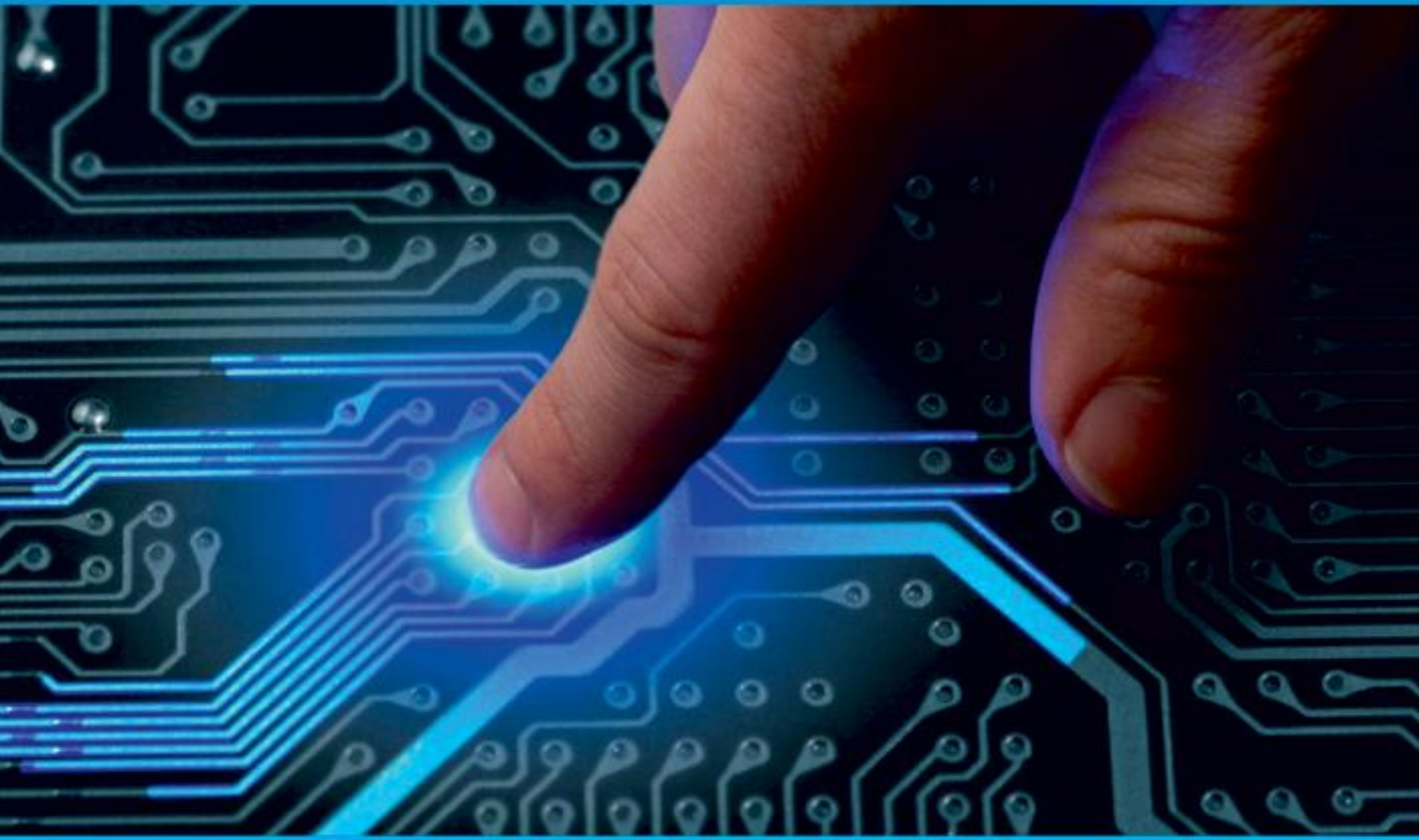
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 4, April 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

Secure Communication using Blockchain & Cryptography

Jyotsna A Nanajkar[1], Prem Singh[2], Priyanka Sutar[3],Akanksha Yadav[4], Siddhi Shinde[5], Shruti Sonone[6]

Professor, Department of Information Technology, Zeal College of Engineering and Research, Pune, Maharashtra, India[1]

Students, Department of Information Technology, Zeal College of Engineering and Research, Pune, Maharashtra, India[2,3,4,5,6]

ABSTRACT: Attribute based Encryption (ABE) is a promising cryptographic leading device to ensure information proprietors' immediate command over their information in broad daylight distributed storage. The previous ABE plans include just a single position to keep up with the entire trait set, which can bring a solitary point bottleneck on security and execution. Accordingly, some multi- authority plans are proposed in which various sources hold disjoint characteristic subsets independently. Be that as it may, the single-point bottleneck issue stays perplexing. In this paper, according to another point of view, we lead an edge multi-authority Code Text Strategy. Attribute Base Encryption (ABE) access control conspire for public distributed storage, named Robust and Auditable Access Control (RAAC) plot, in which different specialists together deal with a uniform quality set. The findings of the security and performance analyses demonstrate that RAAC is not only robust while no less than authorities are active in the system but also verifiably secure when fewer than the authorities are compromised. Additionally, we create a hybrid scheme that effectivelycombines the conventional multi-authority scheme with RAAC to satisfy the situation of attributes coming from several authorities and accomplish security and system-level robustness. Additionally,our system is constructed using blockchain, a ground-breaking technology that enables decentralized data sharing. Fine-grained data access management is made possible, and inefficiencies in centralized systems are decreased. The security analysis and evaluation of our technique showed that it can potentially offer privacy protection, authenticity, and dependability.

KEYWORDS: - Attribute Based Encryption (ABE), Multi-authority scheme, Robust and Auditable Access Control (RAAC) scheme, Role-based access control (RBAC), Internet of Things (IoT), Blockchain, Cryptography, Distributed Denial of Service (DDoS), Peer-to-Peer (P2P), Decentralized Model, Tamper-proof, Data nodes, Proof of Work (PoW), Consensus Algorithm, Cybersecurity.

I. INTRODUCTION

To distinguish between users' eligibility to access different services, roles and titles are always used. Such a mechanism describes access controls between users and services using a role-based access control (RBAC) architecture. Users in RBAC are connected to role services and tied to roles through roles. The usage of this access control is widespread inside an organization; however, it is important to keep in mind that RBAC is a flexible framework and that roles are frequently utilized beyond organizational boundaries. Roles and titles are frequently used to identify a user's eligibility to use a certain service. Due to the role-based access management (RBAC) framework, which outlines the access management relationship between users and services, such a mechanism is created. [1]Compromised devices can be a common occurrence in IoT networks, and conventional IoT systems often rely on a centralized engineering architecture. A chain of Blocks that contain immutable records,such as transactions or files, is what constitutes a Blockchain, and it can be used to store any information deemed necessary.

Users and roles are connected in RBAC, and roles are connected to services. Such computer system frameworks are used by numerous businesses and organizations to implement their internal access management requirements. Through digitalization, the development of communication from the past to the present has reached a worldwide scale. The massive data collection in the communication sector made it the focus of the central systems, such as states and businesses that manage the industry, thanks to the data that gave our period its name. [2] Recently, Blockchain is regarded as a novel technique, which can be used to solve the problems. Blockchain is an open, cryptographic, and distributed data structure, maintaining permanent ledgers accessible but tamper-proof for everyone. Users of blockchain technology have more control over their digital identities and can share and communicate with confidence. Blockchain-based communication applications that make use of asymmetric cyphers, consensus-based algorithms, and P2P network architecture. [3] One of the key features of blockchain technology is its ability to establish trust among untrusted entities, without the need for a central authority or intermediary. Blockchain has modified cryptography to protect user privacy and transaction information while ensuring data consistency.

[4] The importance of access control mechanisms for ensuring data security in digital communication. It also mentions the use of attribute-based encryption (ABE) as a promising cryptographic tool for ensuring information proprietors' immediate control over their data in public distributed storage. It alsotouches upon the importance of communication in the digital age and the need for effective data protection mechanisms. [5] The most common problem IoT security is Distributed Daniel of Service (DDoS) which make the users unable to access the server because the attacker executed a huge number of requests to server. Blockchain provides a decentralized model that makes the network Reliable, safe, flexible, and able to support real-time services

II. LITERATURE SURVEY

Year	Author	Paper Name	Objective	Algorithms	Advantages
2020	Ali MansourAl-madani1	IoT Data Security Via Blockchain Technology and	This study proposed amodel (SCN) for IoT data security using Blockchain	shared ledger, Cryptograp hy	Model features: Decentralized network, encrypted user
		Service-Centric Networking			identity, peer-to- peer data storage.
2020	Bin Xiao	G-PBFT: A Location-basedand Scalable Consensus Protocol for IoT-Blockchain Applications	Study suggests blockchain n-based and scalable consensus protocol forIoT blockchain application.	PBFT algorithm,G-PBFT Algorithm	Managing massiveIoT devices, achieve advanced data security, and data credibility
2020	Jiaqi Yuan	Demonstrationof Blockchain-based IoT Devices Anonymous Access Network UsingZero-knowledge Proof	Paper proposes secure blockchain n-based IoT with zero- knowledge proof for sensitive data protection.	Consensus Algorithm	Blockchain datasecure due to optical fiber network. Verification group members independently match hash value and encrypt user ID.
2020	Chao Qiu	Networking Integrated Cloud-Edge- End in IoT: A Blockchain- Assisted Collective Q-Learning Approach	CQL uses IoT nodes to train learning layersand blockchain to share verifiable results.	Q Learning	ML and IoT are integrated due totheir flexibility, agility, and accessibility.
2020	Abbas Yazdinejad∗ , Gautam Srivastava†,	Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Net works	In this paper, we propose a Secure andLow latency Proof ofWork (SLPoW) protocol.	SLPoW protocol	Blockchain in IoT requires data field identification and control.

III. IMPLEMENTATION DETAILS OF MODULE

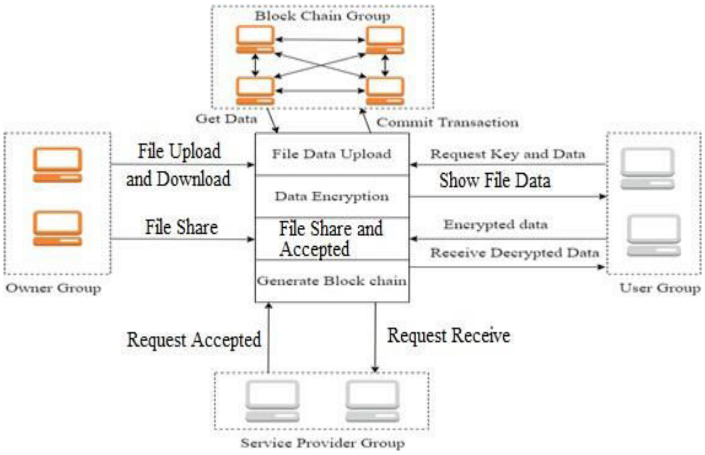


Fig 1: - System Architecture

As from the Fig. 1 we understand that the System must validate the previous block before commit block. User can access the data over the internet 24*7. If any block has changed by third party attackeror unauthorized user, it must show during transaction current blockchain is invalid. It can recover the invalid blockchain using other data nodes, with the help of majority of trustiness. The node or user who wants to initiate a transaction would record and broadcasts the data to the network. The node or user who receives the data verifies the authenticity of the data received in the network. Then the verified data is stored to a block. All nodes or users in the network validate the transaction by executingeither the proof of work algorithm or the proof of stake algorithm to the block that needs validation. Consensus algorithm used by the network will store the data to the block that is added to blockchain. And all nodes in the network admit the respective block and extend the chain base on the block.

IV. CONCLUSION

The fascinating developments in technology include those in information communications and cryptography. The many encryption techniques utilized in blockchain are presented in this study along with the advancement of encryption systems. Also covered are the different security assaults against Blockchain. Brief discussion is given regarding the challenges of blockchain technology as well as the various security services available for authentication and privacy. This program may be used to guarantee the accessibility, confidentiality, and privacy of the private data exchanged across organization users. Future applications for blockchain technology will mostly be found in the area of cybersecurity. The data is protected and validated even though the Blockchain ledger is dispersed and accessible. Encryption is used to achieve this in order to remove risks like illegal data tampering.

REFERENCES

[1] Jiaqi Yuan, Hui Yang, Shuai Dong, Qiuyan Yao,Libin Jiao, Jie Zhang " Demonstration of Blockchain-based IoT Devices Anonymous Access Network Using Zero-knowledge Proof " 2020 IEEE

[2] Chao Qiu, Xiaofei Wang, Haipeng Yao, Jianbo Du, F. Richard Yu,and Song Guo "Networking Integrated Cloud-Edge-End in IoT: A Blockchain-Assisted Collective Q-Learning Approach" IEEE 2020

[3] Ali Mansour Al-madani,Dr. Ashok T. Gaikwad "IoT Data Security Via Blockchain Technology and Service-Centric Networking" IEEE 2020.

[4] Abbas Yazdinejad∗, Gautam Srivastava†, Reza M. Parizi‡, Ali Dehghantanha∗, Hadis Karimipour∗, Somayeh Razaghi Karizno " SLPoW: Secure and Low Latency Proof of Work Protocol for Blockchain in Green IoT Networks " ©2020 IEEE

[5] Laphou Lao∗, Xiaohai Dai∗†, Bin Xiao∗ and Songtao Guo‡"G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications" IEEE 2020

[6] Huang, Zheng, Zeyu Mi, and Zhichao Hua. & HCloud: A trusted JointCloud serverless platform for IoT systems

with blockchain. & China Communications 17.9 (2020): 1-10.

[7] Gheitanchi, Shahin. & Gamified service exchange platform on blockchain for IoT business agility& 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, 2020.

[8] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, \Enabling efficient and geometric range query with accesscontrol over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870{885, 2019.

[9] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. Shen, Privacy preserving attribute- keyword based data publish-subscribe service on cloud platforms," Information Sciences, vol. 387, pp. 116{ 131, 2017.

[10] Choi, Jungyong, et al. & quot;Random Seed Generation For IoT Key Generation and Key Management System Using Blockchain, International Conference on Information Networking(ICOIN). IEEE, 2020.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details