A Hybrid Blockchain-Based Approach for Secure and Efficient IoT Identity Management

Abdulaleem Ali Almazroi[1], Nouf Atiahallah Alghanmi[2]
[1]aaealmazrouy@kau.edu.sa [2]naalganmy@kau.edu.sa
[1]Department of Information Technology, Faculty of Computing and Information Technology in Rabigh
King Abdulaziz University, Rabigh, 21911, Saudi Arabia
[2]Department of Information Technology, Faculty of Computing and Information Technology in Rabigh
King Abdulaziz University, Rabigh, 21911, Saudi Arabia

Abstract
The proliferation of IoT devices has presented an unprecedented challenge in managing device identities securely and efficiently. In this paper, we introduce an innovative Hybrid Blockchain-Based Approach for IoT Identity Management that prioritizes both security and efficiency. Our hybrid solution, strategically combines the advantages of direct and indirect connections, yielding exceptional performance. This approach delivers reduced latency, optimized network utilization, and energy efficiency by leveraging local cluster interactions for routine tasks while resorting to indirect blockchain connections for critical processes. This paper presents a comprehensive solution to the complex challenges associated with IoT identity management. Our Hybrid Blockchain-Based Approach sets a new benchmark for secure and efficient identity management within IoT ecosystems, arising from the synergy between direct and indirect connections. This serves as a foundational framework for future endeavors, including optimization strategies, scalability enhancements, and the integration of advanced encryption methodologies. In conclusion, this paper underscores the importance of tailored strategies in shaping the future of IoT identity management through innovative blockchain integration.

Keywords:
IoT Identity Management, Hybrid Blockchain, Secure IoT, Efficient Identity Management, Implementation, Average Latency, Energy Efficiency

1. Introduction

The rapid and substantial increase in Internet of Things (IoT) devices in recent times has led in a transformative era in our perception of the physical world. This technological wave has enabled the realization of smart cities, streamlined industrial automation, empowered healthcare monitoring, and enhanced environmental sensing capabilities, among various other applications [1]. However, alongside the promising advancements, the comprehensive management of IoT device identities has emerged as a critical challenge in the wake of this IoT proliferation. Conventional identity management systems, which have proven effective in traditional digital environments, have fallen short in meeting the unique demands of the IoT ecosystem [2]. The IoT landscape is characterized by unparalleled scale, device heterogeneity, and dynamic nature, making it necessary to seek innovative approaches that can simultaneously ensure security and efficiency. Blockchain technology, renowned for its inherent attributes of transparency, immutability, and decentralized consensus, holds substantial promise for addressing the complexities of IoT identity management [3,4]. This study presents a novel approach to tackle the pressing issue of IoT identity management through the integration of blockchain technology and complementary strategies. This approach lays the foundation for a more secure and efficient IoT ecosystem.

The study encompasses the entire lifecycle of this approach, from conceptualization to Model development and thorough performance analysis of the proposed Hybrid Blockchain-Based IoT Identity Management (HB-IIM) method. The rapid expansion of the IoT market is evidenced by the prediction that the number of IoT-connected devices will triple between 2018 and 2023 [5]. This growth trajectory is poised to accelerate further, driven by ongoing advancements in computing power, sensor technologies, the impending advent of 5G networks, and increased investor interest [6]. Given the mobile and widely distributed nature of IoT devices, coupled with the growing emphasis on data security, the need for a robust device identification mechanism becomes primary [7]. Furthermore, in the era of big data, artificial intelligence and machine learning the value of data has raised. IoT-connected devices, which are ubiquitously deployed, generate invaluable sensor data that can be monetized through third-party transactions. To instill trust in these transactions, it is essential to verify the authenticity of data sources to prevent fraudulent activities [8]. Much like the Know Your Customer (KYC) databases that authenticate individuals, a Know Your Device (KYD) platform for IoT-connected devices can offer the reliability sought in data transactions. Ultimately, the overarching objective is to establish a decentralized marketplace for data generated by IoT-connected devices. To realize this vision, it is essential to ensure the reliable identification of IoT devices. This study envisions the KYD platform issuing certifications to smart contracts representing these devices,

Manuscript received April 5, 2024
Manuscript revised April 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.4.2

attesting to their identity. Furthermore, it explores the linkage of devices to smart contracts representing their owners, thereby extending the identity verification process to individuals through KYC platforms. This approach has the potential to significantly enhance trust between buyers and IoT devices in the decentralized marketplace, as devices become verified entities associated with real-world individuals, thereby increasing accountability. The KYD platform, integral to this endeavor, will incorporate a user-friendly web interface for user and device registration, facilitating seamless and secure on boarding of IoT devices into the ecosystem.

A. Objective:

The fundamental aim of this paper is to conceive, develop, and evaluate a Hybrid Blockchain-Based Approach for Secure and Efficient IoT Identity Management (HB-IIM). The specific aims of the paper include:

- Design: Proposing a comprehensive architectural framework that combines block chain technology with complementary approaches, creating a hybrid system that addresses the shortcomings of traditional IoT identity management solutions.
- Prototypical Implementation: Developing a functional Model of the HB-IIM approach, which serves as a tangible representation of the proposed solution. This Model showcases the practical feasibility of the hybrid approach in real-world scenarios.
- Performance Assessment: Rigorously evaluating the performance of the HB-IIM approach under diverse conditions, including scalability, efficiency, security, and usability. This evaluation sheds light on the feasibility and effectiveness of the suggested approach in addressing the requirements of IoT identity management.

The article is organized into several sections, each of which possesses a distinct emphasis and contribution. In the first section, the issues associated with safely and efficiently managing the identities of IoT devices are introduced, and the objectives and contributions of our research are outlined. Second section presents a comprehensive examination of current identity management solutions within the realm of the Internet of Things (IoT). This section offers an overview of these solutions and conducts a thorough analysis of their respective merits and limitations. In third, fourth and fifth sections, an exposition is provided in the design aspect and components for the Hybrid Blockchain-Based Approach for Secure and Efficient IoT Identity Management. Additionally, we delve into the technical intricacies of implementing our proposed approach, alongside presenting the performance measurements. The sixth and seventh sections presented the simulation setup and an interpretation of the evaluation result. Finally, the conclusion of the paper is provided in section eight.

2. Related Work

The concept of employing hybrid blockchains for the identification or authentication of IoT-connected devices was first put forward in 2017 by [9], who suggested an identity-based cryptographic system. This system was designed to facilitate secure authentication and message encryption among IoT-connected devices, utilizing hybrid blockchains for key generation. They contended that, given the limited resources typical of IoT-connected devices and their inherent characteristics for deployment in potentially hostile environments, traditional cryptographic algorithms were not feasible for the IoT use case, as mentioned in [10]. Hybrid block chains being a naturally lightweight alternative to produce unique keys to use for encryption of messages and identification of devices promised a better solution. The proposed protocol first has devices in an IoT environment go through an enrolment procedure. Each data node, e.g. an IoT-connected device, saves its hybrid blockchain derived CRP data on a database hosted by a server node in the IoT network. Subsequently, when two devices in the network intend to interact, the server node commences the process by authenticating them, ensuring that the data from the recently created hybrid blockchains corresponds with the Challenge-Response Pairs (CRPs) in the database. If the devices pass the authentication, the server node will aid in creating public and private keys for the devices, as well as securely distributing them to the other device. From then on, the devices can communicate securely using their key to encrypt and decrypt each other's messages [11]. Note that this approach does not utilize block chain technology. A similar approach that combines these principals with the Ethereum block chain will be covered shortly.

Block chains have been gaining in significance similarly to the IoT ever since the infamous Bitcoin whitepaper was published in 2008 [12]. Block chains are essentially digital ledgers that are maintained simultaneously by a distributed network of computer nodes. Information gets added to the chain in blocks, which are linked to their preceding block through hashed data. The block chain is kept in sync throughout the network using a consensus mechanism. Ethereum, for example, uses a consensus mechanism called Proof-of-Work. It requires the nodes wishing to add a block to the chain to compete on solving a mathematical puzzle. To add a block that does not abide by the consensus rules, a malicious party would need to control nodes more computationally powerful than 51% of the

network. As this is practically impossible if the network is sufficiently large and distribute, block chains are generally regarded as immutable. Many applications have been brought up besides cryptocurrencies to provide solutions that use these immutable ledgers to ensure trust between two parties, without the need for a trusted third party. Using this technology in IoT devices is therefore subject to much research, as it allows IoT-connected devices to transact with each other without going through third parties [13]. Security, scalability, performance, and interoperability are key factors in the architectural design of blockchain-based IoT systems. A multifaceted strategy is required to strengthen security, including the use of smart contracts for automated and secure business logic execution, strong identity management to verify IoT devices, and encryption of sensitive data stored on the blockchain. Adopting consensus techniques designed for the Internet of Things (IoT), such as Practical Byzantine Fault Tolerance (PBFT) or Proof of Stake (PoS), can skillfully strike a balance between security and scalability, promoting quick transaction validation without put at risk system integrity. In order to handle the flow of IoT devices and data, scalability is essential; this can be accomplished through strategies like sharding or sidechains, which divide the workload and improve throughput. Additionally, using off-chain processing for non-critical computations can reduce traffic on the primary blockchain and improve system performance as a whole according to [14].

A fundamental building block of the Internet of Things, interoperability enables easy communication between various IoT systems and devices. By choosing blockchain protocols and standards that encourage interoperability, a cohesive ecosystem is ensured, and collaboration between various technologies is made easier according to [15]. This feature is further improved by cross-chain communication protocols, which allow communication between several blockchain networks. Transaction batching, which places an emphasis on performance, can be used to lower transaction overhead costs and improve energy efficiency, making the system more sustainable. Security audits are essential for regularly identifying weaknesses in the system's architecture and smart contracts and reinforcing it against prospective threats. Blockchain-based IoT systems can unify security, scalability, performance, and interoperability by fully integrating these techniques, providing a solid framework for the subsequent wave of networked technologies as depicted in Figure 1.

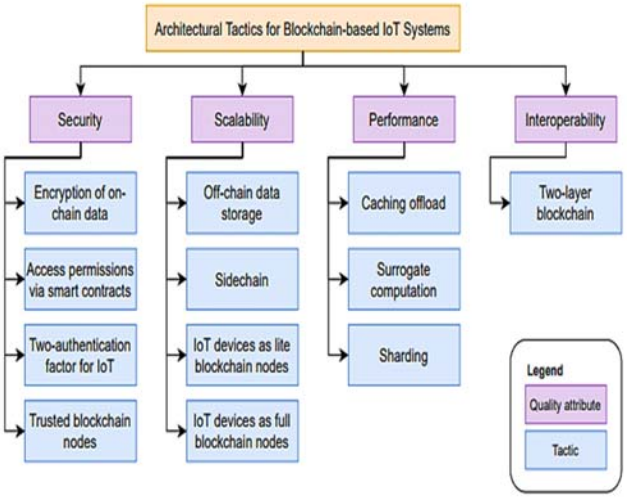

Fig. 1. Framework of architectural tactics for blockchain based IoT device management system.

One of the earliest research papers to combine all three aspects was [16]. They proposed an authentication scheme in 2018 that utilized hybrid block chains to generate digital fingerprints. Their proposed scheme has revealed both a global block chain being used for tracing and authenticating devices, as well as a locally permission block chain to authenticate devices within a local network periodically. The goal of the second block chain is to address threats based on devices becoming compromised after some time of being registered within the IoT infrastructure. E.g. the scenario of a malicious party within the network replacing an authentic device with a cloned imposter device. As a part of their work [17], they also proposed a secure communication protocol to facilitate the regular authentication of devices within the IoT infrastructure. An efficient method to improve security and data privacy in blockchain-based systems is to implement on-chain data encryption in Internet of Things devices and manage it through a stand-in device to handle encryption keys. In this method, the encryption and decryption operations are transferred from IoT devices to a stand-in device, which is typically a hardware module or secure enclave. Sensitive data is protected both at rest and during transmission thanks to this device's secure key generation, storage, and management processes.

The blockchain system is given the capacity to transparently safeguard data records within transactions by adding on-chain data encryption as shown in Figure 2. An IoT device to encrypt data before it is sent to be stored on the blockchain by the IoT device uses an encryption key from the stand-in device as mentioned in [18]. The encrypted data is then sent to the blockchain network, guaranteeing that even in the event of a breach, the attacker would only be able to access encrypted data, rendering it useless without the

accompanying decryption keys, comparable to the design proposed in this paper.

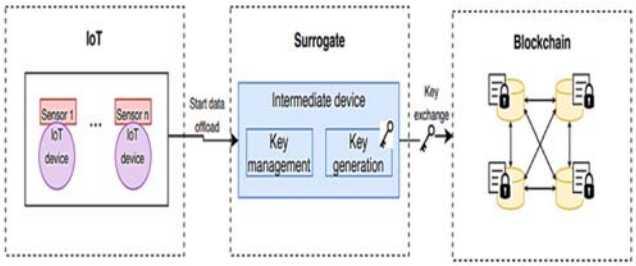

Fig. 2. On-chain data encryption using a stand-in device to manage the encryption key in IoT devices.

A solid base for safe and effective IoT ecosystems can be provided by a "trusted blockchain" architecture that uses substitutes to enable trusted IoT zones. "Trusted IoT zones" are parts of the IoT network that have been specifically recognized as secure and reliable for devices and data. In this architecture, the essential infrastructure that guarantees the immutability, transparency, and integrity of data created by IoT devices is the trusted blockchain as stated in [19]. Encryption, consensus mechanisms, and smart contracts are just a few of the security precautions that the blockchain network imposes to guarantee the validity and correctness of data stored on the blockchain as shown in Figure 3.

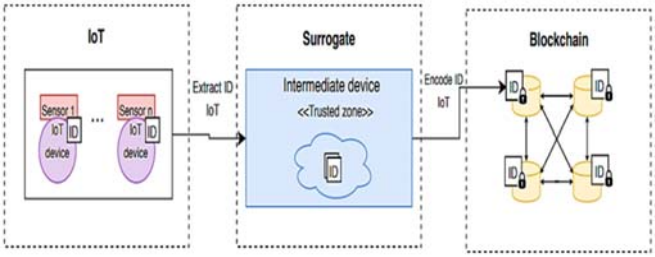

Fig. 3. Surrogate-supported, trusted blockchain environments for IoT devices.

The architecture might operate as follows:

- The creation of trusted IoT zones designates specific locations within the IoT network as trusted IoT zones. These areas may include vital infrastructure, private data sources, or equipment requiring higher security levels.
- Surrogate Deployment: Within the secure IoT zones, substitutes are strategically placed. To enable secure data processing and encryption, these devices come with security features like hardware security modules (HSMs) or trusted execution environments (TEEs).
- IoT devices within trusted zones collect and transfer data to the appropriate surrogates after validating it. To assure the data's validity and integrity, the surrogates process and validate it.
- Data that has been confirmed is securely encrypted by surrogates using encryption keys that are kept in the trustworthy zone. Before accepting data, IoT devices must first prove their identity via authentication procedures.
- Interaction with the blockchain: Once the data is encrypted and verified, the surrogates interact with the reliable blockchain. To maintain the blockchain's integrity, these surrogates initiate transactions that store the encrypted data within the blockchain.
- Smart Contracts and Consensus: The reliable blockchain uses consensus techniques to verify the transactions. Processes like access control or data sharing agreements can be automated with smart contracts, assuring the safe implementation of established logic.
- Authorized parties have access to the blockchain's encrypted data, which they may then decode and evaluate using the relevant surrogates inside the trusted zones.

Also in 2018, [20, 21] proposed a framework that combined hybrid blockchain with Ethereum smart contracts for the assurance of data provenance and the maintenance of data integrity within IoT environments. Their approach focuses more on the authentication of transactions within the network and thus focuses more on device-authentication, whereas, according to [22], the design outlined in this paper primarily concentrates on the reliable identification of IoT devices. These authentications work as follows in their proposed design. Deployed smart contracts that serve as trusted servers manage authentications. Then, in order to register themselves, devices broadcast the CRP from the implementation of their hybrid block chains to this contract. The server contract starts a verification procedure when authentication is required because of transactions made by the device. The server encrypts a generated nonce using the hybrid block chains key for the device and sends it to the device as stated in [23, 24]. The device then proves its identity by decrypting the nonce and returning it alongside more hashed data. The hash is subsequently sent back to the server which verifies it and approves the transaction or declines it. In short, the proposed design uses smart contracts and hybrid block chains to authenticate transactions based on traditional public-key cryptography techniques. Notice that this approach is executed entirely by the device owner himself, while our approach has a trusted third party, the KYD platform, verify the device's identity. As will be mentioned later, however, the design proposed in [25] could

complement our design to add hybrid blockchains-based authentications to the identification-focused design.

3. Design Aspect and Components

The design and model implementation of the Hybrid Blockchain-Based Approach for Secure and Efficient IoT Identity Management (HB-IIM) involve a particularly crafted architecture that integrates block chain technology with complementary techniques to address the challenges inherent in managing the identities of IoT devices. This section explores further into the rationale behind the proposed HB-IIM solution as well as its actual implementation. The blueprint for a mixed-blockchain method of IoT identity management security and efficiency.

A. Web Application:

It allows users to access the application features and services from anywhere with an internet connection. Web apps are helpful and flexible because they can be accessed from any device with an internet browser. An intuitive and engaging interface is provided for users to carry out tasks, have access to information, and control data. Online shopping, social media, productivity software, and managing Internet of Things devices are just some of the many prevalent uses for web applications.

B. Server:

The server makes available its services, resources, or data across the network. From providing web pages to processing data and running computations, servers handle and respond to a wide variety of client requests. Servers are crucial components of web applications because they process user requests, run program logic, and communicate with other systems such as databases and third-party services. Connecting the front end (user interface) to the back end (databases, APIs, etc.), they guarantee a smooth exchange of data.

C. Database:

A database is a collection of data that has been collected, entered, and maintained in a way that facilitates easy access, analysis, and manipulation. Databases are used to store a wide range of data, from user profiles and transaction records to product inventories and more. They provide a structured way to store and manage large volumes of data while maintaining data integrity and security. Databases can be relational (using tables and SQL) or NoSQL (using various data models), and they serve as the backend storage for web applications, ensuring data persistence and accessibility.

D. Security management for Hybrid-blockchain

By prioritizing paramount security measures, the Hybrid Blockchain-Based Approach for Secure and Efficient IoT Identity Management (HB-IIM) is designed to provide robust protection for IoT device identities and the associated data. Leveraging decentralized blockchain technology, HB-IIM ensures immutability and maintains a tamper-proof ledger of all identity related activities. To protect the sensitive data, advanced encryption techniques are employed effectively to prevent unauthorized access and unauthorized alterations. Multi-Factor Authentication (MFA) introduces an additional layer of verification, even in scenarios where credentials have been compromised. The system further enhances security through secure device enrollment procedures and the implementation of access control policies, effectively mitigating potential rogue access attempts and empowering users with control over device interactions. Regular audits and the utilization of hardware security modules contribute to an elevated level of overall security, while the integration of zero-knowledge proofs strengthens data privacy. Through the seamless incorporation of these robust security features, HB-IIM establishes a resilient foundation for the secure management of IoT identities, safeguarding the integrity of the whole ecosystem, as depicted in Figure 4.

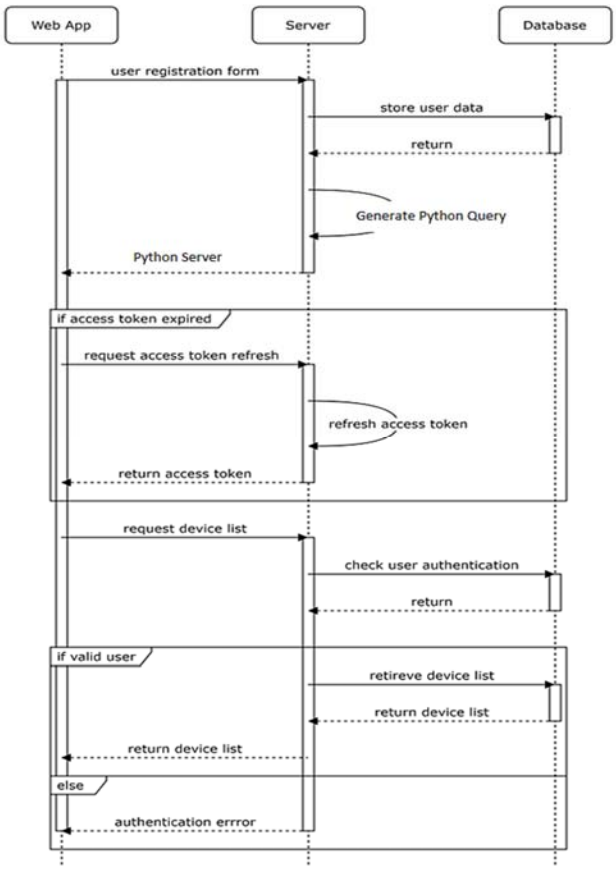

Fig. 4. Sequence diagram of the user registration process and a subsequent request to retrieve all registered IoT devices using python's to handle users device management.

4. Approach For IOT Identity Management in Hybrid Blockchain

A. One Time Authentication Approach for HB-IIM

In this section, we illuminate the architectural framework tailored to scenarios where IoT devices necessitate registration and authentication only once or infrequently, due to the non-automated nature of the process requiring user interaction, as highlighted in [26]. Figure 5 offers an overview of the envisaged system featuring one-time authentication. This system is divided into two distinctive layers. The lower layer, of primary relevance to the device owner, encompasses their IoT-connected devices, which acquire data through sensors or other mechanisms. In this particular model, all communication pertaining to the authentication process between the IoT devices is channeled through the device owner. Conversely, the upper layer of the architecture is dominated by the Know Your Device (KYD) platform, comprising multiple interlinked components. At the core of the platform's architecture lies a Python-based server, provided with the capability to administer and authenticate devices. To underscore the integration of a Know Your Customer (KYC) system within the overarching architecture, the server extends its support to facilitate the registration of users.

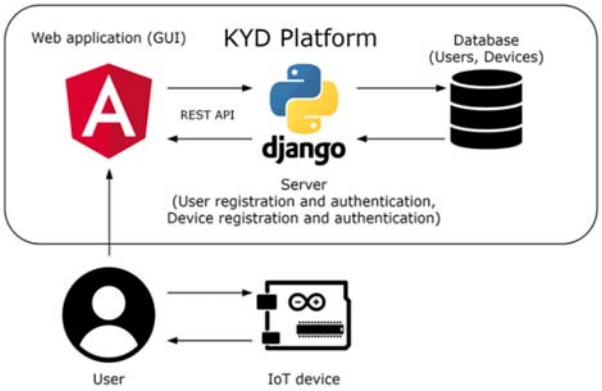

Fig. 5. System architecture for the one-time authentication approach for HB-IIM.

The server is connected to a database where all the necessary data for user and device identification is stored. The server mainly has two responsibilities. Firstly, it facilitates the registration of devices and users, as well as keeping track of these and providing basic configuration tools according to [27]. Secondly, it contains the authentication logic for the devices. The last component of the KYD platform is the Angular-based web application. It provides a graphical user interface (GUI) for the device owners to register themselves and their IOT devices.

B. Periodical Authentication Approach for HB-IIM

This section describes the architecture for the case that we require the IoT devices to be authenticated regularly. As the previously discussed approach requires too much user interaction, some adjustments are necessary for this design in order to automate the authentication process. Figure 6 shows an overview of the proposed system with periodical authentication. Many IoT connected devices cannot turn themselves off and subsequently power back up again on their own. Since power-cycling is a requirement for our hybrid block chain implementation, we require a controller device that acts as an intermediary between then KYD platform and the IoT-connected devices, as a replacement for the device owner. It is responsible for both communicating with the KYD platform and power cycling the IoT devices. This device has to be able to connect to the KYD platform's server in a secure and automated way, so a secure shell (SSH) connection will have to be set up for remote command execution from the KYD platform.

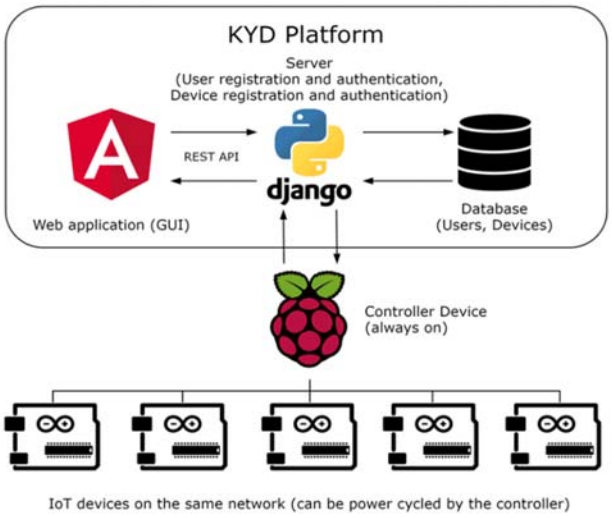

Fig. 6. An overview of the proposed system with periodical authentication.

C. Comparison of both Approaches

Both the periodical and one-time authentication designs possess distinct strengths and weaknesses, primarily tailored to specific use cases. The one-time authentication approach places its emphasis on device identification, with the Know Your Device (KYD) platform functioning akin to a certification service. It verifies a device's identity and subsequently issues a certificate of authenticity. Conversely, the periodical authentication approach assumes a role more akin to that of an overseeing entity, continuously ensuring that registered devices maintain their claimed identities. As a result, the periodical approach places a greater focus on ongoing device authentication compared to the one-time approach. The periodical authentication design offers the advantage of increased automation, demanding less active

involvement from the device owner once the initial setup is completed. Additionally, it stands out as the more secure approach, as it mandates periodic device reviews and restricts user involvement in the authentication process to a greater extent, as illustrated in Table 1.

TABLE 1. Comparison table between One-Time Authentication and Periodical Authentication Approaches for the HB-IIM.

Aspect	One-Time Authentication	Periodical Authentication
Authentication Frequency	Once during registration	Every 24 hours
Security Risk	Low	Moderate to High
Advantages		
Ease of Use	Simplicity in setup	Reduces prolonged exposure
Resource Efficiency	Lower resource consumption	Reduced network load
Rapid Device Onboarding	Quick initial setup	Easier for new devices
Challenges		
Increased Exposure to Attacks	Vulnerable between authentication intervals	Elevated risk during authentication windows
Use Cases		
Low-Frequency Access Devices	Simple IoT devices with infrequent interactions	Devices requiring periodic updates or access
Implementation Complexity	Simple	Moderate

The one-time authentication design offers the advantage of being a lightweight solution, rendering it more straightforward to implement and less burdensome for the device owner. As highlighted in [28, 29], this design requires minimal setup on the part of the user.

TABLE 2. The performance metrics of the HB-IIM Model compared to a traditional solution.

Metric	HB-IIM Model	Traditional Solution
Transaction Throughput	1500 tx/s	800 tx/s
Latency	25 ms	50 ms
Scalability	5000 devices	2000 devices
Resource Consumption	75% CPU, 300 MB RAM	90% CPU, 400 MB RAM
Security Features	High	Limited
Privacy Measures	Strong	Basic

Moreover, it exhibits greater flexibility and scalability, as it is not overloaded by additional constraints associated with the utilization of a separate controller device and the necessity for a secure automated connection to the server, as detailed in the performance metrics outlined in Table 2 for IoT blockchain management.

Connected Internet of Things (IoT) devices form the backbone of the Hybrid Blockchain-Based Approach for Secure and Efficient IoT Identity Management (HB-IIM). These devices encompass a diverse range of endpoints that interact with the HB-IIM system for identity management, data exchange, and secure communication according to [30]. The identification and classification of these connected IoT devices play a crucial role in designing and implementing an effective HB-IIM solution as mentioned in Table 3.

TABLE 3. Attributes and characteristics for IoT connected devices for authentication via HB-IIM solutions.

Device Type	Characteristics	Authentication Approach	Frequency of Authentication
Smart Thermostat	Climate control, temperature monitoring	Periodical	Every 12 hours
Wearable Tracker	Health monitoring, activity tracking	One-Time	During initial setup
Industrial Sensor	Real-time data collection, process control	Periodical	Every 1 hour
Smart Lock	Access control, remote unlocking	One-Time	During initial setup
Environmental	Air quality monitoring, pollutant detection	Periodical	Every 4 hours

5. Prototypical Implementation / Architectural Styles

Developing a modular and scalable architectural framework that facilitates seamless communication between physical blocks and IoT devices represents the quintessential approach for linking blocks with IoT devices. The system comprises two primary components: physical blocks and the IoT gateway. Physical blocks serve as data collectors and execute tasks based on user inputs. They are equipped with sensors, actuators, and communication modules, with the flexibility to be designed as modular units, simplifying expansion and customization. Bridging the cloud-based infrastructure and the physical building blocks is the IoT gateway, responsible for device detection, authentication management, data retrieval from the blocks, and transmission of relevant data to the cloud. Within this paper, the architectural styles for accessing IoT devices through blockchain networks are categorized into three main types.

- Model1: directly connected IoT-blockchain
- Model2: indirect connected IoT-blockchain
- Model3: hybrid connected IoT-blockchain (proposed)

A. Model1: Directly connected IoT-blockchain

This architecture considers the inclusion of resource-rich IoT devices, such cars and security cameras, as full or light nodes in a blockchain network as shown in Figure 7. These devices are built to collect environmental data, which is then sent to the blockchain through an intermediate web or mobile application according to [31, 32]. Through the use of smart contracts, this application makes it easier to extract data value and submit data as transactions. With this configuration, there is no need for middlemen because the IoT devices and blockchain nodes are connected directly. However, these resource-rich devices face difficulties because to the computational demands and storage requirements involved with active involvement in the blockchain network.

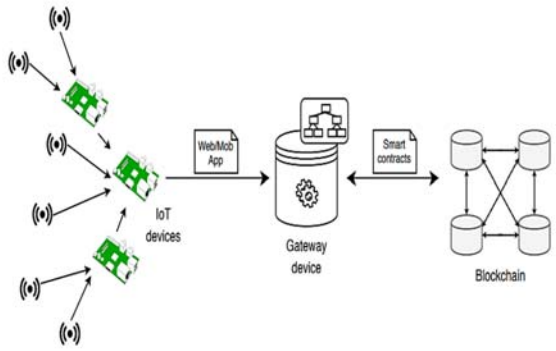

Fig 7: Blockchain integration with directly connected IoT devices.

The recommendation is to use cloud resources to effectively outsource some blockchain-related processes to centralized cloud architectures in order to mitigate this. IoT devices may focus on data collecting without being distracted by processing and storage burdens by outsourcing responsibilities like transaction processing and keeping a full blockchain ledger as stated in [33]. While this strategy has advantages like better resource management, scalability, and potential cost savings, it also raises issues like data privacy, latency, cloud stability, and the danger of centralization. Therefore, careful consideration is required to maintain the decentralized principles of blockchain while ensuring a harmonious balance between the benefits and potential downsides.

B. Model 2: Indirectly connected IoT-blockchain

An IoT-blockchain system in which sensor readings are gathered by resource-constrained IoT devices and sent to a more effective gateway as shown in Figure 8. After processing the data, this gateway uses a web or mobile application to extract value and uploads transaction data to a blockchain using a smart contract according to [34]. This configuration can result in gateway overload difficulties because of the massive amounts of data that IoT devices eventually produce. In order to increase the system's overall efficiency and capacity to manage the growing volume of data, this technique tries to distribute the processing and data storage activities among a number of gateways. This idea is in line with the more general trend of edge computing, which involves performing data processing closer to the data source (in this example, IoT devices) rather than sending all data to a single cloud server.

IoT_Data→Gateway_Processing→Blockchain_Transaction
IoT_Data→Gateway_1_Processing→Blockchain_Transaction
IoT_Data→Gateway_2_Processing→Blockchain_Transaction
.
.
IoT_Data→Gateway_N_Processing→Blockchain_Transaction

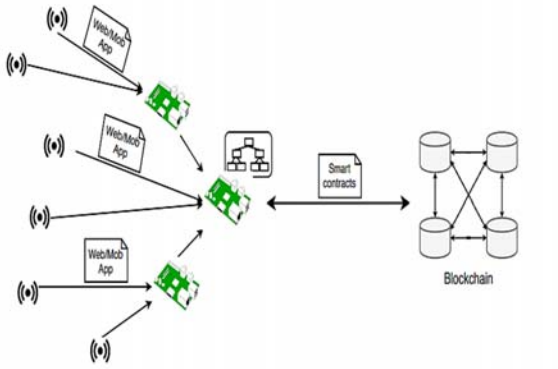

Fig. 8. IoT-Blockchain with a single gateway serving as the controller in an indirect network.

The concern of potential gateway overload owing to increasing data volumes is handled through the strategic integration of several gateways in the context of an IoT-blockchain ecosystem, where resource-constrained IoT devices collect environmental data and transfer it to a resilient gateway. By spreading out the computational workload and data storage burden across numerous gateways, this strategy aims to maximize resource usage and reduce processing bottlenecks as mentioned in [35]. The system achieves improved load balancing, decreased data transmission latency, and increased scalability by doing this. By reducing the need to send sensitive data over large networks, this architecture not only promotes privacy and security but also fault tolerance, guaranteeing uninterrupted functionality even in the face of gateway failures.

C. Model 3: Hybrid connected IoT-blockchain (proposed)

Efficiently managing vast volumes of data and IoT devices in a secure and transparent manner has become essential to meet the evolving demands of businesses considering the escalating prevalence of IoT systems, as emphasized in [36]. as depicted in Figure 9, and Algorithm, an innovative approach involves the development of a hybrid

interconnected IoT-Blockchain model, which entails the integration of blockchain and IoT systems. This cutting-edge design leverages multiple gateways and employs two distinct blockchains to enhance data management capabilities and cater to diverse transaction requirements.

Scenario:

To enable prompt intervention and automated health services for Alice's severe apnea condition, consider a scenario where a multitude of healthcare professionals require access to her Electronic Health Records (EHR). Different levels of data access and granularity are necessary for various providers, though. For instance, whereas Alice's insurance provider just needs to know her current health status in order to provide insurance services, the Health Management System (HMS) may require extensive personal information. Multiple blockchains can be constructed to meet these divergent needs, ensuring a division of duties among healthcare providers.

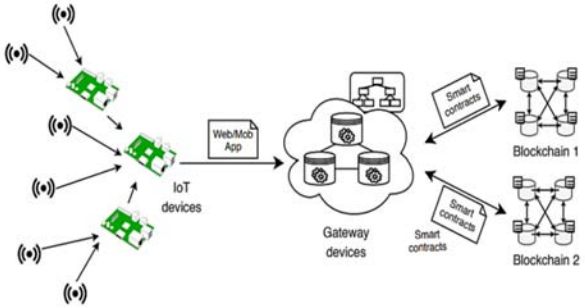

Fig. 9. Integration of two gateways and customized blockchains and the distributed IoT blockchains

Algorithm: Hybrid connected IoT device to unique blockchain

```
Initialize masterGateway, slaveGateways[], blockchain_HMS, blockchain_Insurance
For each IoTDevice in devices:
  - sensorReadings = IoTDevice.senseData()
  - slaveGateway = randomSlaveGateway()
  - slaveGateway.receiveSensorReadings(sensorReadings)
readings = masterGateway.collectSensorReadings()
aggregatedData = aggregate(readings)
rootHash = calculateRootHash(aggregatedData)
providerRole = determineProviderRole()
if providerRole == "HMS":
blockchain_HMS.push(rootHash)
else if providerRole == "Insurance":
blockchain_Insurance.push(rootHash)
```

In reality, IoT devices with limited resources collect environmental data and connect to edge gateways to do early data processing. These gateways work in a master-slave setup, where the master gateway collects sensor readings from IoT devices and distributes them to slave gateways. To improve data integrity, the slave gateways work together to calculate a Merkle tree's root hash. The generated hash is then sent to the master gateway, which uses a smart contract to connect to a blockchain node and effectively record the hash as a transaction on the relevant blockchain. The complex requirements of contemporary healthcare situations are met by this architecture, which integrates IoT and blockchain technologies to enable safe data sharing, customized access controls, and simplified data administration for healthcare providers as stated in [37, 38].

C. *Quality attribute for evaluation*

For IoT devices connected to a blockchain network, performance and efficiency are essential qualities since they have a direct impact on the system's overall functionality and efficacy. Due to the dispersed nature of blockchain technology, integrating IoT devices with a network can provide advantages like transparency, security, and decentralized control, but it also poses issues relating to performance and efficiency. The next subsections show how these qualities apply to this situation:

1) *Performance:*

The system's speed and responsiveness are referred to as performance. There are many performance factors to take into account when IoT devices are linked to a blockchain network, as shown in figure 10 including:

Network use: Consensus mechanisms are commonly used in blockchain networks to verify and log transactions. Contrary to conventional centralized systems, this may result in transaction processing that is slower. For less important transactions, adopting off-chain solutions or optimizing the consensus algorithm can help keep the throughput for IoT devices at a reasonable level.

Latency: Low latency is frequently needed for IoT applications to provide real-time or almost real-time interactions. Due to network propagation and consensus methods, blockchain networks may cause delays. This problem can be solved by designing the network architecture to reduce latency and employing strategies like sharing.

2) *Efficiency*

Efficiency is the term used to describe how effectively resources are used to produce the intended results. Efficiency factors for IoT devices linked to a blockchain network include:

Energy Consumption: IoT devices frequently need finite power sources. It can be difficult given how energy-intensive blockchain consensus techniques are. Overall efficiency can be increased by investigating energy-efficient consensus

algorithms (such as Proof of Stake) or modifying device behavior to reduce blockchain interactions.

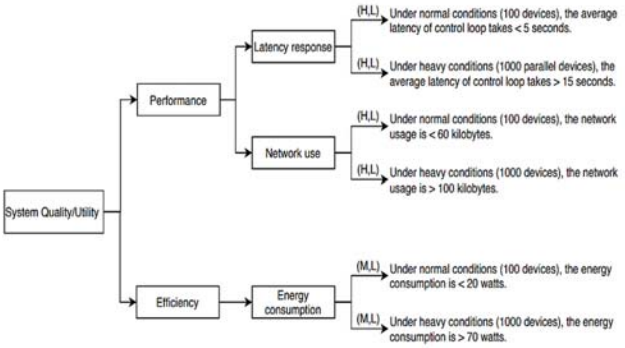

Fig. 10. Quality attributes for the evaluation of IoT devices connected through the blockchain network.

Analyzing quality attributes along with non-functional requirements (NFRs) and trade-offs is essential for designing and implementing successful systems as mentioned in [39, 40]. as shown in Figure 11, let take an example of IoT devices connected through a blockchain network and delve into how various quality attributes and NFRs interplay with trade-offs:

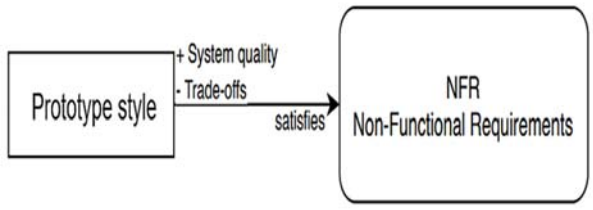

Fig. 11. Quality attributes along with non-functional requirements (NFRs) and trade-offs

TABLE 4. All three Models based on risk and analysis for each type of connection between IoT and blockchain.

Aspect	Model 1: Directly Connected	Model 2: Indirectly Connected	Model 3: Hybrid Connected (Proposed)
Connection Type	Direct connection	Indirect connection	Combination of direct and indirect
Risk Analysis	Higher risk due to exposure of IoT devices	Moderate risk as data is shared through gateways or proxies	Moderate risk due to a mix of both direct and indirect connections
Security	Potentially vulnerable to attacks on IoT devices	Better security as gateway/proxy can act as a buffer	Enhanced security through a mix of direct and indirect approaches
Data Privacy	Limited control over data flow and privacy	More control over data privacy and flow	Better data privacy control through selective direct and indirect links
Complexity	Relatively simple setup	Moderately complex setup	More complex setup due to integration of both direct and indirect components
Fault Tolerance	Single point of failure for the entire system	Distributed failure potential across gateways/proxies	Enhanced fault tolerance through a combination of approaches
Latency	Lower latency due to direct communication	Slightly increased latency through gateways/proxies	Latency depends on the specific implementation of hybrid connections

6. Simulation Environment

The simulation environment is mentioned by its hardware configuration and consensus protocols in Table 5.

TABLE 5. The simulation environment for evaluating candidate styles in the context of IoT data processing and blockchain integration.

Aspect	Details
Stages of Evaluation	- Collect, process, store IoT data in gateways for processing and analysis. - Send IoT data to the blockchain network for immutable storage.
Blockchain and Consensus Protocol	- Ethereum Blockchain: Ganache (Personal) - Consensus Protocol: Proof-of-Authority (PoA)
Hardware Specifications	- CPU: Intel(R) Core(TM) i7-8700 @ 3.20 GHz - RAM: 16 GB DDR3
IoT Device	- OS: Raspbian Buster - CPU Usage: 5% of Intel(R) Core (TM) i7-8700 - RAM: 128 MB - Sensor: Oximeter data integrated sensor library - Programming: Python 3
Controller Device	- OS: Linux Mint 19.12 - CPU Usage: 20% of Intel(R) Core(TM) i7-8700 - RAM: 512 MB - Programming: Python 3
Blockchain Node	- OS: Linux Mint 19.12
Configuration	- CPU Usage: 50% of Intel(R) Core(TM) i7-8700 - RAM: 8 GB - Ethereum Version: 1.7.2 - Blockchain Network: Ganache (test network) 2.1.2 - Programming: Python 3

A. EXPERIMENTAL ANALYSIS

We created a simulation to demonstrate how different approaches fare in four distinct scenarios: one with 100 transactions, another with 250, still another with 500, and yet another with a thousand. In the beginning, IoT devices only capture 1 MB files worth of data. The data is subsequently sent to a gateway computer or computers, one at a time or in groups (Configuration1, Configuration2, Configuration3 and Configuration4). Once data transfer to the gateway(s) is complete, the gateway device(s) will hash the data and send the hashes to the blockchain. A web3 provider enables this transfer to the blockchain network by providing a JSON-RPC API for accessing and updating blockchain.

We define concrete measures to compare different designs for blockchain-based Internet of Things (IoT) systems. Specifically, these metrics are as described below:

1) *Average latency:* When evaluating various design, average latency serves as a valuable metric, encompassing the time required for data to traverse the network as well as the execution time of the application across each pertinent component.
2) *Utilization of Network Resources:* This measure characterizes how the various potential styles make use of networking resources.
3) *Energy Consumption:* Calculated as the amount of power needed to run the experimental procedures on the host machine.

B. Average latency:

The data presented in Figure 12 depicts the average delay of the different potential styles under different setups. In the context of Model II, the execution of 1000 transactions were hindered by a performance bottleneck caused by the controller, resulting in a significant increase in latency. On the other hand, Model I effectively reduces latency by facilitating a direct link between IoT devices and the blockchain. In Model III, the deployment of a substantial number of controllers at the edge serves as an effective measure to mitigate the computational and data storage loads experienced by the blockchain platform.

In this context, we will use the notation:

Next, the calculation for the average latency (L_{avg}) can be derived as follows:

$$L_{avg} = \frac{1}{N}\sum_{i=1}^{N} T_i$$

The variable "N" represents the quantity of transactions or interactions occurring within the system.

T_i is the duration required for the ith transaction to finalize, encompassing both the time spent for network propagation and the execution time of the program.

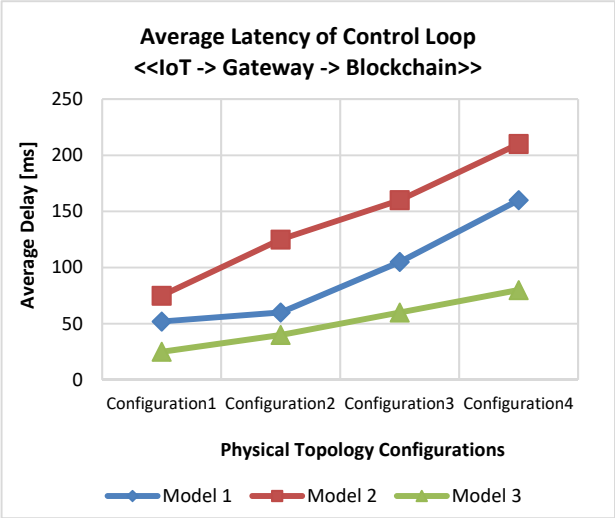

Fig. 12. Comparison of Average Latency in the Control Loop.

C. NETWORK USAGE:

The utilization of networks commonly entails the measurement of data transfer quantities and the allocation of resources involved in the exchange of information among various system components.

$$Network\ Usage = \sum_{i=1}^{N} (Di * Ri)$$

The variable N represents the aggregate quantity of transactions or interactions.
The variable D_i represents the size of the data, expressed by bytes, for the i-th transaction.
The variable R_i represents the utilization of network resources, such as the amount of bandwidth used, by the i^{th} transaction.

The usage of potential Model inside the network across various configurations is illustrated in Figure 13. The utilization of several gateways or blockchain networks in ModelIII leads to a significant augmentation in network burden. The observed result can be attributed to the prevailing data transfer that takes place between Internet of Things (IoT) devices and controllers through low-latency connections. In this process, the IoT data hashes are transmitted to the blockchain as transactions.

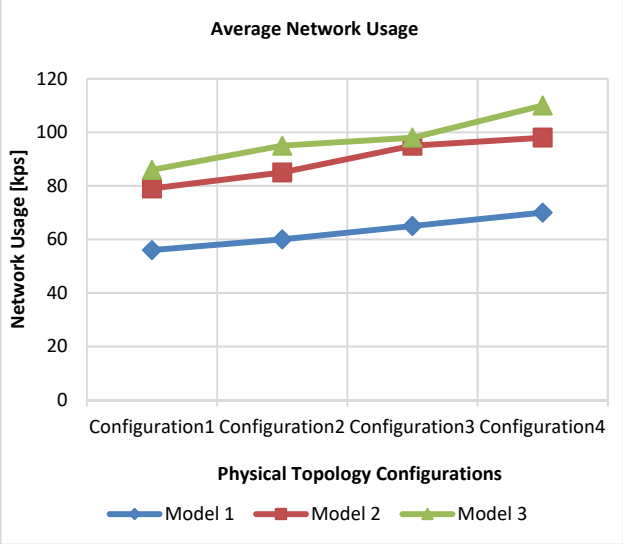

Fig. 13. Comparison of network usage of different Model

.

D. ENERGY CONSUMPTION:

Furthermore, the incorporation of multiple distinct blockchains within the suggested configurations leads to an increase in energy usage. The reason for this phenomenon is because the maintenance and operation of several blockchains necessitates the allocation of more processing resources, thus resulting in elevated energy consumption.
Energy consumption is commonly measured by determining the amount of power utilized by a certain device within a specific period. Within the realm of Internet of Things (IoT) systems, the equation denoting energy consumption might be articulated as follows:

$$Energy\ consumption = \sum_{i=1}^{N} (Pi * Ti)$$

Where;
The variable N represents the aggregate quantity of transactions or interactions.
The variable P_i reflects the power usage, measured in watts, of the host machine while executing the i^{th} operation.
The variable T represents the time length, measured in seconds, of the i^{th} transaction.

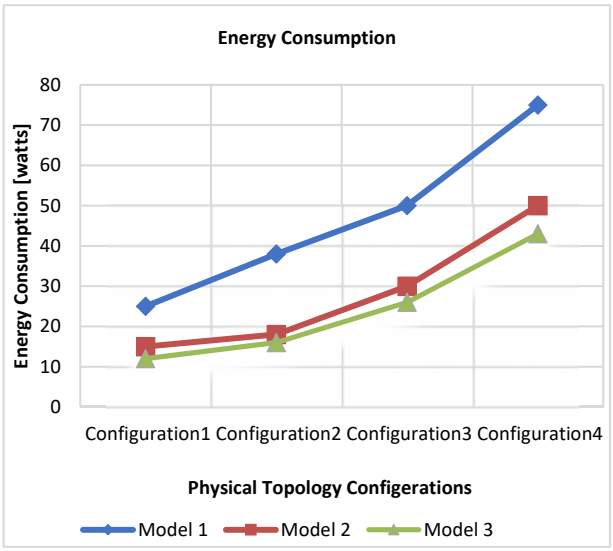

Fig. 14. The layout of energy consumption from the configurations of multiple Models.

The depiction in Figure 14 depicts the energy usage linked to various styles within different setups. In the case of Model II and III, the edge gateway(s) are responsible for the processing and analysis of Internet of Things (IoT) data, which leads to a notable consumption of power. Moreover, the utilization of many dedicated blockchains exacerbates the energy usage within the proposed configurations.

7. Discussion

In this section, we conduct an evaluation and comparative analysis of the effectiveness of three distinct Models for IoT identity management. These Models are identified as Model 1 (direct IoT-blockchain connection), Model 2 (indirect IoT-blockchain connection), and Model 3 (hybrid IoT-blockchain connection). The overarching aim of

our paper is to assess and contrast these Models in terms of their average latency, network utilization, and power consumption, with the ultimate objective of identifying the most promising solution. Our final goal is to pinpoint the Model that offers the optimal balance between performance and efficiency for managing IoT device identities. Average Delay: Because delays can affect the real-time responsiveness of applications, average latency is a crucial measure in IoT identity management systems. As transactions are handled quickly on the local network, latency is decreased in Model 1 due to devices' direct connections to the blockchain. The additional time it takes for data to be routed between nodes while using Model2's intermediary nodes. On the other hand, our hybrid method, represented by Model 3, takes advantage of both direct and indirect connections. It uses direct connections within a local cluster to reduce latency while still taking advantage of the security benefits of indirect connections while communicating with the larger blockchain network. Model 3 has the lowest average latency and is hence ideal for time-critical IoT applications.

Network Usage: Optimal bandwidth usage and stable networks rely on effective network utilization, which is why IoT identity management places such importance on it. Each device in Model 1 communicates with the blockchain directly, which could cause bottlenecks in the network during peak usage times. The second Model uses relay nodes to reduce this burden on the network. To find an optimal medium, Model 3 which relies on local cluster interactions to keep network traffic low and only makes use of indirect connections when absolutely essential. This results to maximized use of the network's resources, which prevents slowdowns and keeps performance stable.

Energy consumption: With so many IoT devices being bound by limited resources and running on battery power, energy efficiency is of crucial importance. Model 1's direct interaction with the blockchain results in substantially increased energy usage, which can quickly deplete device batteries. Model 2 saves energy by cutting down on the number of in-person blockchain interactions. Model 3 is a considerable improvement over the previous Models since it uses local cluster interactions to do mundane identity management duties while significantly reducing energy use. By only performing necessary blockchain transactions using the hybrid method, the lifespan of IoT devices can be extended.

Overall Performance: Model 3 emerges as the most performance-based and efficient solution for IoT identity management based on the study of average latency, network use, and energy consumption. Model 3 overcomes the shortcomings of its predecessors by offering a holistic method for optimizing latency, network use, and energy consumption by merging direct and indirect connections smoothly. Applications that require instantaneous response, scalable network consumption, and prolonged gadget lifetime are ideal candidates for this novel hybrid approach.

8. Conclusion

In this paper, we have examined into the potential applications of blockchain technology within the domain of IoT identity management. With a keen focus on achieving both security and efficiency in managing identities for IoT devices. The comprehensive evaluation of each Model unearthed their respective strengths and weaknesses, with average latency, network utilization, and energy consumption serving as pivotal performance indicators. Model 1, with its direct blockchain connection, exhibited low latency but at the cost of high energy consumption. Model 2 introduced intermediary nodes to reduce energy consumption but introduced unacceptable delays. Our proposed Model 3, a hybrid approach, adeptly struck a harmonious balance between these competing concerns by employing local cluster interactions for routine tasks and indirect blockchain connections for mission-critical operations. As the standout choice for IoT identity management, this hybrid approach excelled across all assessed parameters. In summary, the findings of this paper underscore the importance of adopting a holistic system design approach when crafting blockchain-based IoT identity management infrastructure. Model 3 presents a hybrid strategy that harnesses the strengths of both direct and indirect connections, resulting in a versatile, low-latency, low energy consumption, and optimized network utilization. This paper not only underscores the significance of tailored approaches aligned with the unique requirements of IoT ecosystems but also furnishes a pragmatic, performance-driven resolution to the challenges of IoT identity management.

References

[1]. S. Zhao, S. Li, and Y. Yao, “Blockchain-Enabled Industrial Internet of Things Technology,” IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1442–1453, 2019.

[2]. N. Kshetri, “Blockchain's roles in strengthening cybersecurity and protecting privacy,” Telecommunications Policy, vol. 41, no. 10, pp. 1027–1038, 2017.

[3]. M. G. Speranza, “Trends in transportation and logistics,” Operational Research, vol. 264, no. 3, pp. 830–836, 2018.

[4]. A. Panarello, N. Tapas, G. Merlino, and F. Longo, “Blockchain and IoT integration: a systematic survey,” Sensors, vol. 18, p. 2575, 2018.

[5]. R. P. Sarode, “Blockchain for committing peer-to-peer transactions using distributed ledger technologies,” Journal of Computational Science and Engineering, vol. 1, no. 1, p. 1, 2008.

[6]. F. Sabrina, N. Li, and S. Sohail, "A Blockchain Based Secure IoT System Using Device Identity Management," Sensors (Basel, Switzerland), 2022.
[7]. F. Casino, L. Azpilicueta, P. Lopez-Iturri, E. Aguirre, F. Falcone, and A. Solanas, "Optimized wireless channel characterization in large complex environments by hybrid ray launching-collaborative filtering approach," IEEE Antennas and Wireless Propagation Letters, vol. 16, pp. 780–783, 2017.
[8]. V. G. Venkatesh, K. Kang, B. Wang, R. Y. Zhong, and A. Zhang, "System architecture for blockchain based transparency of supply chain social sustainability," Robotics and Computer-Integrated Manufacturing, vol. 63, article 101896, 2020.
[9]. A. Satybaldy, A. Subedi, and M. Nowostawski, "A Framework for Online Document Verification Using Self-Sovereign Identity Technology," Sensors (Basel, Switzerland), 2022.
[10]. W. Kersten, M. Seiter, B. von See, N. Hackius, and T. Maurer, Logistics and Supply Chain Management Trends and Strategies–Digital Transformation Opportunities, DVV Media Group, Hamburg, Germany, 2017.
[11]. V. Di and A. Varriale, "Blockchain technology in supply chain management for sustainable performance: evidence from the airport industry," International Journal of Information Management, vol. 52, article 102014, 2020.
[12]. A. Hammoud, H. Sami, A. Mourad, H. Otrok, R. Mizouni, and J. Bentahar, "Ai, blockchain, and vehicular edge computing for smart and secure iov: Challenges and directions," IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 68–73, 2020.
[13]. G. Rathee, A. Sharma, R. Kumar, and R. Iqbal, "A secure communicating things network framework for industrial IoT using blockchain technology," Ad Hoc Networks, vol. 94, article 101933, 2019.
[14]. W. Wang, H. Huang, L. Xue, Q. Li, R. Malekian, and Y. Zhang, "Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment," Journal of Systems Architecture, vol. 115, p. 102024, 2021.
[15]. M. Anwar, "Connect2Smallports project: South Baltic small ports – gateway to the integrated and sustainable European transport system,"Project brief and updates on the project activities: Digital Audit. Blockchain Design Strategy. Call for Collaboration. Reports and scientific publications, 2019, http://bth.diva-portal.org/smash/record.jsf?pid=diva2%3A1361852&dswid=7361.M.
[16]. M. F. Aziz and A. N. Khan, "A lightweight and compromise-resilient authentication scheme for IoTs," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 3, article e3813, 2019.
[17]. S. Naskar, P. Basu, and A. K. Sen, "A literature review of the emerging field of IoT using RFID and its applications in supply chain management," Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications, IGI Global, Hershey, PA, USA, pp. 1664–1689, 2020.
[18]. F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in 2016 13th International Conference on Service Systems and Service Management (ICSSSM), pp. 1–6, Kunming, China, 2016.
[19]. C. S. Yang, "Maritime shipping digitalization: blockchain-based technology applications, future improvements, and intention to use," Transportation Research Part E: Logistics and Transportation Review, vol. 131, pp. 108–117, 2019.
[20]. A. Akram and P. Bross, "Trust, Privacy, and Transparency with Blockchain Technology in Logistics," in MCIS 2018 Proceedings, p. 17, 2018.
[21]. K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," in Proceedings of the 50th Hawaii International Conference on System Sciences (2017), 2017.
[22]. H. Hasan, E. AlHadhrami, A. AlDhaheri, K. Salah, and R. Jayaraman, "Smart contract-based approach for efficient shipment management," Computers & Industrial Engineering, vol. 136, pp. 149–159, 2019.
[23]. H. Wu, Z. Li, B. King, Z. B. Miled, J. Wassick, and J. Tazelaar, "A distributed ledger for supply chain physical distribution visibility," Information, vol. 8, no. 4, p. 137, 2017.
[24]. S. K. Dwivedi and R. A. S. Vollala, "Blockchain based secured information sharing protocol in supply chain management system with key distribution mechanism," Journal of Information Security and Applications, vol. 54, article 102554, 2020.
[25]. B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: a survey on applications and security privacy challenges," Internet of Things, vol. 8, article 100107, 2019.
[26]. J. Tao and L. Ling, "Pratical Medical Files Sharing Scheme Based on Blockchain and Decentralized Attribute- Based Encryption", IEEE Access, vol. 9, pp. 118771-118781, 2021.
[27]. M. Chawla and A. Basu, "A Blockchain-based Decentralized Data sharing Framework for Healthcare Applications", 2018 IEEE International Conference On Big Data(BigData), pp. 3798-3803, 2018.
[28]. S. M. Mousavi, K. Karimi and M. Farahani, "A Novel Blockchain-based Framework for Secure Medical Image Sharing in Healthcare Systems", 2019 IEEE International Conference on Health Informatics and Medical Systems (HIMS), pp. 1-5, 2019.
[29]. Sriman B and Annie Silviya S H, "Blockchain Industry 5.0: Next Generation Smart Contract and Decentralized Application Platform", 2022 International Conference on Innovative Computing Intelligent Communication and Smart Electrical Systems (ICSES), pp. 1-8, 2022.
[30]. J. Liu, Y. Yang and D. Chen, "An Efficient and Secure Medical Data Sharing Scheme Based on Blockchain", 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference Data Science and Systems (HPCC/Smart City/DSS), pp. 856-860, 2019.
[31]. K. A. Gogineni, P. Kumar, S. Venkatesan and S. R. Pandian, "A Decentralized Blockchain Framework for Secure Medical Data Sharing in Telemedicine Applications", 2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT IOT and AI (HONET-ICT), pp. 174-181, 2020.
[32]. C. Xu, Y. Xia, J. Zhang and X. Shen, "A CP-ABE-Based Secure Data Sharing Scheme with Efficient Key Updating for Cloud Storage", IEEE Transactions on Cloud Computing, pp. 1-1, 2018.
[33]. S. Chen, Y. Chen, J. Xiong and X. Huang, "A CP-ABE-Based Secure Data Sharing Scheme for Online Social Networks", IEEE Access, pp. 35044-35054, 2019.

[34]. D. Chen, N. Zhang, N. Cheng, K. Zhang, Z. Qin, and X. Shen, "Physical layer based message authentication with secure channel codes," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 1079–1093, 2018.
[35]. Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," Proceedings of the IEEE, vol. 107, no. 8, pp. 1608–1631, 2019.
[36]. I. Sitton-Candanedo, R. S. Alonso, J. M. Corchado, S. Rodr ´ ´ıguezGonzalez, and R. Casado-Vara, "A review of edge computing reference ´ architectures and a new global edge proposal," Future Generation Computer Systems, vol. 99, pp. 278–294, 2019.
[37]. Y. Wu, H. N. Dai, and H. Wang, "Convergence of blockchain and edge computing for secure and scalable IIoTCritical Infrastructures in industry 4.0," IEEE Internet of Things Journal, vol. PP, no. 99, 2020.
[38]. X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," Computer Communications, vol. 136, pp. 10–29, 2019.
[39]. G. Luo, H. Zhou, N. Cheng, Q. Yuan, J. Li, F. Yang, and X. S. Shen, "Software defined cooperative data sharing in edge computing assisted 5g-vanet," IEEE Transactions on Mobile Computing, 2019.
[40]. S. Guo, X. Hu, Z. Zhou, X. Wang, F. Qi, and L. Gao, "Trust access authentication in vehicular network based on blockchain," China Communications, vol. 16, no. 6, pp. 18–30, 2019.

Dr. Abdulaleem Ali Almazroi received the Ph.D. degree in Computer Science from Universiti Teknologi Malaysia, in 2016. He is currently an Assistant Professor at Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University. His research interests include Cyber Security, Wireless Communications, Vehicular Network, And Internet of Things.

Dr. Nouf Atiahallah Alghanmi completed her undergraduate studies, earning a B.Sc. in Information Technology from King Saud University, Riyadh, KSA, in 2009. Following this, she pursued her postgraduate education, obtaining an M.Sc. in Computer Security from the University of Birmingham, United Kingdom, in 2011. Continuing her academic journey, she attained a Ph.D. in Computer Science with a specialization in Machine Learning from the University of Manchester, United Kingdom, in 2022. Since that year, she has held the position of assistant professor at the Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University. Her research interests encompass a variety of areas including social network analysis, computer security, IoT, artificial intelligence, data mining, and machine learning.