Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021).
IEEE Xplore Part Number: CFP21ONG-ART; 978-0-7381-1183-4

2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) | 978-1-6654-1960-4/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICICV50876.2021.9388497

Blockchain-based security algorithm on IoT framework for shielded communication in smart cities

K.Priyadharshini
Research Scholar, School of Computing,
Sathyabama Institute of Science and
Technology(Deemed to be university),
JeppiaarNagar, Rajiv Gandhi Salai, Chennai-119
*priyakannan.it@gmail.com

R.Aroul Canessane
Associate Professor, Department of CSE,
Sathyabama Institute of Science and
Technology(Deemed to be university),
JeppiaarNagar, Rajiv Gandhi Salai, Chennai-119

Abstract: This manuscript describes since the resources are heterogeneous, a smart city is vulnerable to several security attacks, and to devise an effective response, it is necessary to recognize certain risks and their potential implications. The framework is responsible for the data transfer security issues in the smart city to incorporate and maintain physical, social, and industrial systems to provide high-quality secure data transmission to its residents. The proposed method of integrating the Blockchain and Internet of Things (IoT) with a consensus algorithm framework (BCIoT-CAF) to overcome the issues and secure data sharing in smart cities. The data security is enforced by splitting the blockchain network into separate networks, with any channel consisting of a limited number of approved entities, the data stored in the cloud gate server, and analysis of data achieved by IoT applications. The consensus algorithm plays an important role in retaining the blockchain's speed, protection, and performance. Using an appropriate security algorithm, blockchain applications may greatly improve their performance. The modeling simulation of this research improves the speed, protection, and efficiency of 96% and tolerance error as 55%. The integrated evaluation results suggest that the proposed system integrates blockchain with IoT to provide a shielded communication platform in smart cities.

Keywords: Blockchain, Smart City, Internet of Things (IoT), Data Sharing, Consensus, Storage, Secure.

I Overview of the Framework

Blockchain used to share the data information securely and avoid any other fraudulent data threats[1]. IoT system implementations can be challenging and a transmitting ledger ideal for defining, authenticating, and protected data securely from IoT devices [2],[3]. Blockchain and IoT are two innovations rising in importance since they started. IoT can affect nearly ordinary things shortly. In the increased use of this tool, the risk of violence decreases [4]. To cope with this, existing techniques are not adequate. Blockchain has proven to be an innovative approach to IoT security problems and is a distributed network that relies on a consensus algorithm, ensuring agreement between distributed nodes on the status of some data [5],[6]. The central factor of the consensus algorithm that specifically defines a program operates and its output [7]. Blockchain technology attracting more coverage, revolutionize, automate the digital network of internet-based technologies [8]. This is a shared database that tracks each transaction that takes place on a network[9],[10]. It has a block spread over a node network. The consensus algorithm is a mechanism in which all the blockchain system peers decide on the existing state of the decentralized directory [11]. This ensures that consensus algorithms build stability in the blockchain network and confidence in the distributed computing system among unidentified peers [12]. The consensus protocol guarantees that a new block stored on the blockchain is the valid iteration accepted by all of the blockchain peers [13], [14].

The network adhering to nodal exchange protocols and evaluating modern block structures handles blockchain [15]. The sharing of information is at the convergence between economic possibilities and technology advances, and in many aspects makes the community benefit [16]. The shared network provides a collaborative and creative ecosystem that benefits the city in all smart city applications and industries [17]. Access to these data will help identify new ideas, create innovative programs and income sources to increase the performance of international activities, and provide proof of the basis for research and implementation of new technologies and programs [18]. The proposed method integrates blockchain and IoT with a consensus algorithm framework (BCIoT-CAF) to overcome the issues and secure the data transmission in smart cities [19]. Blockchain infrastructure consists of point-to-point connectivity, protocols for consensus, and decentralized cloud storage systems [20]. The IoT system believes that is a very thin and small capacity to communicate with blockchain-complete nodes [21]. The data security is enforced by splitting the blockchain network into separate networks, with any channel consisting of a limited number of approved entities, the data stored in the cloud gate server, and analysis of data achieved by IoT applications[22].

The paper is organized as follows the section 1 overview of the framework, in section 2 discusses the background works. In section 3, the proposed model BCIoT-CAF presented. In section 4, the algorithm of the proposed system presented. The paper ends with a simulation result and discussion, conclusion, and directions for future research in sections 5 & 6.

II Background Works

Abdur Rahman et al. [23] proposed the safety system based on blockchains to facilitate stable data exchange in a smart city. The incorporation of blockchain technologies with devices in a smart city creates a shared forum for safe connectivity among all users in a distributed system. Developed the mobile edge computing (MEC) distributed economy program that uses the blockchain and off-chain systems to store unchanging documents.

Meng Shen et al., [24] suggested the secure support vector machine (SVM), privacy-preserving SVM training strategy over blockchain encrypted IoT data to bridge the difference between ideal expectations and limitations. The blockchain strategies enable to create a safe and transparent network for information exchange between various service providers, which encrypts and records IoT data on a shared database. Paillier used to create effective and exact privacy security that preserves the SVM learning algorithm. Homomorphic cryptosystem has been used to secure SVM performance and health.

Jianjun Sun et al., [25] introduced the three-dimensional philosophical framework such as a person, technologies, and operational, which discusses several fundamental variables, rendered a community smarter from an economic shared perspective. The method used the triangle structure-based blockchain. Technology supports intelligent communities to build shared infrastructure through the triangle structure-based blockchain components.

Jayne Vora et al. [26]suggested the blockchain-based computing capacity system and electronic health records (EHR) managing. In turn, doctors, clinicians, and third parties have reliable and convenient access to medical records, while patient data protected confidentiality. The main objective to examine the new system addresses patients, providers, and third party's needs and explained structure preserves the protection and privacy issues of healthcare 4.0.

Imran Makhdoom et al., [27] proposed the data separated and protected in a database through the use of confidential data storage and authentication. Additionally, dual authentication in the context of allows consumers to communicate with the blockchain network. Consumer data from digital applications such as smartwatches to smart vehicles, sophisticated houses, vehicle networks, etc. nowadays are vulnerable to risks for security and privacy. In this study, blockchain-based "PrivySharing," a revolutionary protected and information sharing system used in smart cities.

Based on this research, the consensus security algorithm used in blockchain applications may greatly improve performance. The consensus algorithm plays an important role in retaining the blockchain's speed, protection, and performance. Within this paper, BCIoT-CAF is being developed and integrates the blockchain and IoT for secure data sharing in smart cities.

III Proposed Framework

The proposed method of integrating the Blockchain and IoT with a consensus algorithm framework (BCIoT-CAF) to overcome the issues and secure data sharing in smart cities. The data security is enforced by splitting the blockchain network into separate networks, with any channel consisting of a limited number of approved entities, the data stored in the cloud gate, and analysis of data achieved by IoT applications. IoT is certainly one of the most interesting subjects in the community and technological sectors. Although the conventional internet makes connections simpler between certain specific devices and people, IoT enables all sorts of things in an entire computer network without the presence of a human being. The introduction of IoT and the advancement of wireless connectivity technology collect the data from appropriate IoT applications. The incorporation of IoT technology in the smart city, however, present some problems data collection, data processing, data sharing between computers, privacy protection, and seamless and all-round access.

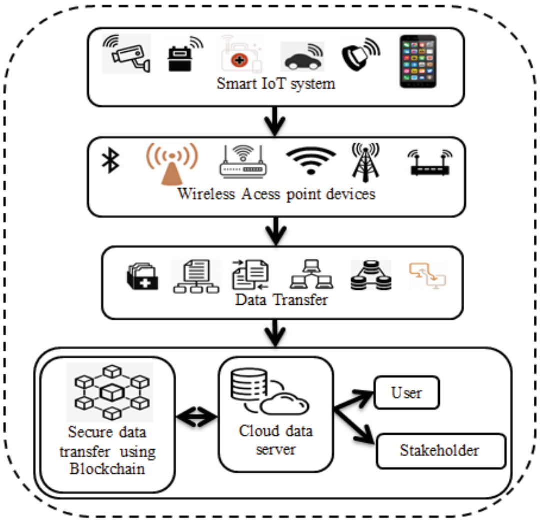
Smart IoT system
Wireless Acess point devices
Data Transfer
Secure data transfer using Blockchain
Cloud data server
User
Stakeholder

Figure 1. Proposed Framework for secure data sharing in Smart Cities

Figure 1, shows the proposed framework for secure data sharing in smart cities. The smart wireless IoT system such as smartwatches, smart vehicles, smart security cameras, smart health, smart energy meter, etc. are connected through a wireless access point devices such as Bluetooth, Wi-Fi, Edge gateway, Zigbee, long-range device (LoRa), etc. The data will be transfer securely with blockchain technology and the data stored on the cloud gate server then send to the user or any stakeholder. The typical program that combines IoT and blockchain, offering ubiquitous and open access to shared data and resources, delivering on-demand services across the system, and running to satisfy that request. Cloud infrastructure offers application technology to enable quicker delivery, more versatile tools, and increased efficiency, including servers, databases, network applications, and data analytics.

The value of a network interface for all nodes to be run seamlessly to allow users to communicate. Data computing and detailed data processing are carried out in the blockchain layer. In the field of IoT computing, the blockchain layer can be reached regularly and managed, leading to the optimal utilization of all existing resources, unlike conventional IoT architecture. The public ledger in blockchain is a sort of shared archive that reports after documents. Smart city systems are fitted with gathering sensors and actuators collect the data to protocols in the upper layer. Many of those instruments are fragile, including thermostats and Fitbit for weak security threats and systems of access management. Retailers need to be negotiated distribution and contact smart system requirements for solving these issues. Smart city services use multiple networking methods, including Bluetooth, WiFi, Zigbee, and a cutting edge gateway for the connectivity between various programs. To have encryption and protection of the data transmission, blockchain protocols need to be incorporated into this system. For instance, transaction information can be translated to separate blocks that can be distributed over the network. The convergence of current networking devices with blockchain is still a significant obstacle, as specifications vary between applications.

Possible alternative use of a blockchain control layer to incorporate multiple blockchains and provide various useful features. Multiple blockchain is a form of decentralized database that records one by one from the blockchain. The consensus algorithm may relate to one of the many suggested software engineering settlement protocols often used on a single specific value between parallel computing or structures, or in the present state of the distributed network. Consensus algorithms are mainly used in a network of different distributed nodes sharing the same knowledge to develop reliability. In the case of a variety of unreliable procedures, aggregate network stability is the central challenge in centralized computer and multiagency programs. Procedures need to decide on some data value while estimating. The consensus in the network used to validate multiple nodes and chain protection introduced by continuous authorization. Build a concept design framework involving a mobile application for the data collection on economic sharing networks and blockchain private sector. The scenario that shares the data from connected IoT sensor data with secure blockchain repository in claims for exchange of economic information or other types. The secured data stored in the cloud gate server and then transfer to the user or stakeholder. The intelligent large datasets applied to store the data will include sensing environment and consumer behavior, energy consumption, different protection factors, and functional data. The IoT architectural design depends on blockchain handler with consensus in a variety of trustworthy nodes to achieve protection, performance, and a significant number of shared data transfers per moment.

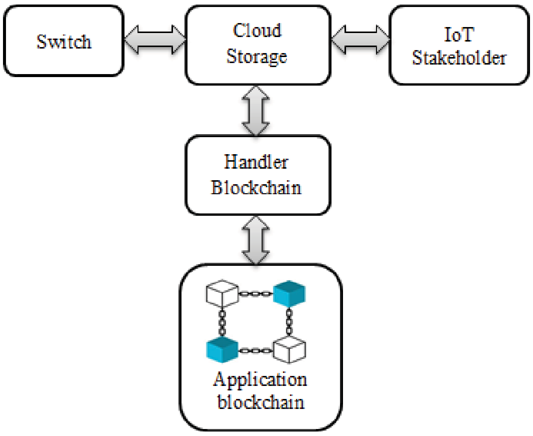

Figure 2. Integration of Blockchain and IoT Architectural design

Figure 2, shows the integration of blockchain and IoT architectural design consist of five entities such as application blockchain, handler blockchain, switch, cloud storage, and IoT stakeholder. For a community of stakeholders of IoT with similar settings, and the IoT domain is a platform capable of processing and user data. It is referred to as the IoT layer interface for middleware that offers the ability to link more services and devices with modules that require low IoT equipment. The switch for forwarding stakeholders IoT to more applications is maintained in every IoT domain. The introduction of two additional controllers namely handler blockchain and switch. The data from the IoT system transfer to the application blockchain and separate it into multiple blocks using handler blockchain. The switch transmits the data stream to a correct handler as stakeholders IoT sign into their IoT domain switch. In other words, the data is directed to the cloud storage server where it is in IoT streaming data types. Similarly, cloud storage organization is a member of the blockchain network, the functionality of IoT networks is customizable without any required modifications. Each consensus algorithm has its features and the proposed method analyzes the speed, protection, efficiency of blockchain, and minimizes the error rate.

IV Consensus Algorithm and flowchart of Proposed framework

Figure 3, shows the flowchart for blockchain-based secure data sharing on IoT. There are many types of blockchains, based on the data handled, functionality, and behavior the user is allowed to take the action. These can be isolated from the public and private and permissionless/permissions blockchains. For public blockchains, anybody can access the blockchain, function as a basic node, or a miner/validator without the permission of a third party. For certain decentralized blockchains such as Bitcoin, miners/validators are granted economic opportunities The controller limits network connectivity for private blockchains. Most private blockchains are permitted to monitor which users are allowed to transfer the data, conduct smart contracts, or operate as a network mine operator, automatically require all private blockchains. Whenever the centralized system is not a reliable mechanism, IoT implementations need decentralization. In IoT most connectivity transmits data to a centralized provider or cloud from nodes to gateways. Many IoT implementations that include financial transfers/data transfer with third parties.

A growing number of IoT networks capture and sequentially store time-signed data. Nevertheless, conventional databases can easily satisfy these criteria, especially in circumstances where protection is guaranteed or attacks are uncommon. Distributed applications are deployed on the cloud server, a storage system, or in other types of modern operating programs distributed. The need for this purpose is not necessary to support using a blockchain the organization that operates the centralized database network must still have at least a lack of confidence. Consensus algorithms from Proof of Work (PoW), Proof of stake (PoS), and Delegated Proof of Stake (DPoS) are common shared blockchain options.

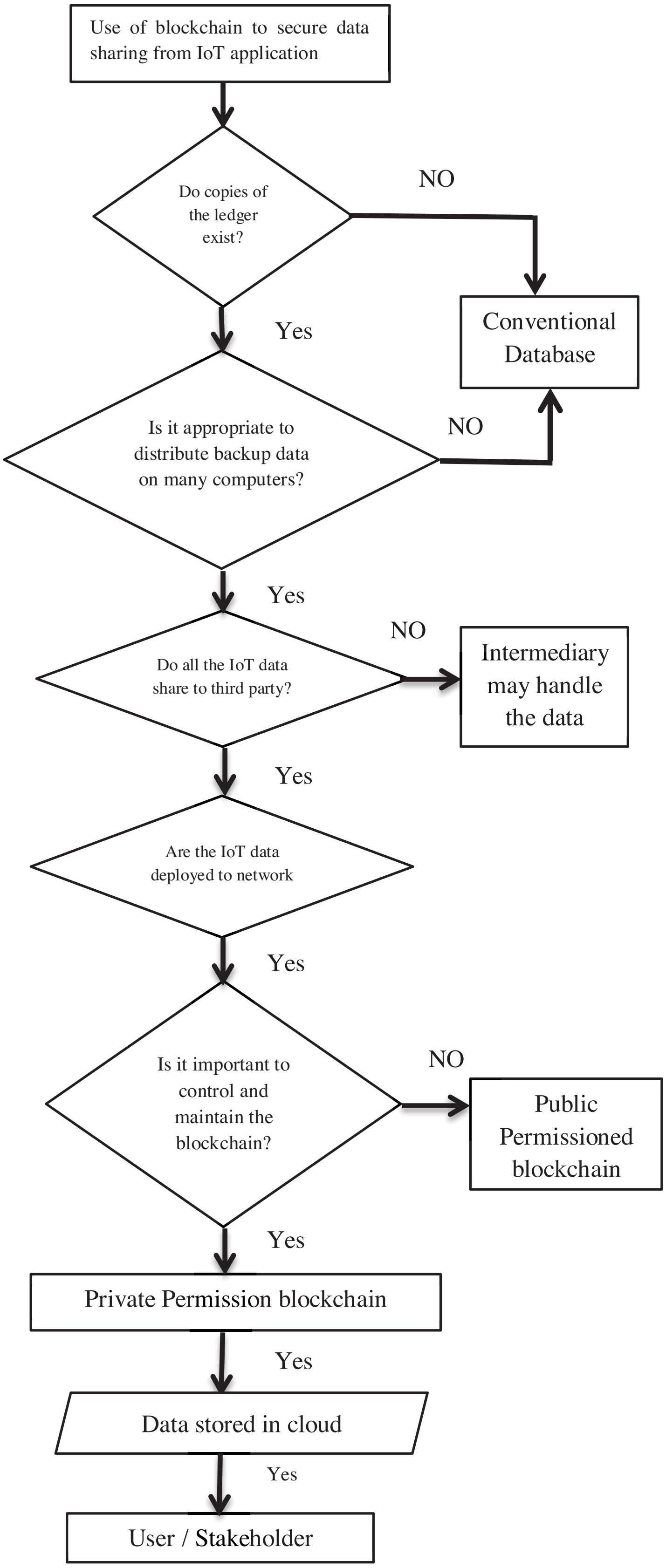
Use of blockchain to secure data sharing from IoT application
Do copies of the ledger exist?
NO
Conventional Database
Yes
Is it appropriate to distribute backup data on many computers?
NO
Yes
Do all the IoT data share to third party?
NO
Intermediary may handle the data
Yes
Are the IoT data deployed to network
Yes
Is it important to control and maintain the blockchain?
NO
Public Permissioned blockchain
Yes
Private Permission blockchain
Yes
Data stored in cloud
Yes
User / Stakeholder

Figure 3. Flow chart for blockchain-based secure data sharing on IoT

The maximum network hazard is G_0, the estimated average formation times are P_0, the highest truthful node hazard rate is AY_0 and the maximum danger rating for compromised users is BY_0. Initially, in event of H blocks dropping behind, determine A_H the chance for a malicious user to the equal list. It is identical to an absorbed on the multiple blockchains. The $Y - axis$ contains the data with the potential B to the left or A the right $(A + B = 1)$, the data may shift the unit destination each time. The node is at $Y = H$ at first, when $Y = 0$ is hit, the data will stop the transfer. A_H the probability of arriving at $Y = 0$.

$A_\varphi = 1, \lim_{H\to\infty} A_H = 0$ ---(1)

$A_H = \mu A_{H+1} + BA_{H-1}, H = 1,2,3, \ldots \infty$---(2)

If $B < A$, use the equation

$D_H = A_{H+1} - A_H = S = \frac{B}{A}$ ---(3)

From equation (2),

$A_H - A_\varphi = \sum_{m=0}^{H-1}(A_{m+1} - A_m) = \frac{1-S^H}{1-S} D_\varphi$ ---(4)

Then, with equation (1), written as

$A_H = S^H = (\frac{B}{A})^H, B < A$ ---(5)

$\mu_s = \gamma m_s - \sum_{j=1}^{H} A \left|(mY_j + q) < 1\right| \times Y_j P_j$ ---(6)

$A_H = 1, B \geq A$ ---(7)

The final equation,

$A_H = \begin{cases} 1, B \geq A \\ (\frac{B}{A})^H, B < A \end{cases}$ ---(8)

The attack on double-spending eventually works when the overall computing capacity of the malicious is above 55 % of the total network. Then calculate the chance of success of H blocks in double expenses to wait until $B < A$.

The node can restart hacking if the right hash in n time is not created. The overall possibility of success of good nodes in n cycles is nA/Qo and malicious nodes are nB/Qo. Unless the malicious nodes need double-spending attacks to succeed, wait before the data transfer is checked for H blocks. The honest nodes and malicious nodes attempted all HQo/nA times during this duration and the honest nodes succeed. So the effective times of the malicious nodes γ Poisson distribution of predicted value

$\gamma = HB/A$ ---(9)

The chance of double spending of malicious nodes is thus

$A = 1 - \sum_{m=0}^{H} \frac{\gamma^m \varepsilon^{-\gamma}}{m!} [1 - (\frac{B}{A})^{H-m}]$ ---(10)

The outcome can clearly be shown that the data transfer is secure if the wait for the transfer to be validated by enough blocks. The blockchain with Proof of stake (PoS) consensus algorithm will handle malicious nodes of up to 55%. The blockchain performance using PoS is constrained to eliminate bifurcations and wait for appropriate blocks to validate everything. All nodes will mine according to the predetermined rules in this blockchain. The number of nodes is not related to the performance and the level of testing. A blockchain network is thus nearly infinite.

V Results and Discussion

IoT implementations that include a network blockchain capable of handling significant data transfer volumes per unit of time and there is a limitation in certain networks. Concerning performance, it's important to remember that it takes a while to process blockchain transfer. The blockchain typically involves separating the blocks before a data transfer is authenticated. However numerous blockchains, the sophistication of the consensus mechanism becomes more significant in terms of performance than individual hashing. Blockchain technologies evolve regularly as users store their data which leads to faster loading times and using more powerful miners. Compression methods in blockchain can be more researched, but in practice, most IoT nodes do not cope with a small fraction of the regular blockchain. This can be stopped by lightweight nodes, which can execute blockchain transfers but do not have to store them. This strategy, however, involves the presence of some strong nodes in the IoT hierarchy that preserve the blockchain of resources-restricted nodes. One option is to use a mini ledger, meaning that use a data transfer account tree to hold the existing account. Therefore, even the current block with the data transfer account tree will be saved on the ledger. The blockchain then expands, additional blockchain applications are introduced. The request and the block size must be scaled to the bandwidth limitations of IoT networks certain small size data transfer maximize the energy usage of communications and some maximize their energy consumption.

Table 1. Performance Analysis

Time	MEC	SVM	EHR	PrivySharing	BCIoT-CAF
20	12	24	32	56	64
40	24	36	49	62	73
60	36	49	62	71	79
80	49	55	69	76	88
100	55	69	75	80	96

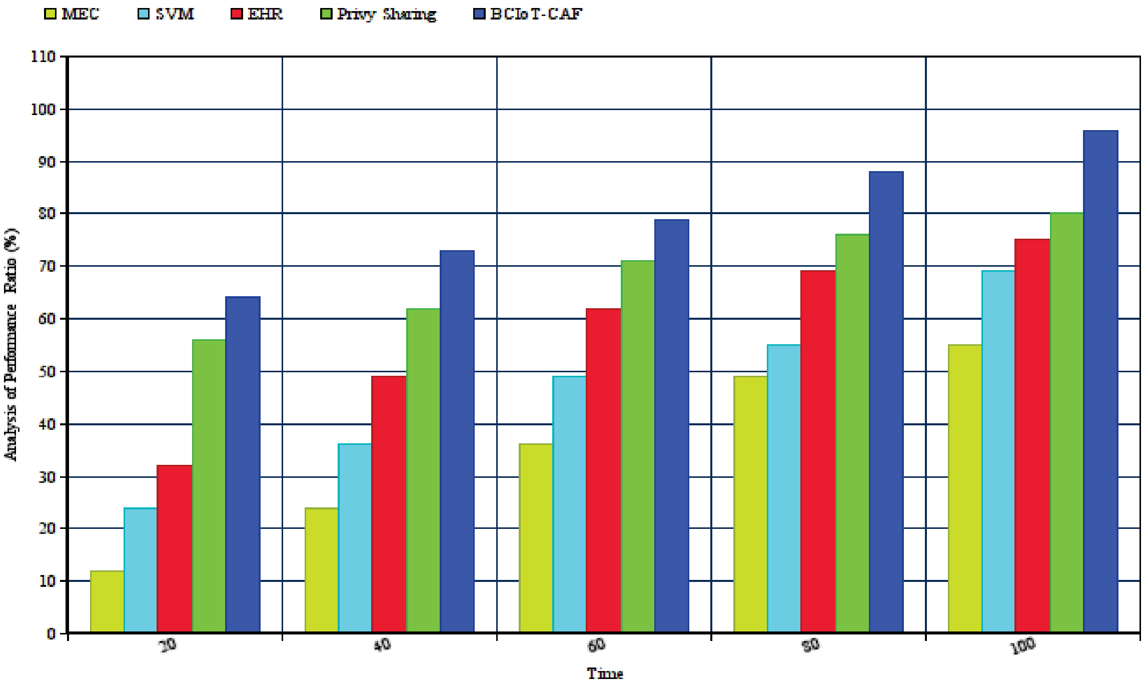

Figure 4. Performance analysis of Proposed Method

Figure 4, shows the performance analysis of blockchain compared to the other existing method. In the proposed method blockchain integrates with IoT with a PoS consensus algorithm. The user needs to compromise to maintain privacy effectively, as the use of blockchain-based IoT requires high computing resources and often takes time to complete each operation, and performance increased maximum. Table 1, shows the performance analysis of the blockchain-based secure data sharing on IoT.

Figure 5, shows the analysis of hashing power and probability success of double-spending. The blockchain with Proof of stake (PoS) consensus algorithm will handle malicious nodes of up to 55%. The blockchain performance using Proof of stake (PoS) is constrained to eliminate bifurcations and wait for appropriate blocks to validate everything. The delegated witnesses build blocks and validate data transfer in the PoS ledger. Table 2, shows the comparison of features with PoW, PoS, and DPoS.

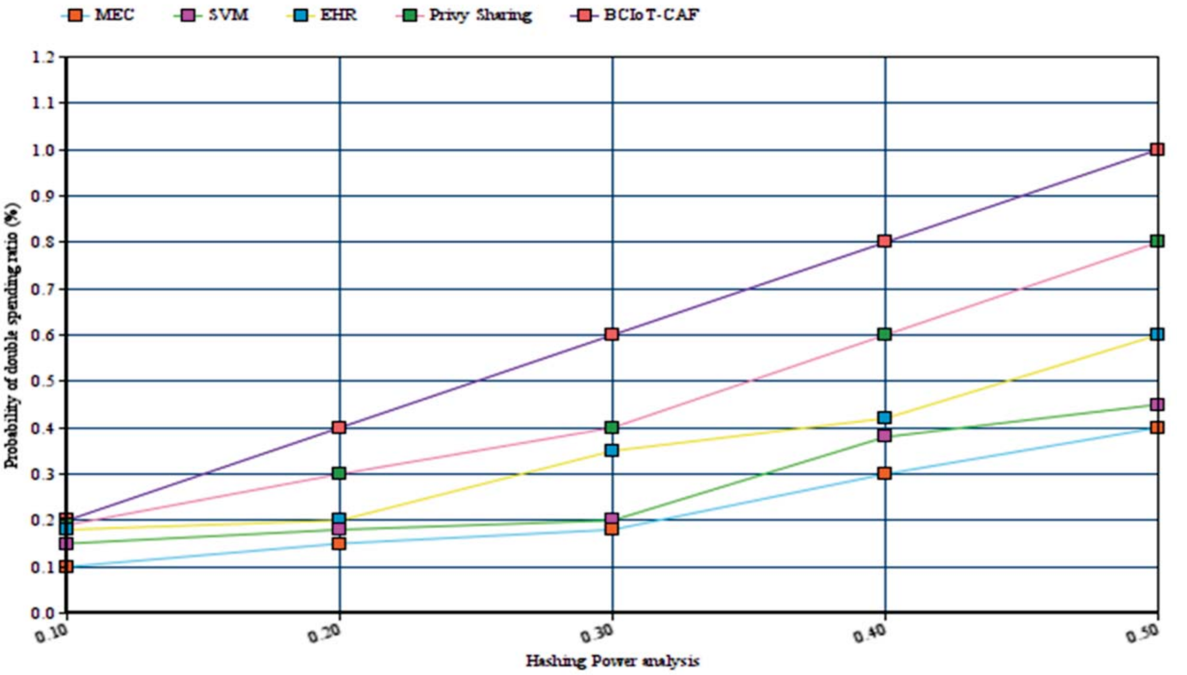

Figure 5. Analysis of Hashing power and Probability success of double-spending

Features	PoS	DPoS	PoW
Tolerance to loss	55%	55%	55%
Tolerance to collision error	55%	55%	55%
Speed Verification	>110Sec	<99Sec	<99Sec
Crossover	<99	<999	<999
Scalable	Good	Good	Good

Table 2. Comparison of features with PoW, PoS, and DPoS

The blockchain with PoS will speed up the development of the blocks and raising the control nodes. PoS speed is higher than PoW and DPoS, crossover lesser than the remaining method, collision error remains the same for three methods, tolerance loss remains the same for three methods, and good scalability. The proposed approach suggested guarantees the safe, protection, and performance of personal and critical user data to stakeholders based on the need to learn in smart links, in compliance with consensus algorithms.

VI Conclusion

Through several studies, researchers have gathered insights into the influence of data sharing, and protection with various methods. The proposed method of integrating the Blockchain and Internet of Things (IoT) with a consensus algorithm framework (BCIoT-CAF) to overcome the issues and secure data sharing in smart cities. Blockchain has decentralization features, transparency, protection, non-alteration, etc. The blockchain has been gaining more interest in many fields with the advancement of technology. Specific performers reduce unwanted access and thinking, decentralization is accomplished when other networks are made up of informal control. The consensus algorithm plays an important role in retaining the blockchain's speed, protection, and performance. The blockchain with Proof of stake (PoS) consensus algorithm will handle malicious nodes of up to 55%. The modelling simulation improves the speed, protection, and efficiency of 96% and minimizes the error rate. The integrated evaluation results suggest that the proposed system integrates blockchain with IoT to provide a shielded communication platform in smart cities. In the future, the consensus algorithm design for the various scenario with advanced technology and improve the interaction with other IoT applications.

References

1. Sushil Kumar, Singh Shailendra Rathore, and Jong Hyuk Park, (2020), BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence, Future Generation Computer Systems, 110, pp. 721-743.
2. Qin Wang, Xinqi Zhu, Yiyang Ni, Liu, and Hongbo Zhu, (2020), Blockchain for the IoT and Industrial IoT: A review, Internet of Things, 10, pp. 100081-100099.
3. Ishan Mistry, Sudeep Tanwar, Sudhanshu Tyagi and Neeraj Kuma, (2020), Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges, Mechanical Systems and Signal Processing,135, pp. 106382-1060402.
4. V. Dedeoglu, R. Jurdak, A. Dorri, R. C. Lunardi, R. A. Michelin, A. F. Zorzi and S. S. Kanhere, (2019), Blockchain Technologies for IoT, Advanced Applications of Blockchain Technology, SBD, 60, pp. 55-89.
5. Tanweer Alam, and Mohamed Benaida, (2020), Blockchain, Fog, and IoT Integrated Framework: Review, Architecture, and Evaluation, Technology Reports of Kansai University, 62 (2), 2003.03596.
6. Anum Nawaz, Jorge Pena Queralta, Jixin Guan, Muhammad Awais, Tuan Nguyen Gia, Ali Kashif Bashir, Haibin Kan, and Tomi Westerlund, (2020), Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain, Sensors, 20 (14), 3965.
7. Saiyu Qi, Youshui Lu, Yuanqing Zheng, Yumo Li, Xiaofeng Chen, (2020), Cpds: Enabling Compressed and Private Data Sharing for Industrial IoT over Blockchain, IEEE Access, 10,1109.
8. Quanyu Zhao, Siyi Chen, Zhi Liu, Thar Baker, and Yuan Zhang, (2020), Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems, Information Processing & Management, 57,(6), pp.102355-102378.
9. Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit,(2020), A Comprehensive Survey on Attacks, Security Issues, and Blockchain Solutions for IoT and IIoT, Journal of Network and Computer Applications, 149 (1), pp. 102481-102510.
10. Faisal Jamil, Shabir Ahmad, Naeem Iqbal and Do-Hyeun Kim, (2020), Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals, Sensors, 20 (8), pp. 2195.
11. Jawad Ali, Ahmad Shahrafidz Khalid, Eiad Yafi, Shahrulniza Musa, and Waqas Ahmed, (2019), Towards a secure behavior modeling for IoT networks using Blockchain, CEUR, 2486, pp. 244-258.
12. Bhabendu Kumar, Mohanta Debasish Jena, Utkalika Satapathy, Srikanta Patnaik,(2020), Survey on IoT security: Challenges and solutions using machine learning, artificial intelligence and blockchain technology, Internet of Things, 11, pp. 100227.
13. Jun Wu, Mianxiong Dong, Kaoru Ota, Jianhua Li, and Wu Yang, (2020), Application-Aware Consensus Management for Software-Defined Intelligent Blockchain in IoT, IEEE Access, 34 (1), pp. 69-75.
14. Daniel Minoli, (2020), Positioning of blockchain mechanisms in IoT-powered smart home systems: A gateway-based approach, Internet of Things, IEEE Access, 10, pp. 100147.

15. Zehui Xiong, Yang Zhang, Nguyen Cong Luong, Dusit Niyato, Ping Wang, and Nadra Guizani, (2020), The Best of Both Worlds: A General Architecture for Data Management in Blockchain-enabled Internet-of-Things, IEEE Access,34 (1), pp. 166-173.
16. Mamoona Humayun, NZ Jhanjhi, Bushra Hamid, and Ghufran Ahmed, (2020), Emerging Smart Logistics and Transportation Using IoT and Blockchain, IEEE Access, 3 (2), pp. 58-62.
17. Daniele Mazzei, Giacomo Baldi, Gualtiero Fantoni, Gabriele Montelisciani, Antonio Pitasi,Laura Ricci, and Lorenzo Rizzello, (2020), A Blockchain Tokenizer for Industrial IOT trustless applications, Future Generation Computer Systems, 105, pp. 432-445.
18. Eric Ke Wang, Rui Pei Sun, Chien-Ming Chen, Zuodong Liang, Saru Kumari, and Muhammad Khurram Khan, (2020), Proof of X-repute blockchain consensus protocol for IoT systems, Computers & Security, 95, pp. 101871.
19. Miao Du, Kun Wang, Yinqiu Liu, Kai Qian, Yanfei Sun, Wenyao Xu, and Song Guo, (2020), Spacechain: A Three-Dimensional Blockchain Architecture for IoT Security, IEEE Access, 27 (3), pp. 28-35.
20. Nazmul Islam, and Sandip Kundu, (2020), IoT Security, Privacy and Trust in Home-Sharing Economy via Blockchain, Blockchain Cybersecurity, Trust and Privacy, ADIS, 79, pp. 33-50.
21. Hongliang Tian, Xiaonan Ge, Jiayue Wang, Chenxi Li, and Hong Pan, (2020), Research on distributed blockchain-based privacy-preserving and data security, IET Digital Library, 14 (13), pp. 2038-2047.
22. Jenil Thakker, Ikwhan Chang, and Younghee Park, (2020), Secure Data Management in Internet-of-Things Based on Blockchain, IEEE Access, 9 (4), pp. 998.
23. Abdur Rahman, Mamunur Rashid, and M. Shamim Hossain, (2018), Blockchain and IoT-based Cognitive Edge Framework for Sharing Economy Services in a Smart City, IEEE Access, 2896065, pp. 2169-3536.
24. Meng Shen, Xiangyun Tang, Liehuang Zhu, Xiaojiang Du, and Mohsen Guizani, (2018), Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities, IEEE Access, 2901840, pp. 2327-4662.
25. Jianjun Sun, Jiaqi Yan, and Kem Z. K. Zhang, (2016), Blockchain-based sharing services: What blockchain technology can contribute to smart cities, Sun et al. Financial Innovation, pp.2-26.
26. Jayne Vora, Anand Nayyar, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, M. S. Obaidat, and Joel J P C Rodrigues, (2018), BHEEM: A Blockchain-based Framework for Securing Electronic Health Records, IEEE Access, pp. 6-18.
27. Imran Makhdoom, Ian Zhou, Mehran Abolhasan, Justin Lipman, Wei Ni, (2020) PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities, Computers & Security 88, pp. 101653-101677.