Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

SECURITY ENHANCEMENT OF SMART CITIES: A BLOCKCHAIN APPROACH

MUHAMMAD ALI
Department of Software Engineering, Superior University, Lahore, 54000, Pakistan.
Email: msse-f21-008@superior.edu.pk

ZAIN UL ABDIN
Department of Software Engineering, University of Sargodha, Sargodha, 40100, Pakistan.
Email: zainulab0@gmail.com

MOODSER HUSSAIN
Department of Information Technology, University of the Punjab, Gujranwala Campus, Pakistan.
Email: moodser.hussain@pugc.edu.pk

RIDA RIAZ
Department of Software Engineering, University of Sargodha, Sargodha, 40100, Pakistan.
Email: ridariaz82@gmail.com

MUHAMMAD WASEEM IQBAL
Department of Software Engineering, Superior University, Lahore, 54000, Pakistan.
Email: waseem.iqbal@superior.edu.pk

SOHAIL MASOOD BHATTI
Department of Computer Science, Superior University, 54000, Lahore, Pakistan.
Email: sohailmasood@superior.edu.pk

Abstract

The Internet of Things (IoT) enables the capturing and storage of detailed information about individuals, their behaviors, and their living environments. The disclosure of this information can compromise people's right to privacy. Hence, it is essential to use and protect users' data responsibly, which they provide while using IoT-based apps, to ensure their private information and data safety. Our objective is to make it simpler for users to claim ownership of their data, distribute it, and audit it. We propose a blockchain architecture that secures data collected from IoT devices throughout their entire existence. To comply with privacy regulations and meet the needs and desires of end-users (data owners), we will incorporate smart contracts into our framework. A comprehensive breakdown of the system architecture, highlighting its key components and functions concerning a specific application scenario, can help us achieve our goal.

Keywords: Blockchain. Privacy, IoT, Smart Cities, Encryption

1. INTRODUCTION

Rapid urbanization is expected to cause a range of challenges across social, economic, technological, and intergenerational realms as over 70% of the world's population is predicted to live in urban areas by 2050 [1]. Numerous countries are aiming to establish "smart cities" in light of increasing urbanization, utilizing technology-driven measures such as the Internet of Things, cyber-physical systems, big data analysis, and real-time control, to enhance the standard of living for citizens. The Internet of Things commonly

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

referred to as IoT is a vital technology that enables sensors and intelligent devices to connect via an open channel, such as the internet, to gather and analyze data in smart city infrastructure [2].

The concept of "smart cities" has a wide range of applications in various fields, such as healthcare, energy management, transportation, water, and irrigation management [3]. The success of these applications is largely dependent on the effective utilization of data gathered from sensors and devices. In smart cities, numerous sensors are linked to the internet, which raises concerns about people's privacy and security [4]. The connectivity of Internet of Things (IoT) sensors is the primary gateway for potential security vulnerabilities, which makes smart cities that use IoT technology susceptible to various forms of attacks. The most significant threats to smart cities are attacks that can occur both in the physical and digital domains [5].

Someone who launches a physical attack on the Internet of Things (IoT) is positioned near the IoT sensors, allowing them to effortlessly disrupt and manipulate the communication of the IoT devices and sensors [6]. The attack involves several components, such as an ongoing denial of service (DoS), injection of malicious code, and insertion of false nodes. The objective of a cyberattack is to gain unauthorized access to different parts of a smart city network, which can be achieved by logging into the system using malware or other damaging software [7]. These attacks may include eavesdropping on conversations, theft, ransomware usage, creating backdoors, conducting distributed denial of service attacks, and denial of service attacks. The second potential threat to privacy is the risk of confidential information being revealed through intrusions, such as data poisoning and inference.

To compromise a smart object, attackers may manipulate the data it provides by injecting false readings, which can be part of a data poisoning attack or an inference attack. These types of attacks pose challenges for machine learning-based intrusion detection and data analysis systems [8]. Furthermore, such attacks can lead to power wastage and disrupt the ability of devices to communicate with each other. Therefore, smart cities must prioritize security and privacy to ensure the safe deployment of IoT devices and sensors, which can enhance the environment and experience for everyone. The primary goal of adopting IoT technology should be to offer secure and private services that are user-friendly and transparent.

A significant number of intrusion detection and prevention systems (IDSs/IPSs) have been developed utilizing statistical and machine learning techniques to ensure security in the Internet of Things (IoT) [9]. In contrast, most traditional security strategies require the use of a centralized system located in cloud to meet computational demands. However, deploying such a system in cloud has numerous drawbacks, including geo-distribution, inadequate support for mobility, a single point of failure, high energy consumption even when the cloud is not being used, significant traffic, and long wait times [10]. The storage of data in the cloud relies on functional provenance to determine various aspects related to the saving, accessing, modifying, and erasing of data, such as the time, location, method, and circumstances. As a threat agent can manipulate provenance records, the system is vulnerable to being disabled or used inappropriately

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

[11]. Centralized systems suffer from a lack of transparency, traceability, and the ability to be administered by more than one entity at a time. One potential solution to this issue is the implementation of fog computing architecture, which involves transporting computer resources to a location near consumers or devices for processing [12]. This approach can enhance the efficiency of cloud computing for the Internet of Things (IoT) by reducing latency and offloading data, among other benefits [13]. Edge devices are responsible for gathering data from the fog and interpreting it. Processed data can then be transferred to the cloud network for further processing and long-term storage or stored locally based on IoT device requirements. The integration of fog computing with the IoT brings new challenges in terms of data review, exchange, security, and privacy [14]. The decentralized structure of blockchain technology has generated considerable attention recently due to its ability to facilitate communication between different components of a system [15]. Key features such as immutability, integrity, and an unalterable ledger have made it attractive for use in IoT-enabled smart cities, where it has the potential to enhance data confidentiality and protection. However, for blockchain technology to effectively resolve these issues in IoT-driven smart cities, thorough research is required. Unlike other technologies, blockchain does not have a central authority controlling it, and its distributed ledger system enables data transparency, immutability, and trust between physically separated IoT nodes. The ledger also maintains an unalterable record of historical events [16]. Despite the high cost of storing data on the blockchain, it is still preferred to store data hashes rather than the actual data as it is more cost-effective. This study utilizes the Interplanetary File System (IPFS) to store data, despite each blockchain node having limited storage capacity. IPFS is a decentralized file system that ensures data integrity and durability by creating and storing copies of data on various nodes dispersed throughout the internet. Every file added to IPFS has a unique hash, and the transaction data is stored in IPFS during the integration process with the blockchain [17]. The hash returned is what goes into the block. Hence, a deployment platform that combines blockchain technology, IPFS fog, and cloud computing could prove advantageous.

2. LITERATURE REVIEW

Myeong *et al* [18], The author argued that smart cities generate vast amounts of data, and more IoT applications can process, analyze, and manage it. Smart cities go beyond location-based services, transit planning, and urban design. Privacy, security, mining, and visualization difficulties plague these apps. Protecting smart cities with blockchain-enabled applications (BIoT) is revolutionary. Due to its decentralized, open, and secure data sharing, the Blockchain Internet of Things (BIoT) is the best solution to the challenges above. The acronym OMLIDS-PBIoT represents a system for detecting intrusions using machine learning that is optimized for maintaining privacy in the context of the Internet of Things (IoT) in smart cities. This system supports smart cities. OMLIDS-PBIoT uses ML and BC methodologies to ensure smart city safety. The OMLIDS-PBIoT strategy begins with data pre-processing to prepare it for analysis. To develop adequate feature subsets, there is a need for a feature selection model based on golden eagle optimization. A random vector functional link network model and a

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

heap-based optimizer classified invasions. Blockchain technology secures data transmission in the Internet of Things smart cities (IoT). Various settings were used to test the OMLIDS-PBIoT technique using benchmark datasets. Additionally, the technique was analyzed and evaluated. The OMLIDS-PBIoT technology outperforms other, more modern methods, according to the studies.

Kumar *et al* [19], the authors state IoT is an intriguing concept that holds a lot of potential for the growth of sustainable smart cities. This is due to developments in sensor technologies as well as low-cost electrical circuits that are becoming more efficient. People's lives can be made easier in smart cities by providing them with smarter modes of transportation and banking, as well as industry 4.0. The safety of its residents is a primary concern for smart cities. Consumers will only benefit from smart IoT infrastructure and applications if they are secure and don't invade their privacy. According to this paper, data collected by IoT devices in smart cities ought to be kept in BPACS. IoT data are encrypted and checked using the blockchain-based approach for data exchange that was recommended in this study. Distributed ledgers are used to store the encrypted data. This research uses cryptosystems to construct safe training algorithms for Principle Component Analysis and Support Vector Machines. It also creates secure building blocks such as secure comparison and polynomial multiplications. The suggested model was subjected to an exhaustive security analysis, which revealed that it safeguards sensitive data for data sources as well as SVM and PCA model variables for data analysts.

Huang *et al* [20], Application service providers (ASPs) can give users access to resources from many trusted domains with the help of secure cross-domain authentication and cross-domain authorization. In this paper, the authors described a single architecture for secure cross-domain resource access in smart cities that uses blockchain technology to allow transparency while protecting user privacy. The architecture makes it possible for ASPs to give the blockchain flexible control over their authentication services. The blockchain can then verify users who have been permitted by different ASPs. It can also let the public audit and track authentication events. Because the blockchain is public, the authentication process may reveal private information about users. Several ways to protect privacy are used to hide sensitive user information on the blockchain, such as homomorphic encryption-based threshold, random permutation, and zero-knowledge proof. This is done to stop privacy leaks caused by authentication events. Also, to make user revocation more efficient, the authors added safe hash functions and a cryptographic accumulator to the system. ASPs can use a global revocation contract to get rid of their users. A prototype based on proof-of-concept consent has been made to show that the proposed framework is correct and works, and our security analysis shows that it can meet all security and privacy requirements.

Khan [21], IoT and networking enable smart gadgets. Smart devices are turning the Internet of Things into a thinking architecture. Cognitive IoT benefits smart cities, healthcare, Industry 4.0, and transportation. Most smart city data is lost because there are no obvious procedures to retrieve and secure it. Academics are developing new

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

machine learning and cognitive learning methods to handle massive volumes of changing data. The integration of the Internet of Things, smart city technology, real-time big data analytics, and AI techniques into preemptive reactions has given rise to the cognitive smart city. Data from users or service providers power smart city services. Because data collection raises privacy concerns, citizen participation in smart cities may decrease. It is essential to uphold privacy standards and regulations that facilitate the sharing of critical information with service providers and third parties, while also preserving public privacy and data integrity. Controlled anonymization and other approaches are needed to maintain data quality. Smart city privacy plans use pseudonymization, clustering, anonymization, and differential privacy. Based on the premise that data order is different, the enhanced clustering algorithm chooses the initial cluster. Smart city privacy protection has been tested. The proposed strategy reduces the discrimination rate.

Peyvandi *et al* [22], for supervised machine learning models like deep learning to be trained, they need high-quality labeled datasets with enough examples from a wide range of categories and situations. Data as a Service (DaaS) can be used to collect these high-quality data, which can then be used to train machine learning models that work well. But data owners might not be able to use DaaS because of privacy concerns. The study introduces Decentralized Computational Intelligence as a Service (DCIaaS), a blockchain-powered platform that ensures private, scalable, and secure computational intelligence. This approach aims to enhance the quality and equality of data and computational intelligence in challenging machine-learning problems. By utilizing the blockchain network, the proposed solution facilitates the safe and decentralized sharing of machine learning data and models. The study evaluates the effectiveness of the DCIaaS framework in biomedical image categorization and controlling hazardous waste as a case study for multimedia applications. The experimental results demonstrate that the proposed method achieves more accurate model training than decentralized training. The suggested method employs distributed ledger technology and serves as a platform for crowdsourcing machine learning model training to overcome the challenges of ensuring privacy in DaaS.

Dwivedi *et al* [23], The IoT has evolved as a novel technology capable of enhancing the standard of living and services within intelligent urban areas. This is because smart technologies have gotten better over time. Smart city apps and services can help improve areas like healthcare, transportation, education, and more. Even though the idea is interesting, consumer privacy on IoT devices is a big worry. Most methods of authentication don't give privacy or anonymity to people who are allowed to use them. The authors of this study presented an authentication approach that relies on Zero-Knowledge proof to confirm the identity of network devices while keeping the user's identity and any other provided information confidential. On a small scale, the authors used IoT-based healthcare applications to show how our system framework works. However, it's easy to make it work for a wider range of use cases where privacy-preserving authentication is needed. The second important thing that came out of this study was the creation of the ZKNimble data encryption technology, which is especially good for small devices. After verifying a user's identity through Zero Knowledge Proof, it

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

is possible to utilize the ZKNimble cipher to encrypt and decrypt information. Almaiah *et al* [24], argued that industrial IoT is becoming more important as it connects to more technologies and applications. It also has a lot of small sensors that it uses to sense its surroundings and collect data. These devices constantly collect, monitor, analyze, exchange, and send data to other nearby devices or servers through an open channel, such as the internet. Still, a centralized approach to IIoT makes security and privacy risks more likely to happen in IIoT networks. The authors addressed these concerns by showing a deep-learning architecture based on blockchain having two levels one is security and the other is anonymity. To provide security and anonymity, a blockchain scheme is built in which each participant is registered, verified, and certified using an improved Proof of Work based on smart contracts. A Bidirectional Long Short-Term Memory technique is employed in the development of a deep learning system to identify intrusions, while the Variational Auto-Encoder technique is utilized to safeguard privacy. The ToN-IoT datasets and IoT-Botnet are open to the public, so the results of the experiments are based on them. When the results of the simulations are matched to the standard models, it is clear that the new framework is better than the old one.

Kummar *et al* [25], The wide use of blockchain technology and big data (BD), which can be used in many different ways and is the subject of a lot of scientific and practical research, is being studied the most. Despite being in their nascent stages and undergoing testing, both Big Data and the Internet of Things (IoT) exhibit a promising capability to complement each other in terms of data collection. Blockchain has altered the way crucial business development matters, such as data-driven decision-making, data ownership, identification, trust, and decentralization, are addressed. In the present day, both machines and humans generate a wider variety of data than in previous times. Blockchain technology can serve as a solution for situations where there is no optimal method for managing, arranging, and preserving such data. The proposed blockchain solution for decentralized public institution management, IoT connectivity, solving problems with the digital property, and protecting private data has had a big impact on how BD has changed over time. This paper shows a cutting-edge way to solve the BD technology gap using Blockchain [23] [26] [27].

3. PROPOSED ARCHITECTURE

Observing privacy standards throughout the entire data lifecycle is crucial due to the mandatory compliance with GDPR legal requirements. This includes every stage, such as data collection, transmission, storage, and processing. Our responsibility is to ensure that the entire IoT ecosystem adheres to the privacy legislation and standards mentioned above. To achieve this, we offer the PrivChain platform, which safeguards data collected by IoT devices throughout their lifecycle. PrivChain's foundation is based on three principles: user-driven transparency, a decentralized design without a central authority, and strict privacy regulations [14] [28]. The proposed architecture, as shown in Figure 1, comprises two networks. One of these networks is designed for use in smart homes, buildings, and other similar settings and is referred to as a private IoT. The ownership of the data generated by the Internet of Things devices that make up this network can belong to either an individual or a corporation. The second network is a

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

public Internet of Things network that acts as an interface between the private Internet of Things network and the external world. There are three types of nodes in the network for the Internet of Things devices: storage nodes, public nodes, and private nodes [8] [20] [29] [30].

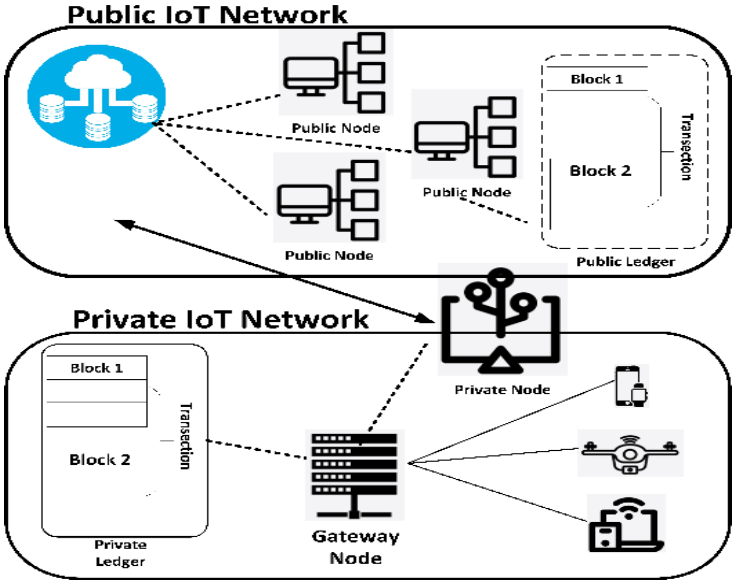

Figure 1: PrivChain Architecture

Both nodes that store data and those that connect to the IoT belong to the public network. A node in the IoT that can connect with both the public and private IoT networks is commonly called a private node, gateway node, or private IoT resource. In a private Internet of Things network, each data owner bears the responsibility of operating one or more gateway nodes to manage the devices within their control. Utilizing a private ledger or private IoT resources, a private blockchain enables the communication between the IoT assets of a data owner and the owner [6].

In an IoT network, the "public blockchain" is utilized to transfer messages between private nodes and other public nodes. The blockchain serves as an immutable public ledger that is safeguarded by a peer-to-peer network of participants using pseudonyms in the form of addresses. As a result, personal data protection can be achieved in the IoT using this approach. The use of a distributed public ledger allows for an increase in both the security and anonymity of user identities in IoT networks. Our solution provides users with the protection of their anonymity and pseudonymity at all times by utilizing public and private keys [9] [31].To ensure that individual transactions cannot be connected, it is essential to utilize a unique set of keys for each transaction. For instance, in a public Internet of Things network, the gateway node may use a different key pair for each transaction that occurs with an external node. This approach may necessitate users adhering to privacy best practices, in addition to the blockchain's inherent security features such as anonymity, pseudonymity, and unlinkability. A set of privacy principles for the Internet of Things has been developed to gain support from all stakeholders, which is based on a literature review, ISO standard (number 8), and the

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

General Data Protection Regulation (GDPR). We will describe the main components of the proposed framework in the following section.

A. Core Components

Table 1 illustrates the different elements that constitute a blockchain-driven resolution. The PrivChain framework is comprised of nine primary components, including a smart contract, a transaction, a private IoT network, a private ledger, a gateway node, local storage, a public IoT network, a public blockchain, and a storage node [1] [7] [16] [21] [32] [33].

Table 1: PrivChain Component

Name	Description
Transaction	Through transactions, IoT resources and network nodes can talk to each other. We define transaction types like TLocalStore, TAdd, TRemove, TAccess, TStore, TMonitor, TGrant Permission, TGetPermission, and TGetSharedResource.
Smart contract	It is a deal that everyone knows about and that is kept on the blockchain. We came up with three ideas for smart contracts: ownership, a privacy policy for subscriptions, and privacy permission settings. On the private blockchain, there are two smart contracts. The third can be found on the distributed ledger right now.
Private IoT network	It's a site where the owner can manage a variety of personal IoT resources, like smart homes or buildings.
Private ledger	Data owners can manage their own IoT resources with the help of a local private blockchain.
Gateway node	It has plenty of memory and storage space. Each gateway node produces keys for a specific set of private IoT resources and adds those keys to the IoT network.
Local storage	It is a program for saving data on your computer. It stores the data collected by IoT resources before sending it to the storage node, which is an external storage facility.
Storage node	It is a public node on the IoT network that stores data collected by IoT resources and the public blockchain.
Public blockchain	It's a record of all the transactions that public nodes in the public IoT network send to access or share IoT data. It can guarantee the procedures for auditing.
Public IoT network	It is a peer-to-peer network with many nodes that all have different amounts of memory and storage space.

B. Functionality

Our approach to ensuring privacy throughout the entire process is reliant on the implementation of smart contracts, which possess the following attributes: First, the Ownership smart contract must be modified to include the newly acquired Internet-of-Things asset. Secondly, all data obtained from a secure Internet of Things asset should be stored securely. Lastly, the individuals who employ the data should be informed about the outcomes generated by the IoT resource. To guarantee that PrivChain remains adaptable to evolving conditions, the succeeding prerequisites must be fulfilled:

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

1) Transaction Protocol for Adding Resource

A private blockchain stores the Ownership smart contract, and each gateway node contributes the addresses of its Internet of Things resources to the contract. Additional outputs can be installed on each IoT device, and the smart contract governs the level of protection and access for each output. The smart contract ensures that the owner's chosen privacy protection levels are maintained while they control the resource. The figure below illustrates the steps that an administrator must follow to set up a new Internet of Things resource. Suppose a gateway node generates two keys for an IoT resource and the corresponding smart contract for ownership management [3] [11] [17] [23] [34] [35].

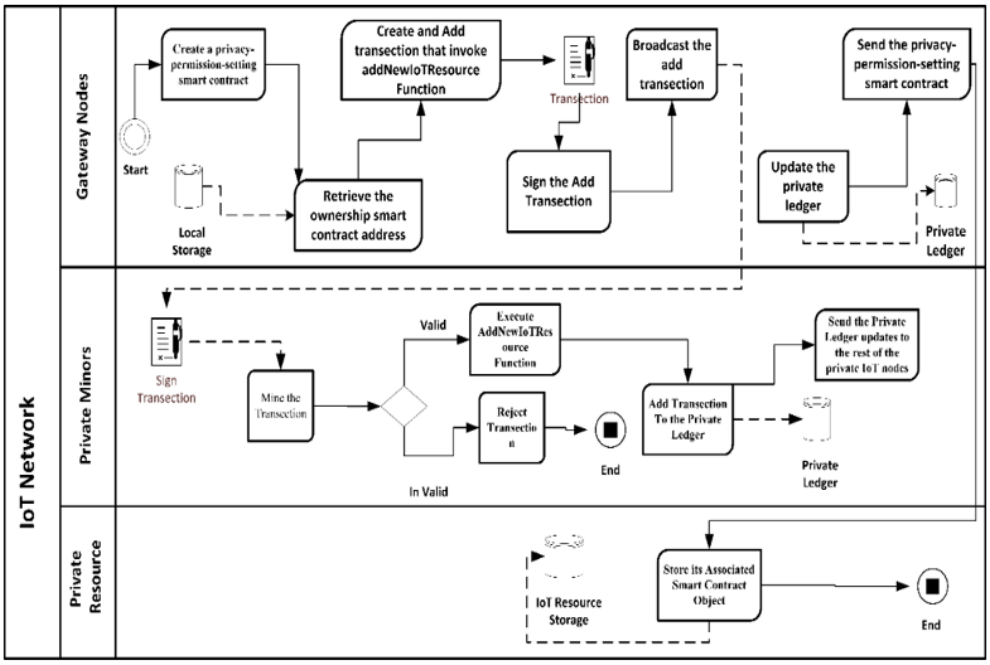

Figure 2: Addition of New IoT Resource

2) Transaction Protocol for Storing Resource

To achieve the task of storing data locally, the IoT device will send a TLocalStore transaction to the gateway node regularly. It is assumed that everyone is familiar with the location of the relevant gateway node, smart contract, and IoT resource.

I. Initially, the Internet of Things (IoT) resource generates a hash value, and subsequently, the outcome is encrypted with fast AES encryption. After the encryption, the encrypted data is transmitted to the gateway node through a secure connection.

II. The gateway node will first determine the data's hash before proceeding to decode the information it has been given.

III. The Local Store function of the smart contract is called into action whenever an Internet of Things (IoT) resource begins a new TLocalStore transaction.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

The data type, as well as the hash, are both a part of the transaction. Once the TLocalStore transaction is signed, it can only be sent to the relevant gateway node by the parent who holds the private key.

IV. Once the transaction has been received by the gateway, the data hash is compared to the data hash that was created in Step 2 to confirm that the data is correct. Before transmitting the transaction to the private IoT network, the gateway will check the credentials and, if they are valid, digitally sign the transaction. A denial will be sent for both the transaction and the related information unless one of the aforementioned conditions is met.

V. Once the miners have confirmed the correctness of the LocalStore function, it will be put to use to check who has access to the IoT resources. The data type that is associated with a transaction needs to be compatible with the output types that are supported by the Internet of Things (IoT) resource that is relevant to the transaction before it can be processed. If this condition is satisfied, the Privacy-Permission-Setting smart contract address for the Internet of Things resource output is retrieved and compared to the address that was supplied in the transaction. The gateway node will add the transaction to the blockchain and preserve the data locally if there is a match between the addresses and if the storage permission is set to "Permit." Should you fail to comply, you will risk having the information denied to you.

3) Transaction Protocol for Sharing Resource

When a client registers for an Internet of Things resource, a connection is made between the node where the registration took place and the output of the resource.

I. To begin, the customer will submit a subscription request, during which they will define the parameters of their desired subscription. These details will include the type of material, the distribution method, the target audience(s), and the length of time for the service. A TGetPermission transaction is utilized to submit this request to the data owner, and it should be directed to the email address provided by the data owner.

II. Secondly, a matching manager in the gateway node compares the subscriber's request to the security settings of the data owner. The Matching Manager takes into consideration both the consumer subscription demands as well as the constraints for user anonymity that are imposed by the output privacy regulation. If a match is found when getting the right address for the Subscription-Privacy-Policy smart contract, the Matching Manager will check to see if a file that already has the required information has been published. If it has, the Matching Manager will go on to the next step. In such a scenario, the results of processing the data that was given are saved in a fresh file. Last but not least, the Object() [native code] function of the Subscription-Privacy-Policy smart contract is carried out to generate a brand new instance. In addition to that, it gives the address of the node and a hash of the contents of the file.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

III. In the third step of the process, the gateway node is responsible for receiving the transaction before signing and broadcasting it to the rest of the network.

IV. After a data consumer has the smart contract address for the Subscription-Privacy-Policy, they can submit a TGetShared-Resource transaction, which utilizes a sequence of smart contract operations to manage the data. These operations can be found in the TGetShared-Resource transaction. Each function undergoes a preliminary check against the list of consumer rights to ensure that it complies with the privacy settings that have been selected by the data owner. If the retention period has not yet ended and the consumer has permission to share the contents of the file with other consumers, then the consumer can use the add-Consumer function to grant another consumer read-only access to the file for a specified amount of time. This access will expire after the retention period has ended.

4. PSEUDO ALGORITHM

Algorithm 1: Registration

Input:
- device_id
- device_address
- policy, contract_address

Output:
- **Transection_Status**

Start

1) If (user-verification(user-id) = = True)
a. register_device(device_id, device_address)
b. connect_to_network(node_address)
c. create_smart_contract(policy)
d. deploy_smart_contract(contract_address)

2) If (data-available() = = True)
a. create_blockchain_node()

3) If(get_smart_contract_state(contract_address) → True
a. get_device_address(device_id)
b. execute_smart_contract(contract_address, **device_id, action)**

ELSE
Transaction→ Failed
ELSE
create_blockchain_node()→ Failed
ELSE
User-verification(user-id)→ unsuccessful
End

register_device (device_id, device_address): It creates a new device with the given device_id and device_address, generates a unique address for the device, and stores the device address, id, and location locally.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

connect_to_network(node_address): This function connects to the network using the provided node_address. Then synchronize the local blockchain with the network blockchain. After that update the locally stored blockchain with the latest blockchain from the network.

create_smart_contract(policy): This function creates a new smart contract with the given policy, then compiles the smart contract code, generates a unique address for the smart contract, and Stores the smart contract address and code locally.

deploy_smart_contract(contract_address): It deploys the smart contract to the blockchain network at the given contract_address, verifies the deployment was successful and updates the locally stored smart contract address with the deployed address.

create_blockchain_node(): This function initialize an empty blockchain. Next, generate a unique address for the node. Finally, store both the node address and blockchain locally for future reference.

get_smart_contract_state(contract_address): It retrieves the state of the smart contract at the given contract_address and returns the state of the smart contract.

get_device_address(device_id): It searches the local device registry for the given device_id and return the device address associated with the device_id.

execute_smart_contract(contract_address, device_id, action): It retrieves the code of the smart contract at the given contract_address, verifies the validity of the device_id and the requested action against the contract policy, executes the requested action on the smart contract, and updates the state of the smart contract.

5. RESULTS AND DISCUSSION

To evaluate the effectiveness of our proposed approach, we conducted a simulation study using the Ethereum blockchain network. We simulated the deployment of 100 IoT devices in a smart city environment, each collecting data on a different aspect of the city. The simulation study was conducted using the following parameters:

Block size: 1 MB

Block time: 15 seconds

Gas limit: 10,000,000

We recorded the number of transactions, the transaction speed, and the amount of data stored on the blockchain network. The results are presented in the below Table 2.

Table 2: Results of the simulation study

Metric	Metric
Number of devices	Number of devices
Number of transactions	Number of transactions
Transaction speed	Transaction speed
Data stored on the blockchain	Data stored on the blockchain

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

As shown in the above table, our proposed blockchain-based approach was able to handle the data collected by the 100 IoT devices in the smart city environment, with a total of 2,369 transactions and 95.6 MB of data stored on the blockchain network. The transaction speed was 14.29 seconds per transaction, which is within an acceptable range for real-world applications. To compare our proposed approach with other approaches, we conducted a comparative analysis of centralized, hybrid, and blockchain-based approaches. The comparison was based on the following criteria:

Decentralization: the extent to which the approach is decentralized, with high indicating a fully decentralized approach and low indicating a centralized approach.

Privacy: the level of privacy offered by the approach, with high indicating a high level of **privacy and low indicating a low level of privacy.**

Security: the level of security offered by the approach, with high indicating a high level of security and low indicating a low level of security.

Scalability: the ability of the approach to scale up to handle large amounts of data, with high indicating high scalability and low indicating low scalability.

Efficiency: the efficiency of the approach in terms of processing power, memory usage, and energy consumption, with high indicating high efficiency and low indicating low efficiency.

Transparency: the level of transparency offered by the approach, with high indicating a high level of transparency and low indicating a low level of transparency.

Interoperability: the ability of the approach to interoperate with other systems and technologies, with high indicating high interoperability and low indicating low interoperability.

The results of the comparative analysis are presented below in Table 3.

Table 3: Comparative analysis of different approaches with the Proposed Approach

Approach	Decentralization	Security	Scalability	Interoperability	Efficiency	Transparency	Cost
Centralized	Low	Low	High	High	High	Low	Low
Hybrid	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Proposed Approach	High	High	High	High	Medium	High	High

6. CONCLUSION

Researchers found that blockchain and IoT produce strong, completely distributed, trustless, verifiable peer-to-peer networks. There are few IoT privacy solutions. Despite stricter rules, the Internet of Things industry has ignored privacy standards like consent, choice, purpose specificity, and collection restrictions. Due to these issues, we have prioritized blockchain-based privacy standards to protect IoT data at all times. We presented a smart contract-based system for end-to-end IoT data privacy. We created a

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

PrivChain with a few nodes to show the concept. Our multi-node IoT inquiry will let us test our architecture. Before we understand the PrivChain, we will publicly disclose many permission-granting and -requesting transactions. We compare gas performance. PrivChain's expected computing costs will be compared against other initiatives. Analyzing the blockchain may reveal a node's webpage or action frequency. Our technique allows one IoT resource to have many addresses. Our approach will leverage differential privacy to protect user data without sacrificing usability. Tampering with transactions prevents real-world blockchain analysis.

References

1. E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, “Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework,” *Information Systems Frontiers*, vol. 24, no. 2, pp. 393–414, 2022.
2. Z. Xihua and S. Goyal, “Security and privacy challenges using IoT-blockchain technology in a smart city: critical analysis,” *IJEER*, vol. 10, no. 2, pp. 190–195, 2022.
3. A. Rejeb, K. Rejeb, S. J. Simske, and J. G. Keogh, “Blockchain technology in the smart city: A bibliometric review,” *Quality & Quantity*, vol. 56, no. 5, pp. 2875–2906, 2022.
4. I. Calzada, “Citizens’ data privacy in China: The state of the art of the Personal Information Protection Law (PIPL),” *Smart Cities*, vol. 5, no. 3, pp. 1129–1150, 2022.
5. U. Khalil, O. A. Malik, and S. Hussain, “A Blockchain Footprint for Authentication of IoT-Enabled Smart Devices in Smart Cities: State-of-the-Art Advancements, Challenges, and Future Research Directions,” *IEEE Access*, vol. 10, pp. 76805–76823, 2022.
6. D. Li, Z. Luo, and B. Cao, “Blockchain-based federated learning methodologies in smart environments,” *Cluster Computing*, vol. 25, no. 4, pp. 2585–2599, 2022.
7. N. Six, N. Herbaut, and C. Salinesi, “Blockchain software patterns for the design of decentralized applications: A systematic literature review,” *Blockchain: Research and Applications*, p. 100061, 2022.
8. S. Myeong, J. Park, and M. Lee, “Research Models and Methodologies on the Smart City: A Systematic Literature Review,” *Sustainability*, vol. 14, no. 3, p. 1687, 2022.
9. D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, “A survey on blockchain for information systems management and security,” *Information Processing & Management*, vol. 58, no. 1, p. 102397, 2021.
10. M. A. Ferrag and L. Shu, “The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial,” *IEEE Internet of Things Journal*, vol. 8, no. 24, pp. 17236–17260, 2021.
11. O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, “A comparative study: Blockchain technology utilization benefits, challenges, and functionalities,” *IEEE Access*, vol. 9, pp. 12730–12749, 2021.
12. M. Das, X. Tao, and J. C. Cheng, “BIM security: A critical review and recommendations using encryption strategy and blockchain,” *Automation in construction*, vol. 126, p. 103682, 2021.
13. A. Vacca, A. Di Sorbo, C. A. Visaggio, and G. Canfora, “A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges,” *Journal of Systems and Software*, vol. 174, p. 110891, 2021.
14. P. Patil, M. Sangeetha, and V. Bhaskar, “Blockchain for IoT access control, security, and privacy: a review,” *Wireless Personal Communications*, vol. 117, pp. 1815–1834, 2021.

ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

15. K. Dey and U. Shekhawat, “Blockchain for sustainable e-agriculture: Literature review, architecture for data management, and implications,” *Journal of Cleaner Production*, vol. 316, p. 128254, 2021.

16. D. Guru, S. Perumal, and V. Varadarajan, “Approaches towards blockchain innovation: A survey and future directions,” *Electronics*, vol. 10, no. 10, p. 1219, 2021.

17. M. A. Jan *et al.*, “Security and blockchain convergence with the Internet of Multimedia Things: Current trends, research challenges, and future directions,” *Journal of Network and Computer Applications*, vol. 175, p. 102918, 2021.

18. A. Al-Qarafi *et al.*, “Optimal Machine Learning Based Privacy Preserving Blockchain Assisted Internet of Things with Smart Cities Environment,” *Applied Sciences*, vol. 12, no. 12, p. 5893, 2022.

19. P. M. Kumar, B. Rawal, and J. Gao, “Blockchain-enabled Privacy Preserving of IoT Data for Sustainable Smart Cities using Machine Learning,” presented at the 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), 2022, pp. 1–6.

20. C. Huang *et al.*, “Blockchain-assisted Transparent Cross-domain Authorization and Authentication for Smart City,” *IEEE Internet of Things Journal*, 2022.

21. M. A. Khan, “A formal method for privacy-preservation in cognitive smart cities,” *Expert Systems*, vol. 39, no. 5, p. e12855, 2022.

22. A. Peyvandi, B. Majidi, S. Peyvandi, and J. C. Patra, “Privacy-preserving federated learning for scalable and high data quality computational-intelligence-as-a-service in Society 5.0,” *Multimedia Tools and Applications*, pp. 1–22, 2022.

23. A. D. Dwivedi, R. Singh, U. Ghosh, R. R. Mukkamala, A. Tolba, and O. Said, “Privacy-preserving authentication system based on non-interactive zero-knowledge proof suitable for Internet of Things,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 10, pp. 4639–4649, Oct. 2022, doi: 10.1007/s12652-021-03459-4.

24. M. A. Almaiah, A. Ali, F. Hajjej, M. F. Pasha, and M. A. Alohali, “A Lightweight Hybrid Deep Learning Privacy Preserving Model for FC-Based Industrial Internet of Medical Things,” *Sensors*, vol. 22, no. 6, p. 2112, 2022.

25. S. Kummar, B. Bhushan, and S. Bhatia, “Blockchain Based Big Data Solutions for Internet of Things (IoT) and Smart Cities,” in *New Trends and Applications in Internet of Things (IoT) and Big Data Analytics*, Springer, 2022, pp. 225–253.

26. N. Rasool, S. Khan, U. Haseeb, S. Zubair, M. W. Iqbal, and K. Hamid, “Scrum And The Agile Procedure’s Impact On Software Project Management,” Jilin Daxue Xuebao GongxuebanJournal Jilin Univ. Eng. Technol. Ed., vol. 42, pp. 380–392, Feb. 2023, doi: 10.17605/OSF.IO/MQW9P.

27. K. Hamid, M. W. Iqbal, H. Muhammad, Z. Fuzail, and Z. Nazir, “ANOVA Based Usability Evaluation of Kid’s Mobile Apps Empowered Learning Process,” Qingdao Daxue XuebaoGongcheng JishubanJournal Qingdao Univ. Eng. Technol. Ed., vol. 41, pp. 142–169, Jun. 2022, doi: 10.17605/OSF.IO/7FNZG.

28. H. Riasat, S. Akram, M. Aqeel, M. W. Iqbal, K. Hamid, and S. Rafiq, “Enhancing Software Quality Through Usability Experience and HCI Design Principles,” vol. 42, pp. 46–75, Feb. 2023, doi: 10.17605/OSF.IO/MFE45.

29. D. Hussain, S. Rafiq, U. Haseeb, K. Hamid, M. W. Iqbal, and M. Aqeel, “HCI Empowered Automobiles Performance by Reducing Carbon-Monoxide,” vol. 41, pp. 526–539, Dec. 2022, doi: 10.17605/OSF.IO/S5X2D.

30. K. Hamid, H. Muhammad, M. W. Iqbal, A. Nazir, shazab, and H. Moneeza, “ML-Based Meta Model Evaluation of Mobile Apps Empowered Usability of Disables,” Tianjin Daxue Xuebao Ziran Kexue Yu Gongcheng Jishu BanJournal Tianjin Univ. Sci. Technol., vol. 56, pp. 50–68, Jan. 2023.

ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 04-2023
DOI 10.17605/OSF.IO/8BMZ4

31. K. Hamid, H. Muhammad, M. W. Iqbal, S. Bukhari, A. Nazir, and S. Bhatti, “ML-Based Usability Evaluation of Educational Mobile Apps for Grown-Ups and Adults,” Jilin Daxue Xuebao GongxuebanJournal Jilin Univ. Eng. Technol. Ed., vol. 41, pp. 352–370, Dec. 2022, doi: 10.17605/OSF.IO/YJ2E5.
32. K. Hamid, M. W. Iqbal, Z. Nazir, H. Muhammad, and Z. Fuzail, “Usability Empowered by User’s Adaptive Features In Smart Phones: The Rsm Approach,” Tianjin Daxue Xuebao Ziran Kexue Yu Gongcheng Jishu BanJournal Tianjin Univ. Sci. Technol., vol. 55, pp. 285–304, Jul. 2022, doi: 10.17605/OSF.IO/6RUZ5.
33. K. Hamid et al., “Usability Evaluation of Mobile Banking Applications in Digital Business as Emerging Economy,” p. 250, Feb. 2022, doi: 10.22937/IJCSNS.2022.22.2.32.
34. H. Muhammad et al., Usability Impact of Adaptive Culture in Smart Phones. 2022.
35. K. Hamid, M. waseem Iqbal, M. Aqeel, X. Liu, and M. Arif, “Analysis of Techniques for Detection and Removal of Zero-Day Attacks (ZDA),” 2023, pp. 248–262. doi: 10.1007/978-981-99-0272-9_17