Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 3, pp. 1321–1331, DOI 10.12694/scpe.v25i3.2628

MINIMIZING OVERHEAD THROUGH BLOCKCHAIN FOR ESTABLISHING A SECURE SMART CITY WITH IOT MODEL

ZHIXIONG XIAO[*]

Abstract. Conventional safety measures are inconsistent with inexpensive technologies like the Internet of Things (IoT) due to their significant storage traces, which are prohibitive to their utilization. The blockchain (BC) framework maintains the five essential security primitives: genuineness, credibility, secrecy, accessibility, and non-renunciation. Most IoT gadgets have limited resources, so a traditional blockchain deployment is inappropriate. Traditional deployment of blockchain computing in the Internet of Things leads to significant power consumption, delay, and computational inefficiency. The proposed solution improves the blockchain's conception to serve IoT technologies better. This article proposes a blockchain-based intelligent city design for the IoT that keeps all encryption safety precautions in place. Adding blockchain to an IoT platform does not add much extra labour. After comparing all safety requirements to existing literature, it is clear that the proposed method achieves satisfactory safety effectiveness.

Key words: Internet of Things, Blockchain Computing, Smart City, Encryption, Cyber Security.

1. Introduction. The Internet of Things (IoT) might provide high-quality, low-overhead, and human-free answers to many problems in many fields. Developing "smart communities," which integrate various IoT-enabled activities such as intelligent conveyance, intelligent garbage administration, smart accommodation, and smart water, is an essential use of the technology. Such a wide range of offerings gives developers of smart city collaboration apps much flexibility [1].

The concept of a "smart community" within a "smart city" refers to creating information technology to provide comprehensive regional collaboration services based on electronic records and technology, with the ultimate goal of enhancing the standard of life for city citizens. When multiple companies must work together to get a job done, keeping private data safe and secure cannot be easy [2]. Information security and privacy must be prioritized, and citizens and policymakers require reliable data access. The online security framework for software-defined networks (SDN) and smart contract-enabled governmental smart towns relies on authorization and validation for usage in limited environments. This layout was developed for times when funds are tight. The proposed security framework for shared service delivery is now being piloted on the distributed ledger Blockchain networks [3].

The shared task of designing a smart city, a fresh take, is provided for using intelligent agreements in numerous blockchains to protect sensitive information at every stage [4]. The safety measure uses the adaptable nature of intelligent contracts for the confidentiality and integrity of all transactions and interactions between diverse IoT networks. The authors built and ran a use case involving collaborative services inside an SDN-enabled Internet of Things framework to test the viability of the proposed service safety framework. As the global population increases and the idea of smart cities becomes a reality, developing novel approaches to environmental tracking and management, citizen well-being, and government effectiveness will become more crucial. This research's proposed design aids the communication framework of disparate Internet of Things (IoT) networks, letting them link up and cooperate on various tasks. The strategy suggested by the authors will utilize novel safety techniques [5].

The recommended structure for a smart city explains how the IoT gadgets on various networks should register with one another, exchange data, and carry out adaptive application security measures. The researchers found that the proposed method scales well, even when the number of queries made throughout the length of

[*] Urban Construction College, Fuzhou Technology and Business University, Fuzhou, Fujian, 350715, China (Corresponding author's e-mail: zhixiongxiao7@126.com)

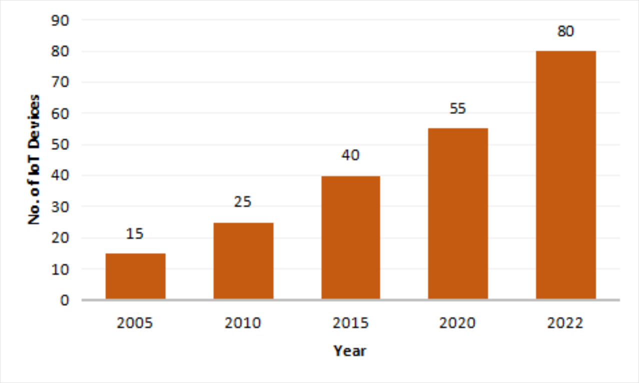

Fig. 1.1: Survey report for the blockchain-based IoT in smart city

an interaction between two separate IoT networks during work together. A high degree of authorization, compatibility, and the transfer of health data are all made possible through the application of blockchain-based technologies for drug supply management (DSM). Academics have shown a surprisingly high interest in IoT-based urban planning during the past several years [6,7].

By providing access to various high-tech services, ”smart cities” (SC) aim to raise the living standards of their residents. Smart cities, the Fourth Industrial Revolution, and innovative banking are just a few examples of these uses. SC may offer a higher level of security by implementing blockchain technology (BCT). For this goal, events are recorded in an immutable, encrypted, autonomous online database open to public inspection. The study's overarching goal is to thoroughly explore the present state of research using state-of-the-art technologies like BCT and the IoT in DSM and SC. Figure 1 shows the blockchain in the IoT model under a secure smart city.

2. Literature Review. The development and layout of DSM and SC programs that use BCT and IoT are focused on the first group. The second category includes a wide range of research into BCT and IoT applications in DSM and SC settings. The third type of contribution is reviewing papers on incorporating BCT and IoT into DSM and SC-based systems. The author provides an overview of the many benefits of employing BCT and IoT in DSM and SC, as well as suggestions for overcoming some of the challenges that have been identified. The new work adds to the corpus of information by analysing all potential avenues in-depth and pinpointing gaps in the understanding. The relevance of BCT and its execution are thoroughly discussed, giving academics a thrilling opportunity to develop more decentralized DSM and SC applications and resulting from extensive dialogue on the usefulness of BCT and the steps needed to put it into practice [8].

This research analyses the chosen literature to determine how BCT is used for IoT and how it enhances the organization of data processes. This study is an in-depth examination and classification of blockchain technology with the IoT and other SC and DSM applications. This analysis and classification reveal many recurring themes in the literature on the topic. BCT can handle several types of big data, use secure information in both digital and physical environments, and not depend on a single point of failure, all contributing to its rising appeal as a solution for handling data. Furthermore, it can decode encrypted data even when disconnected from the internet. Several studies have looked into different aspects of data management to see if these objectives have been met. These aspects include data collection, processing, security, distribution, retrieval, and storage [9].

The BCT-based solutions raise the standard in IoT and secure communication areas. Enhanced identification features like data collecting may allow BCT-based computer systems to produce more. One application of this idea is the usage of public keys inside encryption methods. The improved authentication capabilities provided by BCT-based systems also facilitate other data management activities, such as data collection [10].

A safer cryptographic method provides the features of data collection. Various authentication procedures, from biological processes to public-key encryption techniques, have allegedly been used. Fingerprinting is one method in this category. Similarly, a growth in the popularity of electronic contracts is an advantage brought about by using BCT in data processing. Although smart contracts were around long before BCT became popular, they were rarely employed as a data processing tool until BCT became mainstream. However, blockchain technology is used in various ways by platforms built on it, including handling data automatically. Transmission and recovery professionals in the field of data management should be noticed. Despite this, several writers provide a clear and concise account of the distribution strategies they employed in their deployments. However, the authors found various factors significantly impact data storage. The designers find ways around these restrictions by establishing a data lake, registering a file catalogue, and storing only file locations. Developers constantly adjust their code to adhere to regulations [11, 12].

BCT and IoT devices have immense potential to revolutionize the healthcare industry, smart cities, and other sectors like agriculture, transportation, and manufacturing. Because the Internet of Things (IoT) uses such a wide variety of recent technological advancements, it is not feasible to construct a single suggested architecture that could be used as a master plan to accommodate all potential requirements. There are specific potential applications of the IoT that have yet to be investigated or need sufficient knowledge on how to approach them [13]. It demonstrates the need for further study in this challenging field to discover new and possibly significant societal advantages. Although smart cities give inhabitants and suppliers of capital a variety of benefits, there are many ways in which breaches might endanger people's health and safety. As a direct consequence of this, the IoT may accommodate several distinct suggestion schemes at the same time. This study investigates the relationship between technology and morality related to the safety of IoT-enabled technologies in modern urban construction. Therefore, it offers a secure IoT network architecture for smart cities that combines blockchain technology and deep intelligence to protect users' privacy and trustworthiness [14].

The structure was developed by combining blockchain technology with advanced intelligence. This system uses the blockchain network for risk assessment and mitigation in the context of intelligent city facilities. A neural network model and an optimization approach are both included in this structure. The optimization algorithm ensures that the smart city infrastructure optimizes its resources. In this study, a secured smart city infrastructure employing a blockchain and deep intelligence architecture is built. This infrastructure aims to guarantee that IoT connectivity in smart cities is trustworthy and protects users' privacy. According to the prior discussion, sophisticated deep learning powered by blockchain mechanisms might be merged to handle computational intelligence and security challenges on the IoT-enabled intelligent urban infrastructure. The operational insights made possible by fog and edge cloud apps increase the ability to transform massive amounts of data that are either stationary or in motion into activities that begin immediately. A neural network model and an optimization algorithm are both included in this structure. The optimization algorithm ensures that the smart city infrastructure optimizes its resources [15].

To succeed smart city new solutions will be required in the following six areas: ecological living and health, energy, safety and security, finance, government and schooling, and transportation. Many recent technological advances may be traced back to the exponential growth of the IoT over the past few decades, including the notion of the smart city. To improve the quality of life in healthcare, trade, farming, and conveyance, a ”smart city” is built by integrating IoT devices with technological advances in communication and information. It is crucial to build these technologies safely to prevent attackers from penetrating the existing systems, but many new privacy hazards and challenges have emerged due to this advancement [16].

Blockchain, a relatively recent innovation built on cryptographic rules, may play a crucial role in the safety of future smart cities. This research covered a wide range of blockchain applications for smart cities. The authors examined whether and how blockchain technology's openness, republic, restructuring, and safety advantages may improve smart city services. This research will allow the implementation of an intelligent contract voting system based on the Ethereum blockchain, revolutionizing electronic voting use. The authors focused on the problem of inadequate security precautions in smart cities and offered many options for improving safety based on the research. The studies have focused primarily on blockchain technology and its potential to enhance the safety and privacy of smart city services. Based on the blockchain platform, researchers' solution will facilitate the development of a trustworthy and distributed digital voting mechanism. The authors suggested a voting system that uses technology as the principal service to facilitate voting in smart towns. Voting in smart cities may be simplified with the help of our technology. After all, a distributed digital voting system may have its flaws owing to the reality that it is still an infant technology. Therefore, additional study and investigation of the technology are needed. Sybil's attack is one of the threats to a digital voting system because it uses a vulnerability that may enable a voter to create many identities on a blockchain network [17].

The Ethereum blockchain houses intelligent contracts and user funds in a wallet. On the digital currency Ethereum, accounts manage user authentication by generating encoding content, which forms the backbone of the existing construction for voting online. While the user's private key remains secure, any other peer on the internet may read the public key [18, 19]. Smart contracts are used to automate core aspects of the voting process, including voter verification and tallying. Once consensus is reached across nodes, payments are checked for accuracy before being added to a new block on the distributed ledger. The computerized voting procedure is speculated to be powered by the Ethereum blockchain. Adding a block to the blockchain causes irreversible changes to the blockchain. The update is also sent to all nodes through broadcasting. Furthermore, it guarantees that voters are legitimate, that contract events are widely broadcast and distributed, and that all network participants may access these exchanges, but only one person can unlock them [20].

Multiple safeguards are in place to secure users' private data stored in the public cloud, which is essential for the growth of smart cities. Social manipulation and hacking are two forms of deception that criminals may employ to get access to private user data. These methods may be exploited to steal users' credentials and financial data. Phishing is still the initial stage of a multiple-phase assault, although its technological sophistication has dramatically increased over the past few years. Deception kits have evolved into tools for attack that have become more intuitive, readily available, and simple to deploy over time [21].

Utilizing non-Latin symbols in the URL, typo-squatting of eminent domains, using protected symbols in redirections, and multiple chains scamming indicate a successful scamming campaign. When files containing phishing URLs are uploaded to cloud storage, hackers are offered a helping hand and a push in the right direction. Criminals' use of cloud servers for these kinds of assaults is becoming more common. Current spoofing URL blocking software does not provide enough defence against multilayered phishing. Instead, it is up to the user to take precautions, making them ultimately responsible for their safety. The indestructibility of blockchain data and the impact of avalanches further demonstrate the efficacy of these protections as prerequisite measures to implement. Altering in a method supported by blockchain technology is the most effective solution to safeguard users' cloud-based data [22].

Certain restrictions are embedded in phishing, and the time it takes to mine a block on the Ethereum network has increased due to the standard complexity level. If the CSP has access to a privately configured blockchain with the Phish Block algorithm, then the CSP may change the protocol to speed up the blockchain's block generation process. Incorporating Phish Block as a product would increase security for cloud data and users and provide value as a trust component to the cloud provider's service level contract [23].

3. Materials and Methods. The entire system may be classified into three distinct components: programmable blocks, canopies system, and cloud computing [24]. The components are explained as follows:

A. Programmable Blocks. ”Smart constituents” are commonly referring to these smaller divisions. Each smart building block has various detectors, including a sensor for imaging, temperature, LDR, etc. These sensor-equipped gadgets belong to a single block administrator and may only be accessed by that individual. The many bits of data gadgets are kept on an encrypted blockchain managed by the blocking administrator. In contrast to how Bitcoin's database is managed—by a decentralized network of nodes—the local BC is managed by a central authority. The block operator will connect all activities made with or via the devices.

The block administrator is responsible for updating the ledger with new gadgets or removing existing ones. Adding device operations will operate similarly to Bitcoin's' make coin' operation. The local BC has an authority element that allows the block administrator to control every exchange throughout the local blockchain. Only with the approval of the block's operator will electronic devices be allowed to communicate and share any necessary data. Authorization for the operations, it may be possible to utilize the Diffie-Hellman algorithms key transfer mechanism to enable the collaboration of a shared key. While the entry header for each block in the blockchain is recorded in that block's header, only the latest header is used to verify transactions. The suggested encrypted blockchain does not use evidence of work or any other challenges to reduce the associated expenses.

After appending a reference to the initial transaction and duplicating the policy from the preceding block's header, the user attaches the entire block to the distributed ledger. When an activity is included in a block using the algorithm underpinning Bitcoin, it is regarded as legitimate, irrespective of the fact that the block has been processed. Keep in mind that a personal blockchain may be set up to manage not just user authorization but also collaboration between gadgets, in addition to generating and recording securely in an immutable ledger, both operation data and scenario-based IoT agreements. Every intelligent building block will have its digital storage and a set of public credentials to provide user entry to the information stored in neighbouring units.

B. Canopy Network. Lantern is a network operated by peers made up of intelligent buildings and other individuals, including law enforcement agencies and government public administration entities. Every group of the canopies network's nodes elects a Group Head (GH) by a majority vote of the cluster's participants. Each GH must keep a public blockchain operational. The GHs remember the public key pairs of the consumers and use this information to decide whether or not the requester is authorized to see the information stored in the associated intelligent blocks. The public keys of requestors of bright bricks that belong to this set and may be retrieved are likewise managed and stored by the GHs.

C. Cloud Computing. The cloud is an official associate of the Group Head. The smart block's constituent gadgets could sometimes choose to back up their information to the cloud. This information must be shared with an outside organization to make these features available on mobile platforms. Suppose a limited number of additional state or centralized institutions opt to access the information in creative blocks. In that case, they will have read-and-write access to the information preserved in the data centre.

All interactions between nearby gadgets and canopy nodes are identified with activities. The proposed platform can accommodate five distinct types of trades. Suppose the intelligent gadgets inside the block want to save their data somewhere other than in memory, such as the block administrator's file system or the cloud. In that case, this will be considered as a Write operation. A read transaction will be started if the block manager, several states, or a central institution decides to access information stored in the cloud. A monitor transactional will be generated if additional states, centralized businesses, or block managers want to request data from monitor devices directly. An inception operation is utilized to add a new device to the intelligent block, and an elimination activity is performed to remove a device that already exists from the smart block. Every transaction entering or leaving the intelligent block will be documented on the distributed local ledger to the intelligent block. Data security concerns will be addressed by using an inexpensive hashing technique.

4. Proposed Methodology. The process for this inquiry may be broken down into four main parts. The low-processing platform's requirements are defined during the setup phase. Higher productivity (HP) nodes have their underlying files, including block admin and group head, set before launch. It shows how actual data is sent across the local and canopy networks throughout the exchange of information. A smart city's whole infrastructure, comprising intelligent interference, overhead system, and online storage, is shown in Figure 4.1.

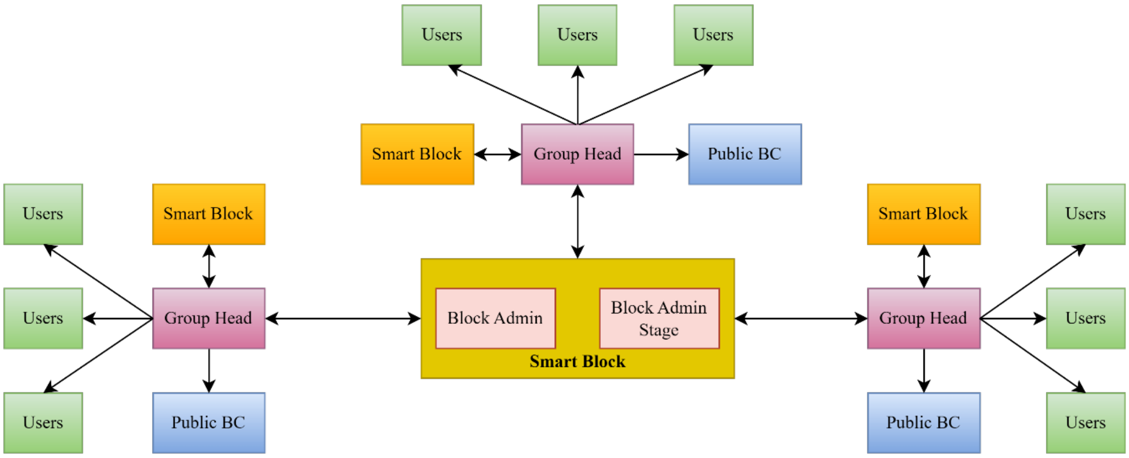

Fig. 4.1: Proposed Intelligent Smart City Infrastructure

a) Initialization. Low-processing (LP) area and high-processing (HP) block administrators and canopies networks are catered to design by two distinct startup methods. Both HP and LP have limited computational capabilities.

In step one, Low Processing (LP) Initialization has ’m’ total connections. An unlimited number of ’n’ sensors may be connected to each system component. Each node has its unique device ID and three keys. Three keys are required to encrypt a symmetrical key: the public, private, and actual. All nodes and block administrators get the encrypted key using an efficient critical transfer procedure. The unique identification of the gadget is the hash of its standard key. The Bitcoin account ID may also be calculated using the public key’s hash value. The uniqueness of a random integer’s hash might be verified using the hash attribute.

In step two, high-performance (HP) initialization, low-performance nodes use an inexpensive cryptographic approach to protect the data they collect from the sensors before sending it to the high-performance (HP) end nodes. High-level nodes that process messages will receive these packets and check their sender equipment ID, sensors ID, list of public keys, authorization header, transactional type, and hash information before continuing the procedure. All high-end processing nodes must agree that the transaction is valid before authorization, and their copy of the transactions is added to the blockchain. The organizational head in the overhead networks and the blocking administrator in the local network are examples of the high-processing units that we have encompassed into our architecture. The local blockchain maintained by the block supervisor must keep a copy of all transactions. Under certain conditions, the deal may be published on the public blockchain managed by the group’s leader. The group’s leader and the block administration are privy to the node’s open keys and the header controlling who may access them. Validation of the access management header, receiver devices ID, sensor ID, list of publicly accessible keys, and hash information will precede every interaction from the minor processing nodes to the district admin and the block administrator to the group person.

b) Transactions. Introducing new gadgets, deleting old ones, and transferring information comprise the three activities that may be performed in the proposed design. Like the genesis operation of BC, the add device operation will add the new gadget’s public key to the list of publicly accessible keys the block manager keeps. The public key will be deleted from the essential public list maintained by the blocking administrator as part of the deactivated device operation. It will keep the chain alive and well in the blockchain itself. There will be two distinct types of data transmission operations. The first tier of the structure consists of minimally processed nodes, which may transmit sensor data to the block administrators and receive data from the block admin.

Assume that video gauges are relaying, from the low analyzing node to the block manager, the number of automobiles that have passed through a given lane and that the block administrators utilize the resulting data to continually calculate the length of time that the green light must stay on for vehicles passing through that

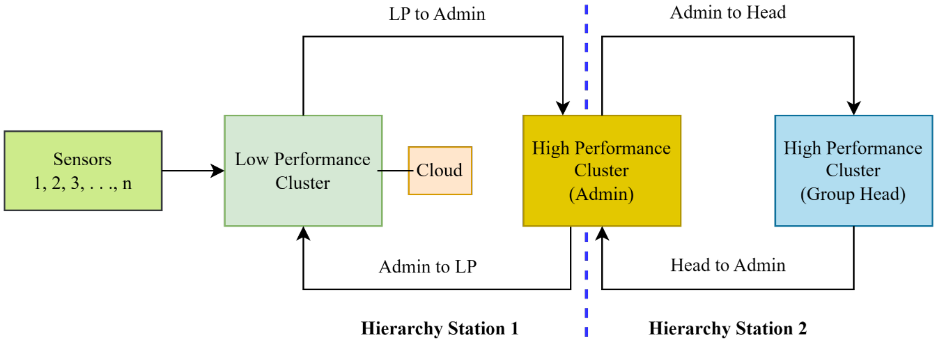

Fig. 4.2: Transactions at various Hierarchical levels

lane. The block administration can send information to the organization's group head, and the group head can send information back to the block manager at the subsequent level of the structure. Let us pretend that the state or federal government has to keep an eye on data gathered from a camera put in some intelligent block through the group head. Figure 3 depicts the two operations that involve the organizational structure.

c) Packets. Every message in this architecture travels only between the LP and HP nodes. The data within the frame is constantly generated by the LP and is used either in the HP memory or at the LP's production. Three parts make up the package that is made in LP.

1. The data collected by the LP's detectors is protected using the symmetrical key algorithm for encryption. The blockhead HP is given access to the encrypted symmetrical key using the Diffie-Hellman method.
2. The LP generates a hash of every sensor reading using the lightweight method to ensure the packet is uncorrupted.
3. An electronic signature is generated when the LP encrypts the encrypted information using a personal key and a public-key encryption algorithm.
4. Accessibility Control Preamble: The access management header stores the different storage types' read/write authorization. Each LP has its specialized sensor, and the results of these readings are often saved in either the block administrator's local database or the principal network's cloud database. Each output in an LP may access the block administrator's storage for retrieving information. According to the use case, numerous sensors can need access to different data or systems.
5. Extra Information: Time mark, biosensor ID, and gadget ID (LP ID) are also included in the previously mentioned package.

d) Process Flow. The following is the sequence in which components of the regional network's design are activated:

- All private and public keys are precomputed and maintained in LPs; connected block managers get LPs' public keys using the Diffie-Hellman technique. Due to its limited computational power, the architecture never generates private and public keys at the LP level.
- The standard symmetrical key is sent from the block administrator to the LPs via the Diffie-Hellman method.
- After various LP nodes collect information from different devices, it is scrambled and encoded using symmetrical keys before being put to use. The scrambled information is re-encrypted with the corresponding private key to create an electronic signature.
- The data is encrypted with a symmetrical key, the hash value is generated using a mapping technique, and the private key is encrypted with an asymmetrical essential cryptographic procedure, all inside the context of the LP technique. The resultant data packet is secure, and the wireless network device relays this signal to the building manager.
- All of the data streams from the different LPs are received by a PHP-based applications periphery

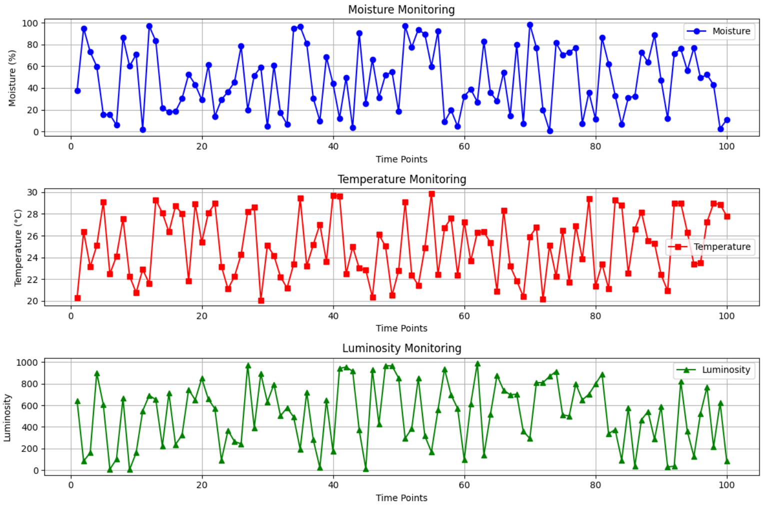

Fig. 5.1: Moisture, temperature and luminosity monitoring at various time points

interface (API). To verify the electronic authorization, the preceding API collects the device or LP ID and receives the corresponding public key from the LP. If the electronic identity checks out, the packet comes from the expected device or LP ID. The shipment will be returned to the sender if its signature does not match. The hash value will likewise be checked to ensure the packet's authenticity.

After verifying the algorithm's hash and authorization, the raw data can be accessed using the standard key and recorded in the relevant record of the block administrator's blockchain. To organize head operations, the block administration must follow the same steps.

5. Experimentation and Results. The single-chip Node MCU acts as the LP in our structural concept and is connected to monitors for measuring moisture, temperature, and luminosity. Figure 5.1 demonstrates the moisture, temperature, and luminosity monitoring at various times.

The DHT11 sensor is a combination thermometer and hygrometer, the level of light detection and the Light Detection Resistant (LDR) tool for taking measurements. The block administrator uses a standard personal computer. The LP public essential list, authorization header, and local network are all stored in a MySQL store. The API is written in PHP to get all the information from the sent packets. The Ethereum infrastructure activates the shade connection, and Figure 5.2 defines the data train Vs test.

Table 5.1 ensures that the five principles of cryptography are satisfied by the appropriate measures. The five principles are secrecy, accessibility, reliability, verifiability, and nonrepudiation. An analysis of the suggested layout of the existing Bitcoin structure and a recent application as a standard is provided in Table 5.2.

The most fundamental issue with constructing a distributed ledger is the Merging Overhead, discussed in considerable detail in the third row of Table 2. All previous activities are part of the Bitcoin blockchain, and new mining is needed to download the entire chain in its present form and the article. The proposed solution adds the public identity of each newly joined user to a separate private ledger and retrieves every previous transaction recorded in its blockchain. This blockchain stores the public keys of all permitted users, including the block admin's public key.

In this blockchain, all changes, including additions and deletions of devices, are continuously recorded by cryptography. The canopy network's leader also adopted this strategy across its system. The simulated result of blockchain technology for IoT with a mini batch size of data processing in percentage is shown in Figure 5.3.

When public keys are stored using blockchain systems, malicious devices cannot access networks or communicate with block controllers to obtain passwords. Due to the absence of the malicious device's public key in the public key blockchain, it will be unable to complete any packet transactions.

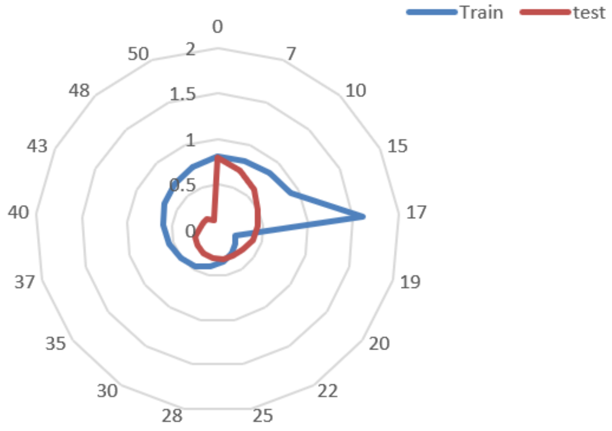

Fig. 5.2: Data Train Vs Test

Table 5.1: Principles of Cryptography

Safety Problems	Recommended Response
Secrecy	Every exchange is encrypted with a symmetric key.
Reliability	It is the hash of all transactions.
Accessibility	When a legitimate user requests an internet service, the regional and remote networking permissions management header processes the inquiry.
Validation	Using a ”connection statement” and ”displayed keys” does this.
Nonrepudiation	The agreement creator signs all regional and global operations to ensure no repudiation. Furthermore, as a result, no party can dispute their role in an arrangement.

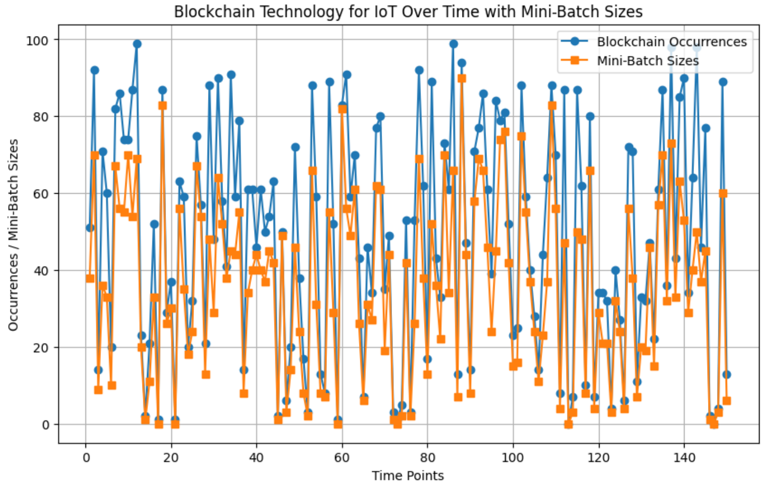

Fig. 5.3: Mini batch size of data in percentage for IoT over time

Table 5.2: Examination of New and Established Blockchains

Factor	BitCoin	Local BC	Public BC	Proposed Local BC	Proposed Public BC
Removal	PoW	Nothing	Nothing	Nothing	Nothing
BC capacity	Public	Private	Private	Private	Private
Client combination in the clouds	Download all blocks on the PC	Download all blocks on the PC	Download all blocks on the PC	Download all blocks in PC and public key	Download all blocks in PC and public key
BC manage	Nothing	Owner	Nothing	Owner	Nothing
Double spend	Not possible	Not applicable	Not applicable	Not applicable	Not applicable
Operation Type	Broadcast	Unicast	Unicast/ Multicast	Unicast	Unicast/ Multicast
Operation Parameter	Input, Coin output	Block-no, Hash data, PK time, Output, Policy rules	Output, PKs	Block-no, Hash data, PK time, Output, Policy rules	Output, PKs
Block Description	Hash puzzle	Policies	Policies	Access header	Access header
Encryption procedure	Public key cryptography	Not studied	Public key, Symmetric key	Public key, Symmetric key	Public key, Symmetric key
Forking	Not Permitted	Permitted	Permitted	Permitted	Permitted
54% attack	Double spending	Not possible	Not possible	Not possible	Not possible
Remuneration	Coins	Nothing	Not defined	Nothing	Nothing
Pool removal	Permitted	Can't be defined	Can't be defined	Can't be defined	Can't be defined
Malicious User	Permitted	Possible	Not possible	Not possible	Permitted
Miner division	Self- -selection	Owner choice	Node in group choice	Owner choice	Node in group choice

6. Conclusion. Conventional safety measures should be avoided wherever possible due to the enormous temporal and spatial requirements of IoT applications. The traditional structure of the blockchain system is altered in this study so that it may be used for IoT applications. The structure that is being suggested maintains anonymity while also ensuring genuineness, accessibility, honesty, and acceptance. This blockchain relies on the IoT program, and it can prevent various common assaults, including the denial access threat, the 53 % threat, the alteration threat, the computational threat, the person in the centre attack, the throwing threat, and others. The analysis of the suggested layout is better than the previously published material, and demonstrates that it satisfies and exceeds the expectations of several significant concerns.

REFERENCES

[1] M. E. Pamukov and V. K. Poulkov, ”Multiple negative selection algorithm: improving detection error rates in IoT intrusion detection systems,” in Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), pp. 543–547, Bucharest, Romania, September 2017.

[2] A. Islam, A. Al Amin, and S. Y. Shin, ”FBI: a federated learning-based blockchain-embedded data accumulation scheme using drones for internet of things,” IEEE Wireless Communications Letters, vol. 11, no. 5, pp. 972–976, 2022.

[3] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram. Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pages 618–623, March 2017.

[4] A. Islam, T. Rahim, M. Masuduzzaman, and S. Y. Shin, ”A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using internet of drone things,” IEEE Wireless Communications, vol. 28, no. 4, pp. 166–173, 2021.

[5] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan. Future internet: The internet of things architecture,

possible applications and key challenges. In 2012 10th International Conference on Frontiers of Information Technology (FIT): Proceedings, pages 257– 260. Institute of Electrical and Electronics Engineers Inc., 2012.

[6] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, Princeton, NJ, USA, 2016.

[7] A. Khannous, A. Rghioui, F. Elouaai, and M. Bouhorma, "MANET security: an intrusion detection system based on the combination of Negative Selection and danger theory concepts," in Proceedings of the 2014 International Conference on Next Generation Networks and Services (NGNS), pp. 88–91, Casablanca, Morocco, May 2014.

[8] A. Mosenia and N. K. Jha. A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4):586–602, Oct 2017.

[9] P. Widulinski and K. Wawryn, "A human immunity inspired intrusion detection system to Search for infections in an operating system," in Proceedings of the 2020 27th International Conference on Mixed Design of Integrated Circuits and System (MIXDES), pp. 187–191, Lodz, Poland, June 2020.

[10] Manik Lal Das. Privacy and security challenges in internet of things. In Raja Natarajan, Gautam Barua, and Manas Ranjan Patra, editors, Distributed Computing and Internet Technology, pages 33–48, Cham, 2015. Springer International Publishing.

[11] A. Borkar, A. Donode, and A. Kumari, "A survey on intrusion detection system (IDS) and internal intrusion detection and protection system (IIDPS)," in Proceedings of the 2017 International Conference on Inventive Computing and Informatics (ICICI), pp. 949–953, Coimbatore, India, November 2017.

[12] M. Kumar and A. K. Singh, "Distributed intrusion detection system using blockchain and cloud computing infrastructure," in Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), pp. 248–252, Tirunelveli, India, June 2020.

[13] S. Ouiazzane, M. Addou, and F. Barramou, "Toward a network intrusion detection system for geographic data," in Proceedings of the 2020 IEEE International conference of Moroccan Geomatics (Morgeo), pp. 1–7, Casablanca, Morocco, May 2020.

[14] Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76:146– 164, 2015.

[15] J. Yu, P. Tian, H. Feng, and Y. Xiao, "Research and design of subway BAS intrusion detection expert system," in Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 152–156, Chongqing, China, October 2018.

[16] X. Zhan, H. Yuan, and X. Wang, "Research on block chain network intrusion detection system," in Proceedings of the 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA), pp. 191–196, Xi'an, China, September 2019.

[17] L. Hong, "Immune mechanism-based intrusion detection systems," in Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, pp. 568–571, Wuhan, China, April 2009.

[18] E. D. Alalade, "Intrusion detection system in smart home network using artificial immune system and extreme learning machine hybrid approach," in Proceedings of the 2020 IEEE 6th World Forum on Internet of Bings (WF-IoT), pp. 1-2, New Orleans, LA, USA, June 2020.

[19] Y. Shen, Y. Fei, L. F. Zhang, A. Ji-yao, and M. L. Zhu, "An intrusion detection system based on system call," in Proceedings of the 2005 1st IEEE and IFIP International Conference in Central Asia on Internet, p. 4, Bishkek, September 2005.

[20] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of things: a survey on machine learning-based intrusion detection approaches," Computer Networks, vol. 151, pp. 147–157, 2019.

[21] E. M. Campos, P. F. Saura, A. Gonz'alez-Vidal et al., "Evaluating federated learning for intrusion detection in internet of things: review and challenges," Computer Networks, vol. 203, Article ID 108661, 2022.

[22] A. Mihoub, O. B. Fredj, O. Cheikhrouhou, A. Derhab, and M. Krichen, "Denial of service attack detection and mitigation for internet of things using looking back-enabled machine learning techniques," Computers and Electrical Engineering, vol. 98, Article ID 107716, 2022.

[23] Z. S. Malek, B. Trivedi, and A. Shah, "User behavior pattern -signature based intrusion detection," in Proceedings of the 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp. 549–552, London, UK, July 2020.

[24] G. Zhu, H. Yuan, Y. Zhuang, Y. Guo, X. Zhang, and S. Qiu, "Research on network intrusion detection method of power system based on random forest algorithm," in Proceedings of the 2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), pp. 374– 379, Beihai, China, January 2021.

Edited by: Venkatesan C
Special issue on: Next Generation Pervasive Reconfigurable Computing for High Performance Real Time Applications
Received: Sep 26, 2023
Accepted: Feb 8, 2024