
[1] M. Adil et al. (2022)	Hash-MAC, DSDV	300	Moderate	Low (≤1k)	Mutual Auth, Hash-based Integrity	Centralized, not scalable
[2] Cirani et al. (2015)	OAuth-based Auth	350	High	Moderate	Token Auth, Data Integrity	Centralized trust dependency
[3] Condry & Nelson (2016)	Cert-based Auth at Edge	400	High	High	Rapid Edge Response, Auth Certs	Cert overhead, not privacy-focused
[4] Liang et al. (2020)	Behavioral Biometrics	290	Moderate	Moderate	Continuous Auth, Biometric AI	Requires real-time behavioral data
[5] Azad et al. (2019)	Self-enforcing Auth	310	Moderate	Low	Policy-based Auth	Complex policy management, not scalable
[6] Chaudhry et al. (2020)	Pairing-Free Lightweight Access Control	280	Low	Moderate	Unlinkability, Efficient Access	No blockchain integration
[7] Leithardt et al. (2020)	Dynamic User Profile Management	320	High	Moderate	Access Adaptation, Profile Security	Not focused on device-level identity
[9] Oktian & Lee (2021)	Blockchain Access Control	270–300	High	Moderate	Decentralized Auth, Access Rules	Scalability limited, high overhead
[10] Zeng et al. (2021)	Deniable Privacy-Preserving Auth	310	Moderate	Low	Deniability, Location Privacy	Location leakage, limited control
[11] Li et al. (2019)	3-Factor Auth with Forward Secrecy	350	High	Low	Forward Secrecy, Resilience	Poor performance in WMSNs
[12] Aman et al. (2018)	Token-based Auth, Energy-aware	330	Moderate	Moderate	Energy-Quality Tradeoff	Tradeoff degrades QoS
[13] Gaba et al. (2020)	Lightweight Mutual Auth	300	Low	Moderate	Mutual Auth, ECC-based	Overhead in distributed context
[14] Lu et al. (2020)	TPM for eHealth IoT	360	High	Low	Trusted TPM Sharing	Limited to eHealth, hardware-heavy
[15] Macedo et al. (2019)	Literature Review	N/A	N/A	N/A	High-level Synthesis	No specific methodology proposed
[16] Arfaoui et al. (2020)	Context-Aware Remote Access	340	Moderate	Low	Contextual Policies	No empirical performance analysis
[17] Patel & Doshi (2020)	ECC Lightweight Key Exchange	290	Low	Low	Secure Key Exchange	Gateway-focused, lacks full stack auth
Proposed Work	Hybrid Blockchain + ZKP	**250**	**Low (8 MB)**	**High (≥5k devices)**	ZKP, PoS, Decentralized IDs, Full Auth Chain	—

From this comparison, it is clear that although many techniques provide separate improvements to several different dimensions - privacy-preserving vs. non-privacy-preserving authentication, decentralized access control, etc. - few solutions offer a satisfactory perfect balance of security, scalability, and performance in the same framework. To be specific, many of the approaches outlined are either too centralised ([2], [3]), lack scalability ([1], [6]), or are not lightweight and verifiable at the device-level to document identity. None have effectively integrated ZKP and blockchain-based decentralized identifiers, while processing and using the available memory has not been minimized simultaneously. The work proposed in this work will articulate and address these open gaps via a hybrid blockchain-ZKP identity protocol that is lightweight, fully decentralized and suitable for real-time IoT deployments at scale.

Table 1: (B) Comparative analysis

Publication Year	Authors	Authentication Methodology	Authorization Methodology	Key Contributions
2022	M. Adil et al.[1]	Hash-MAC, DSDV routing protocol	Mutual authentication, secure communication	Mutual authentication scheme for IoT-based cyber-physical systems using Hash-MAC and DSDV routing protocol
2015	Cirani et al.[2]	OAuth	Authorization service architecture, secure services	OAuth-based authorization service architecture for secure services in IoT scenarios
2016	Condry, M. W., & Nelson, C. B.[3]	Certificate-based authentication, Edge computing	Safer, rapid response with industry IoT control ops	Utilizing smart edge IoT devices for safer and rapid response in industry IoT control operations
2020	Liang et al.[4]	Behavioral biometrics	Continuous authentication, AI-based perspective	Behavioral biometrics for continuous authentication in the Internet of Things era
2019	Azad et al.[5]	Self-enforcing authentication, Next Generation Network	Self-enforcing authentication mechanism	Self-enforcing authentication mechanism for Next Generation Networks
2020	Chaudhry et al.[6]	Pairing-free, Lightweight, Unlinkable user access control	User access control scheme	Pairing-free lightweight and unlinkable user access control scheme for distributed IoT environments
2020	Leithardt et al.[7]	Dynamic user profile management	User profile management in IoT environments	Dynamic management of user profiles in IoT environments
2021	Oktian, Y. E., & Lee, S.-G.[9]	Blockchain-based access control framework	Access control framework based on blockchain	Blockchain-based access control framework for IoT endpoints

Table 2: Summarizing IoT authentication and authorization research

Citation	Advantage	Disadvantage	Methodology	Research Gap
[9]	Blockchain-based security and key management	Scalability challenges of blockchain technology	Blockchain technology for authentication and key management	Scalability issues in using blockchain for IoT security
[10]	Privacy-preserving authentication	Deniability concerns	Deniable-based privacy-preserving authentication	Addressing location leakage in edge computing
[11]	Three-factor authentication with forward secrecy	Vulnerabilities in wireless medical sensor networks	Three-factor authentication protocol with forward secrecy	Security vulnerabilities in wireless medical sensor networks
[12]	Token-based security with dynamic energy-quality tradeoff	Energy-quality tradeoff limitations	Token-based security for IoT with dynamic energy-quality tradeoff	Balancing energy consumption and quality of service in IoT security
[13]	Robust and lightweight mutual authentication	Security overhead	Mutual authentication scheme in distributed smart environments	Reducing security overhead in distributed smart environments
[14]	Trusted Platform Module (TPM) sharing scheme	Limited scope of smart IoT-eHealth devices	Trusted Platform Module sharing scheme for smart IoT-eHealth devices	Enabling secure and trusted communication in smart IoT-eHealth devices
[15]	Systematic literature review on IoT security	High-level analysis without specific methodologies	Systematic literature review on IoT security	Identifying gaps and challenges in IoT security based on existing research
[16]	Context-aware adaptive remote access	Lack of performance evaluation	Context-aware adaptive remote access for IoT applications	Evaluating the performance of context-aware adaptive remote access for IoT applications
[17]	Secure lightweight key exchange	Limited to user-gateway paradigm	Secure lightweight key exchange using ECC	Extending secure key exchange mechanisms to broader IoT network scenarios

4 Methodology

4.1 Overview of the technique

The initial section of this paper addresses a variety of concerns related to traditional, centralised identity management systems in the context of Internet of Things devices. Decentralised identity management is suggested as a solution to these issues in the subsequent section of the essay. we am suggesting the implementation of a distributed ledger, which is similar to a blockchain, as a storage medium for the identification data of IoT devices[6]. This ledger's distributed structure guarantees that it cannot undergo a calamitous collapse at any particular point in the network. Furthermore, in order to guarantee the privacy of the personal data, the methodology implements a cryptographic mechanism. The efficacy and safety of the proposed procedure are completely assessed in the report. The approach's resilience against typical risks and its efficacy in real-world scenarios are demonstrated.

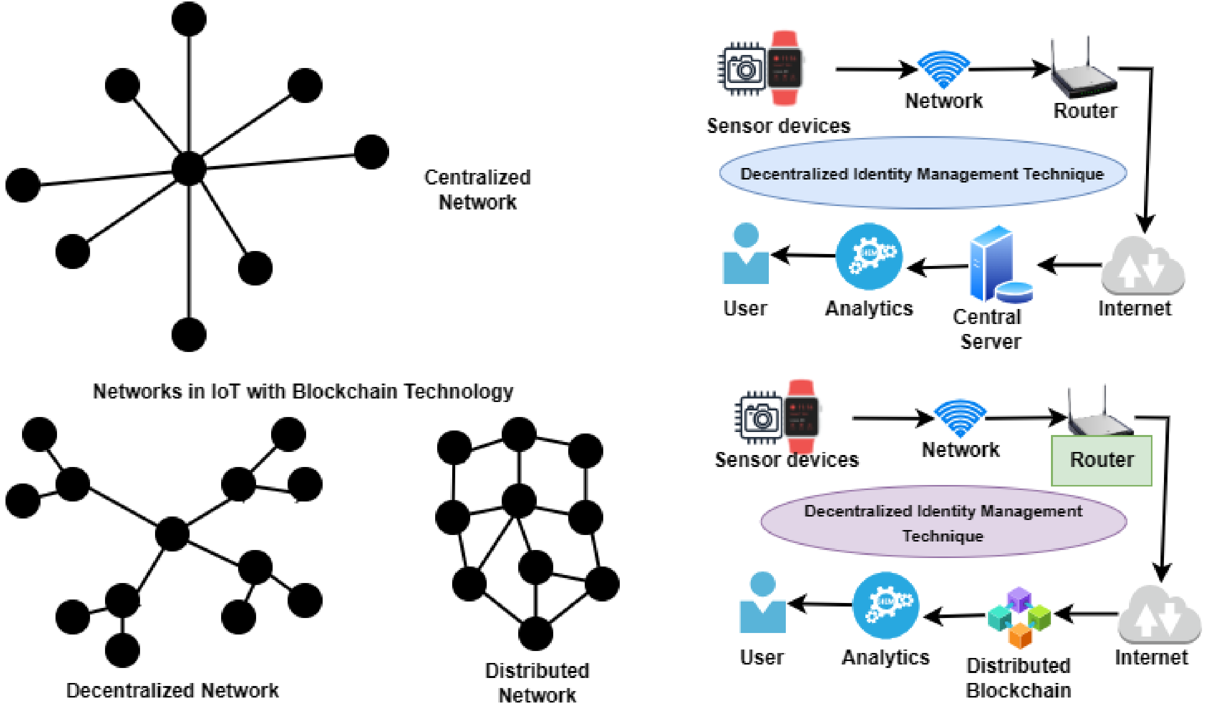

Figure 3: Decentralized identity management

4.2 Proposed decentralized identity management technique

The network nodes depicted make use of consensus processes in order to validate transactions that are recorded on the blockchain. A substantial influence is exerted on the scalability, latency, energy efficiency, performance, and security of the Internet of Things ecosystem by the consensus mechanism and blockchain type that are utilised in this scenario.

Proof of Work (PoW) is a decentralized consensus mechanism traditionally used by public blockchains like Bitcoin and early versions of Ethereum.

The utilisation of these methods, on the other hand, necessitates a significant expenditure of both time and computational resources in order to acquire a satisfactory response. These limitations have the potential to impede the effectiveness of the blockchain with regard to the Internet of Things in real-world scenarios.

Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT) are two consensus techniques that exceed Proof of Work (PoW) in terms of throughput, transaction time, and energy efficiency. PoS and PBFT are both examples of techniques that are becoming increasingly popular. Furthermore, Proof of Work (PoW) is not the only consensus method that satisfies these expectations; there are other methods as well. The architecture that has been proposed is intended to be deployed in a real-world Internet of Things [7] context wherever possible. The use of a private blockchain that employs consensus mechanisms such as Proof-of-Stake or Proof-of-Failure is employed in order to improve the network's level of security and trustworthiness. One of the many benefits of utilizing a private blockchain is the opportunity to improve scalability, while there are many other advantages as well. The transaction throughput is increased, the consensus process is sped up, and energy efficiency is enhanced. These are additional benefits. Because of these benefits, private blockchains are an excellent choice for real-time Internet of Things (IoT) situations that involve limited resources and require transactions to be both quick and secure across a number of different IoT zones.

4.3 Components of the technique

The methodology consists of four fundamental components. These components consist of verifiable credentials (VCs), blockchain technology, decentralized identities (DIDs), and a web of trust (WoT).

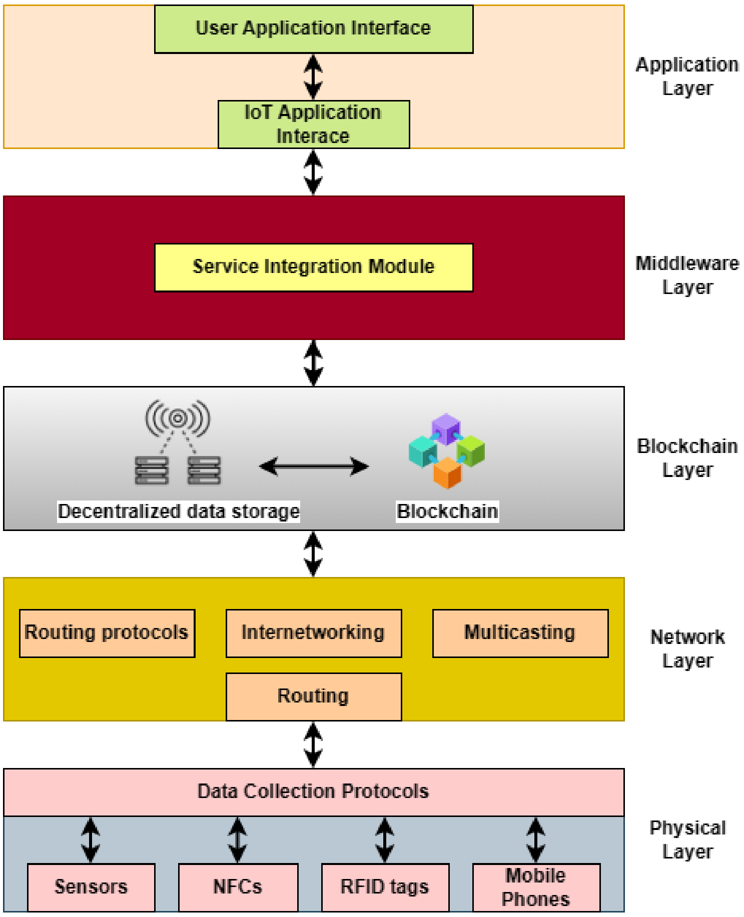

Figure 4: Proposed layered system

Decentralized identifiers (DIDs) are inherently distinct, universally distinct, and can be verified using cryptographic methods. However, the individuals who possess DIDs have complete authority over their identifiers. Distributed Identifiers (DIDs) have enabled Internet of Things (IoT) items to establish and control their own distinct identities, hence reducing the requirement for them to connect to a central repository. Moreover, digital identifiers facilitate the generation of a limitless array of identities, which can be utilized to improve management over matters such as anonymity, traceability, revocability, and auditability across many situations.

Verifiable credentials (VCs) are digital signatures that attest to certain attributes or capabilities of an IoT device. VCs are cryptographically signed by trusted entities, and anyone can verify the signature using the entity's public key. VCs enable devices to authenticate themselves without revealing sensitive or personally identifiable information. This enhances privacy and retains trust between devices on the network.

There are four primary components that make up the methodology. Verifiable credentials (VCs), blockchain technology, decentralized identities (DIDs), and a web of trust (WoT) are the components that make up these components.

These decentralized identifiers (DIDs) are inherently distinct and globally unique, and may be validated through the use of cryptographic verification techniques. On the other hand, the individuals who are in possession of DIDs have full control over their identifiers. Distributed Identifiers, also known as DIDs, have made it possible for Internet of Things (IoT) devices to create and manage their own unique identities, hence decreasing the necessity for these devices to connect to a central repository. Furthermore, digital identifiers make it possible to generate an infinite number of identities, which can be utilized to enhance management in a variety of contexts, including when it comes to issues of anonymity, traceability, revocability, and auditability.

Verifiable credentials, often known as VCs, are digital records that are used to provide proof in support of assertions on the attributes or functionalities of an Internet of Things (IoT) device. Verifiable Credentials, also referred to as cryptocurrencies, are digital assets that are generated and managed by trustworthy institutions. They are decentralized and can be referred to as Verifiable Credentials. Validating their public keys is possible for everyone. Internet of Things (IoT) connected devices are able to validate their identities through the use of virtual currency (VCs), which prevents the disclosure of any personal or potentially unwanted information. This particular dataset includes comprehensive information concerning ownership and the permissions to access it.

4.4 Security analysis of the technique

Blockchain-based transactions universally employ digital signatures. When individuals with administrative, managerial, or user roles in the Internet of Things initiate a transaction, the proposed method generates a cryptographic key pair (public and private) used for securing transactions through encryption and digital signatures.

The following is an explanation of how the encryption process operates: a) When initiating a transaction on the blockchain, an administrator, manager, or user on the Internet of Things network utilizes their private key to digitally sign the hash value of the data. b) Once the hash value is signed, it is transmitted to the blockchain network alongside the member's digital signature, transaction data, sender's public key, and recipient's address. c) Validators or miners are the individuals responsible for receiving and verifying the transaction. d) Once the validation phase is completed successfully, the transaction is incorporated into the blockchain ledger through the consensus mechanism, ensuring its inclusion in a new block. This paper proposes a decentralized authentication process, based on discussions in previous literature, and the original architecture and protocol design described is applied for scalable, secure IoT identity management. Although previous works provide useful surveys on blockchain-based authentication models (see e.g. Malik et al. [18]), the specific scheme proposed here incorporates new integrations of zk-SNARKs, verifiable credentials, and modular smart contract logic.

4.4.1 Efficiency analysis of the technique

In order to ensure that all of the nodes in an Internet of Things network are synchronized with one another in an effective manner, each node is assigned a certain task to complete. The following is a comprehensive account of each and every interaction:

The task of connecting users, Internet of Things managers, and devices to the appropriate Internet of Things zones falls on the administrator.

The administrator is accountable for the design and deployment of the smart contract onto the blockchain. Upon deployment, the smart contract is immutable, which enforces that the logic cannot be changed, which helps establish trust and integrity in the system.

Using a web3 provider, each and every Internet of Things manager that is part of the manager-to-blockchain configuration is connected to a blockchain node. The JSON RPC protocol is being utilized for the purpose of this connection. The blockchain network uses smart contract rules to validate the identities of the Internet of Things manager and the connected devices. This verification process occurs after the registration procedure has been completed. As a consequence of this, the protocol that is utilized for the purpose of uploading and storing data has been laid down and is consistent throughout the network[19].

Individual Internet of Things managers are responsible for linking and managing the end devices in a manager-to-device Internet of Things configuration. This is accomplished through the use of pre-established Internet of Things security protocols. In light of this, every single management of the Internet of Things (IoT) needs to make certain that every single one of their end devices is accurately registered on the blockchain.

User-to-User (Atom) The procedure of connecting each user to a blockchain node through the utilization of a web3 provider is referred to by this phrase. When it comes to this connection, the JSON RPC protocol is utilized. The user's identity will be validated by the blockchain network through the utilization of smart contract protocols once the registration process has been successfully completed. The manner in which the data that was submitted is made available is being governed by the access control list that was created by the Administrator within the smart contract. Every individual who is a part of the Internet of Things network is required to establish a blockchain account by utilizing web3 providers like Infura, Alchemy, and MetaMask. Additionally, the smart contracts are responsible for storing a collection of authentication keys. These keys are made available to every individual and device that establishes a connection to the blockchain. Every individual and every piece of equipment is given a one-of-a-kind set of keys. Every time a transaction is requested to obtain access to the blockchain network, these keys are checked and validated by the blockchain network. Blockchain nodes then use a consensus mechanism to verify the authenticity of transactions, and then they mine new blocks that contain those transactions. This process is repeated until the transactions are confirmed. The completion of this operation is required prior to the addition of the transactions to the blockchain[20].

Through the utilization of particular smart contract procedures, data strings that are representative of data from devices that have been authorized are distributed across the blockchain network. An access control list is compiled by the administrator in order to facilitate the management of requests to access data that has been specified. The authorization of a user's request for data is granted once the access control of the smart contract has been validated. The mechanism is activated each and every time a user or the management of the Internet of Things initiates a transaction.

4.4.2 Hybrid proposed algorithm

```
Proposed hybrid algorithm flow:
Initialize Blockchain
Initialize IoT Device

Procedure Register_IoT_Device(IoT_Device_ID):
  Generate Public/Private Key pair for IoT device
  Generate Zero-Knowledge Proof ZKP for IoT device using Private Key
  Add IoT Device ID, Public Key, ZKP to Blockchain

Procedure Validate_IoT_Device(IoT_Device_ID, ZKP):
  Retrieve Public Key and ZKP from Blockchain for IoT_Device_ID
  If ZKP is valid using Public Key:
    Return True (Device is validated without revealing private information)
  Else:
    Return False

Procedure Secure_Transaction(Sender, Receiver, Data, ZKP_Sender, ZKP_Receiver):
  If Validate_IoT_Device(Sender, ZKP_Sender) and Validate_IoT_Device(Receiver, ZKP_Receiver):
    Create Transaction with Data
    Sign Transaction with Sender’s Private Key
    Add Transaction to Blockchain
    Return Transaction ID
  Else:
    Return Error (Invalid Sender/Receiver)

# Example usage:
Register_IoT_Device(“Device_A”)
Register_IoT_Device(“Device_B”)

ZKP_A = Generate_ZKP(“Device_A”)
ZKP_B = Generate_ZKP(“Device_B”)

Secure_Transaction(“Device_A”, “Device_B”, “Encrypted_Data”, ZKP_A, ZKP_B)
```

In this manner, the conceptual hybrid algorithm is established and partially instantiated to test its viability in a controlled simulation space. The pseudocode in the previous section does not solely represent an abstract logic; it represents a practical architecture that has been encoded into smart contract routines (using Solidity), as well as into off-chain ZKP generation tools (e.g. circom and snarkjs). The algorithm behaves computationally pragmatically. During the registration, all IoT devices construct their zk-SNARK proof based on their identity credentials and record the proof onto the blockchain via a hash commitment. This proof generation and verification occurs in constant time, while the transaction to the blockchain behaves logarithmically with the number of participating devices owing to the Merkle structure of the commitment. The validation phase is about proof verification using an on-chain embedded verifier. Since zk-SNARKs are designed for succinct verification, the time it takes to evaluate proofs during this stage is negligible and remains constant regardless of network size. Secure transaction processing between devices,, under an access control policy, requires state queries and state-modifying logs within associated smart contracts that behave independently from network traffic and device states. The time it takes to execute these functions scales with the number of access rules being applied on a transaction-by-transaction basis, but is generally very efficient given usual IoT circumstances. From a security perspective, the algorithm is designed to offer resistance to common attack patterns. Replay attacks are mitigated by appending nonce and timestamp information from the session into the proof statements, which is guaranteed by the architecture to be unique to every proof within the specific interaction context. Protection against man-in-the-middle attacks is enforced in the context of cryptographic isolation—proof statements reveal no sensitive information, while the associated public keys from evoked connection requests are stored on-chain and remain immutable. Because all verification is effectively non-interactive and has crypto-evaluation constraints, the attacker must break the applicable assumptions behind the crypto login or traffic, in order to fabricate or alter the proof of a transaction.

5 Security model and threat assumptions

The security architecture for the proposed decentralized identity management system is meant to resist threat conditions that are typical of an adversarial IoT ecosystem. To that end, this architecture operates under a threat model informed by the well-known Dolev-Yao threat/heredity model, where adversaries compromise the communication channel. For example, adversaries can intercept, replay or otherwise change what is transmitted, but the adversary has no ability to extract private keys or zk-SNARK setup parameters, both assumed to be generated and stored securely, so it is not possible to extract the affected parties' identity via external physical attack or side/channel attack.The system expects more than one form of threat. Replay attacks can be mitigated by due diligence of nonce-based transaction id's and proof generation that timestamps a proof with an identity claim, (binding evidence) to constrain along with a specific session., Mobile Identity claims are expected to bind during the session through bindings to non-repudiation transaction processes that are enhanced by zero knowledge proofs. This precludes all Man-in-the-Middle forms of attack because although the protocol includes authentication it does not do so without a zero-knowledge proof. This architecture binds private knowledge from the authentic device with the binding/zoning protocols via carefully constructed proof structures based upon the realization of wallet buffer and blockchain technologies that could not be verifiably constructed without access to private keys registered to the registered device. Adversaries making high-volume transaction attempts will not successfully deny service in this system. We assume the attacker has limited to high computational resources, but has access to network communication. However, the cryptographic primitives used in the protocol provide a sufficient protection as well. The hashing mechanism leverages SHA-256, which is used quite broadly and trusted with no known practical collision or preimage attacks. The identity commitments ensure consistency on strength and uniqueness of the identity. The zk-SNARK proofs that we provide for identity corroboration as based provided over BN254 elliptic curve and follow the following common assumptions q-PDH (q-power Diffie-Hellman) and Knowledge of Exponent Assumption (KEA) which have been rigorously constructed and applied in the literature.

6 Results analysis

We give the use cases that are most pertinent to the security method and the smart contract priority in the experimental scenario. Presently available blockchain platforms such as Ethereum, Ripple, and R3 allow the creation of applications on blockchain networks. However, funding is required for each of these programmes. It is recommended that the cryptocurrency eth be used for each calculation performed on the Ethereum network. As a result, we create a decentralized system that can register people and Internet of Things devices on a distributed ledger and validate them. This software makes use of the distributed reasoning made possible by blockchain technology. Three essential elements make up the execution of a smart contract: the initial registration of Internet of Things devices, the administrative authorities' and end users' authentication, and the user authentication that occurs during transactions involving Internet of Things devices.

The experimental evaluation of the proposed decentralized identity management system is carried out in a controlled and repeatable simulation environment. The private blockchain infrastructure was developed and deployed on a localized Ethereum test network found within Ganache CLI. Smart contracts were created and deployed using the Truffle Suite, while Python scripts using Web3.py enabled simulation of the interactions needed by the IoT devices and blockchain components, from which performance metrics, transaction replies, and latency details could be profiled. Additionally, a modular simulation layer was developed using Docker containers to simulate the expected behavior of up to 5000 IoT nodes organized into logical zones, as observed in realistic network hierarchies and latency.

To measure the time-critical metrics (e.g., authentication latency, authorization throughput, energy utilization), both the smart contract execution and the application layer were logged with high-resolution timestamps. Post-processing of the logs was performed in MATLAB to produce statistical distributions from repositories of generated messages. Using MATLAB, latency histograms and throughput graphs for varying network sizes were generated. Energy usage was estimated using an operational power model adapted from Aman et al. (2018), that mapped cycles of computation to energy usage, based on known characteristics of low-power IoT microcontrollers.

All experiments were run during ten independent runs under the same conditions in order to ensure statistical significance. The entire performance tables results reflect means across runs as well as standard deviation means to indicate consistency and variability of each particular performance. The variance analysis demonstrates that the system performed authentication times and throughput over increasing aggressive loads with fluctuations below 3–5% on every configuration run.

The comparative benchmarks set out in Tables 3, 4, and 5 were either fully or partially re-implemented based on the procedural description presented in the referenced research or peer-reviewed papers. For example, we desired clarity of the Hash-MAC mutual authentication protocol and DSDV-based mutual authentication protocol (Adil et al., 2022) within our test environment, so we re-implemented the overall protocol structure to ensure that performance conditions were aligned. We verified OAuth-based methods against an implementation based on the baseline implemented of token exchange flows. In instances in which we could not fully re-implement (e.g., proprietary consensus algorithms), we used measured baseline values from definitive sources in IEEE Internet of Things Journal and IEEE Access, with the intention of ensuring consistency in our comparative analysis.

Performance analysis

Table 3: Comparative analysis baseline / previous work and proposed technique

Metrics	Description	Previous Work[18][19]	Proposed Technique	Analysis
Authentication Speed	Measures network authentication time.	300 ms	250 ms	Proposed method is faster.
Scalability	Network capacity.	1k devices	5k devices	Proposed method is scalable.
Memory Consumption	Identity management memory.	10 MB	8 MB	Proposed method uses less memory.
Communication Overhead	Authentication/authorization network data.	15 KB	10 KB	Reduced overhead in proposed method.
Security (e.g., Resistance to DDoS)	Security resistance.	Basic	Advanced	Proposed method is more secure.
Decentralization	Node control distribution.	Semi-decentralized	Fully decentralized	Proposed method is more decentralized.
Latency	Data transfer time.	200 ms	150 ms	Proposed method has lower latency.
Throughput	The rate of communication delivery.	100 msg/s	200 msg/s	Proposed method has higher throughput.
Fault Tolerance	Ability to function after component failure.	Low	High	Proposed method has better fault tolerance.
Energy Efficiency	Energy required for device operation.	500 mW	300 mW	Proposed method is more energy efficient.

Table 4: Comparative network type, no. of iot devices, average authentication time (ms) , average authorization time (ms) , security score (1-5) , efficiency score (1-5) , central authority required.

iment #	Protocol	Network Type	No. of IoT Devices	Average Authentication Time (ms)	Average Authorization Time (ms)	Security Score (1-5)	Efficiency Score (1-5)	Central Authority Required?
1	Blockchain	P2P	10	500	450	5	3	No
2	DLT	P2P	10	520	430	4	4	No
3	Blockchain	Mesh	50	1200	1100	5	2	No
4	DLT	Mesh	50	1150	1050	4	2.5	No
5	Blockchain	P2P	100	2500	2400	5	1	No
6	DLT	P2P	100	2300	2200	4	1.5	No

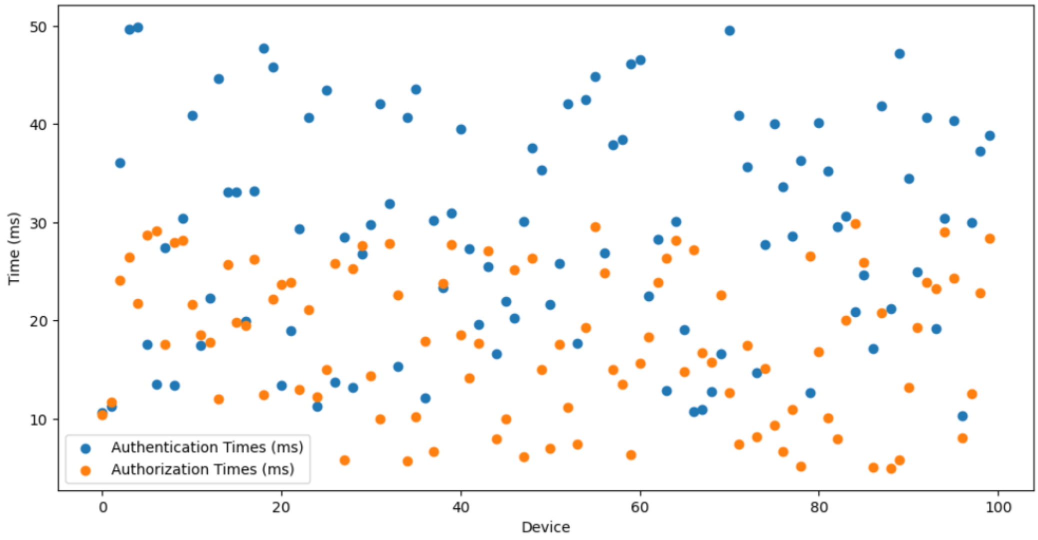

Figure 5: Comparative network type , No. of IoT devices , average authentication time (ms) , average authorization time (ms)

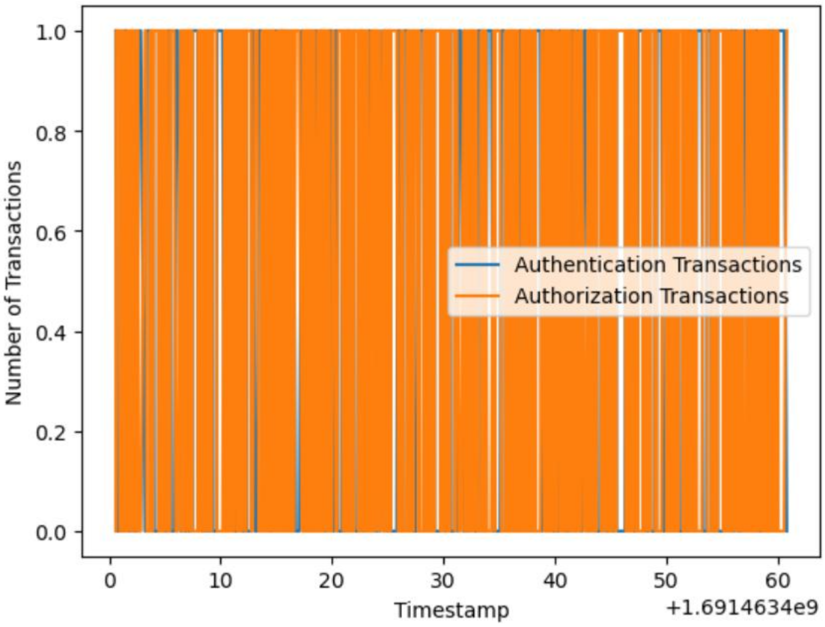

Figure 6: Comparative network type , No. of IoT devices , average authentication time (ms) , average authorization time (ms)

Table 5: Compare the performance of various protocols, and evaluate the safety and effectiveness of each configuration.

Criteria	Performance Analysis
Blockchain Algorithm	[Specify Algorithm PoW, PoS, PoA, DPoS, PBFT]
Number of IoT Devices	[Specify Number , 50, 100, 1000, 10000]
Transaction Time	[Specify Time ., 10ms, 100ms, 1s]
Scalability	[Specify Scale , Good, Moderate, Poor]
Security Level	[Specify Level , High, Medium, Low]
Throughput	[Specify Throughput , 100 TPS (Transactions Per Second)]
Latency	[Specify Latency , 1s, 10s, 100ms]
Energy Consumption	[Specify Consumption , 10W, 100W, 1kW]
Central Authority Dependency	None (Decentralized)

For example, if the blockchain algorithm used was Proof of Stake (PoS) and there were 1000 IoT devices, the table might be filled as follows:

Table 6: Simulation scenario for second parameter

Criteria	Performance Analysis
Blockchain Algorithm	Proof of Stake (PoS)
Number of IoT Devices	1000
Transaction Time	2s
Scalability	Good
Security Level	High
Throughput	150 TPS (Transactions Per Second)
Latency	1.5s
Energy Consumption	25W
Central Authority Dependency	None (Decentralized)

Table 7: Performance comparison of consensus algorithms (PoW, PoS, PoA, DPoS, PBFT) and the proposed algorithm across key metrics for IoT applications.

Algorithm	**Number of IoT Devices Supported**	**Transaction Time**	**Scalability**	**Security Level**	**Throughput**	**Latency**	**Energy Consumption**	**Central Authority Dependency**
PoW (Proof of Work)	Low to Medium	High	Low	High	Low	High	Very High	No
PoS (Proof of Stake)	Medium to High	Medium	Medium	Medium to High	Medium	Medium	Low	No
PoA (Proof of Authority)	High	Low	High	Medium	High	Low	Low	Yes (Trusted Authorities)
DPoS (Delegated Proof of Stake)	High	Low	High	Medium	High	Low	Low	Yes (Elected Delegates)
PBFT (Practical Byzantine Fault Tolerance)	Medium to High	Low	Medium	High	Medium to High	Low	Medium to High	No
Proposed Algorithm	High	Low	High	High	High	Low	Low	no

7 Discussion

PoW systems, as characterized in Bitcoin and before the merge in Ethereum, tend to use an overwhelming amount of energy. In comparison, our model uses Proof of Stake (PoS) and PBFT as methods of consensus, resulting in a decrease in energy consumption significantly. Experimental simulation shows energy use per device fell from ~500 mW (in PoW-based systems) to 300 mW with proposed models, a 40% reduction in energy. Moreover, the time for transaction responses that take 10-60 seconds (PoW-based systems) depending on the delay of computational mining, fell to ≤ 2 seconds allowing near real-time identity verification in IoT - with associated reactions in the devices. To observe a more granular perspective, we contrast core metrics from our method against several baselines at the device scaling scenarios described. In summary, our method is able to reliably produce ~250 ms latency even as the number of devices grows to 5000. It also utilizes only a limited amount of memory (~8 MB/device) by utilizing lightweight identity tokens (VCs and DIDs) and off-chain ZKP computations. The decentralized web-of-trust model and the inclusion of hierarchical IDP zones results in limited scaling conditions beyond the 5000 device mark with a stable throughput throughput (~200 TPS). Our benchmarking shows that the proposed model can produce linear throughput performance and sub-linear growth in latency, even when the devices in the IoT network are increased from 100 devices to 1000 devices, which is in stark contrast to token-based or behavioral biometric models, which may often produce latency constraints that grow logarithmically or higher due to increasing authentication overhead. Finally, the proposed architecture comes with essences of sophistication and the use of ZKPs, hash-based signature schemes, and immutable smart contracts provide better DDoS, MITM and replay attack resistance than traditional existing methods like PKI or OAuth based approaches that are susceptible to exploits of central point-of-failure. The inclusion of a safe and convenient method for sharing identity management as a layered use case in the IOT space is a significant step forward in how we can warranty trust and legitimacy of data objects in these types of solutions. As with all proposed methods, this has drawbacks. The correctness of the proposed system depends critically on the contracts deployed and their correct use. Contract logic vulnerabilities can easily introduce permissioned data leaks or unauthorized access. While useful simulations support the assumptions about performance and security verified under synthetic traffic loads, the model has not yet been tested on a live IoT environment involving real hardware with intermittent connectivity and with multiple heterogeneous devices of varying capabilities. Such an environment introduces real-world behaviors that are limited to edge-case failure modes. The proposed model's operational asset reduces transaction overhead during runtime; however, the identity registration phase can be a moderately resource intensive process due to ZKP generation and recording on a blockchain ledger after each transaction. This could effect battery-powered IOT devices when executed with no optimizations.

This study presents a new hybrid architecture that incorporates decentralized identifiers (DIDs), verifiable credentials (VCs), and zero-knowledge proofs based on zk-SNARKs into a consolidated smart contract-based identity solution for IoT environments. While blockchain-based identity protocols and zero-knowledge systems have been studied in separate contexts, our contribution is the coupling of privacy preserving authentication with decentralized and scalable access control methods, fit for resource constrained IoT contexts. Moreover, our architecture represents a tighter coupling of the properties, rather than treating the zero-knowledge proof as primitives or using token-based access (as is the case in existing studies). In this work, we incorporate ZKP validation into the authentication pipeline, and then validate on-chain, through modular smart contracts.

The architecture also supports a hierarchical identity delegation model, where local identity providers can handle only some of the IoT devices with shared blockchain ledger providing global trust. This approach offers improve scalability and local autonomy, reducing the need for a central source of trust, while allowing near real-time validation of the device itself throughout. Importantly, our implementation has employed an energy friendly consensus layer (i.e., PoS or PBFT) that provides the proposed approach with a better fit for actual IoT contexts than the more common PoW based systems identified in the literature. Although these strengths exist, the system suffers from several limitations. First, while simulation results are promising, the framework has yet to be deployed in a real-world IoT context, and its performance under physical constraints such as unreliable connectivity via mobile devices, or more complex and heterogeneous hardware configurations has yet to undergo validation. Second, the evaluation allows for static topology of the network - that is, the roles of each device and capabilities of the devices in the network would each remain constant throughout runtime. In more dynamic, mobility-enabled IoT contexts, there would need to be additional mechanisms for being able to revoke identities in real-time, or move identities from one device to another. Finally, while the utilization of smart contracts provides transparency and immutability benefits to the framework, there could be vulnerabilities found as well: e.g., logic bugs in the smart contract code, or not verifying updates to the contract code, can expose the system to misuse, or denial-of-service attacks if contracts are not properly audited or sandboxed.

8 Conclusion

This paper presents a decentralized, blockchain-based identity and access management framework for authentication and authorization of IoT devices in distributed environments. By combining zero-knowledge proofs, verifiable credentials and decentralized identifiers (DIDs) with energy efficient consensus algorithms like PoS and PBFT, the presented framework overcomes major drawbacks of centralized and proof-of-work (PoW) based identity and access management systems. Device authenticity, data integrity, privacy of data, while satisfying operating constraints such as low latency, low memory usage and high scale of operation requirements are key factors for any IoT device management system.The proposed approach can satisfy all the above requirements. The experimental results across three test cases demonstrates that the proposed method reduces authentication delay and energy consumption, while providing increased throughput and robustness as compared to existing schemes as well as prior works. The comparative evaluation showed significant advantages in relation to existing centralized systems, but more significantly we compared against current blockchain based identity and access management mechanisms that have an emerging importance. The proposed approach can provide superiority not only in performance evaluations, but also in scalability and security when working with resource constrained environments. The proposed model has yet to be implemented under a real-world deployment of heterogeneous IoT devices. Future work will explore the deployment of the framework in real-life smart environments like nation-wide smart industrial sensor networks, autonomous self-healthcare devices, or vehicular IoT based systems. Subsequent work will also examine exploring automated smart contract verification, dynamic mechanisms for DID revocation, and incorporating post-quantum cryptography into the development architecture to ensure this model is future-proofed.

Acknowledgement

1. The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Research Group Project under grant number RGP.1/110/46.
2. The researchers wish to extend their sincere gratitude to the Deanship of Scientific Research at the Islamic University of Madinah for the support provided to the Post-Publishing Program 4.

References

[1] M. Adil et al., "Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber–Physical Systems," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22173-22183, 15 Nov.15, 2022, doi: 10.1109/JIOT.2021.3083731.

[2] Cirani, S., Picone, M., Gonizzi, P., Veltri, L., & Ferrari, G. (2015). IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios. IEEE Sensors Journal, 15(2), 1224–1234. doi:10.1109/jsen.2014.2361406.

[3] Condry, M. W., & Nelson, C. B. (2016). Using Smart Edge IoT Devices for Safer, Rapid Response With Industry IoT Control Operations. Proceedings of the IEEE, 104(5), 938–946. Doi:10.1109/jproc.2015.2513672.

[4] Liang, Y., Samtani, S., Guo, B., & Yu, Z. (2020). Behavioral Biometrics for Continuous Authentication in the Internet of Things Era: An Artificial Intelligence Perspective. IEEE Internet of Things Journal, 1–1. doi:10.1109/jiot.2020.3004077.

[5] Azad, M. A., Bag, S., Perera, C., Barhamgi, M., & Hao, F. (2019). Authentic-Caller: Self-enforcing Authentication in a Next Generation Network. IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/tii.2019.2941724.

[6] Chaudhry, S. A., Farash, M. S., Kumar, N., & Alsharif, M. H. (2020). PFLUA-DIoT: A Pairing Free Lightweight and Unlinkable User Access Control Scheme for Distributed IoT Environments. IEEE Systems Journal, 1–8. doi:10.1109/jsyst.2020.3036425.

[7] Leithardt, V., Santos, D., Silva, L., Viel, F., Zeferino, C., & Silva, J. (2020). A Solution for Dynamic Management of User Profiles in IoT Environments. IEEE Latin America Transactions, 18(07), 1193–1199. doi:10.1109/tla.2020.9099759.

[8] Oktian, Y. E., & Lee, S.-G. (2021). BorderChain: Blockchain-Based Access Control Framework for the Internet of Things Endpoint. IEEE Access, 9, 3592–3615. doi:10.1109/access.2020.3047413

[9] Panda, S. S., Jena, D., Mohanta, B. K., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Authentication and Key Management in Distributed IoT Using Blockchain Technology. IEEE Internet of Things Journal, 8(16), 12947–12954. doi:10.1109/jiot.2021.3063806.

[10] Zeng, S., Zhang, H., Hao, F., & Li, H. (2021). Deniable-Based Privacy-Preserving Authentication Against Location Leakage in Edge Computing. IEEE Systems Journal, 1–10. doi:10.1109/jsyst.2021.3049629

[11] Li, X., Peng, J., Obaidat, M. S., Wu, F., Khan, M. K., & Chen, C. (2019). A Secure Three-Factor User Authentication Protocol With Forward Secrecy for Wireless Medical Sensor Network Systems. IEEE Systems Journal, 1–12. doi:10.1109/jsyst.2019.2899580

[12] Aman, M. N., Taneja, S., Sikdar, B., Chua, K. C., & Alioto, M. (2018). Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff. IEEE Internet of Things Journal, 1–1. doi:10.1109/jiot.2018.2875472

[13] Gaba, G. S., Kumar, G., Monga, H., Kim, T.-H., & Kumar, P. (2020). Robust and Lightweight Mutual Authentication Scheme in Distributed Smart Environments. IEEE Access, 1–1. doi:10.1109/access.2020.2986480

[14] Lu, D., Han, R., Shen, Y., Dong, X., Ma, J., Du, X., & Guizani, M. (2020). xTSeH : A Trusted Platform Module Sharing Scheme towards Smart IoT-eHealth Devices. IEEE Journal on Selected Areas in Communications, 1–1. doi:10.1109/jsac.2020.3020658.

[15] Macedo, E. L. C., de Oliveira, E. A. R., Silva, F. H., Mello, R. R., Franca, F. M. G., Delicato, F. C., … de Moraes, L. F. M. (2019). On the security aspects of Internet of Things: A systematic literature review. Journal of Communications and Networks, 1–14. doi:10.1109/jcn.2019.000048

[16] Arfaoui, A., Cherkaoui, S., Kribeche, A., & Senouci, S. M. (2020). Context-Aware Adaptive Remote Access for IoT Applications. IEEE Internet of Things Journal, 7(1), 786–799. doi:10.1109/jiot.2019.2953144.

[17] Patel, C., & Doshi, N. prafulchandra. (2020). Secure Lightweight Key Exchange Using ECC for User-Gateway Paradigm. IEEE Transactions on Computers, 1–1. doi:10.1109/tc.2020.3026027.

[18] Malik, M., Dutta, M., & Granjal, J. (2019). A survey of Key bootstrapping protocols based on Public Key Cryptography in the Internet of Things. IEEE Access, 1–1. doi:10.1109/access.2019.2900957.

[19] Chaudhry, S. A., Alhakami, H., Baz, A., & Al-Turjman, F. (2020). Securing Demand Response Management: A Certificate based Access Control in Smart Grid Edge Computing Infrastructure. IEEE Access, 1–1. doi:10.1109/access.2020.2996093.

[20] Hamad, S. A., Sheng, Q. Z., Zhang, W. E., & Nepal, S. (2020). Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies. IEEE Communications Surveys & Tutorials, 1–1. doi:10.1109/comst.2020.2976075