IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205411 |

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]

ABSTRACT *:* Attribute-based encryptions (ABE) is a promising cryptographic technique to guarantee that data owners have total control over their data in public cloud storage. Early ABE schemes were vulnerable to performance and security issues since they depended on a single authority to maintain the whole set of characteristics. Then, a few multi-authority approaches are presented, where several sources each have a unique, discontinuous attribute subset. But the single-point bottleneck problem hasn't been solved yet. In this paper, we approach a multiauthority threshold cypher text policy from a new perspective. The Robust and Auditable Access Control (RAAC) method is a cooperative Attribute Base Encryption (CP-ABE) access control approach for managing a shared attribute set in public cloud storage. The results of the security and performance analyses show that RAAC is both dependable while at least t authorities are engaged in the system and verifiably secure when no more than t authorities are compromised. Additionally, in order to address the problem of characteristics originating from several authorities, achieve security, and achieve system-level resilience, we develop a hybrid scheme that successfully integrates the traditional multi-authority scheme with RAAC.

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

Roles and titles are constantly used to distinguish between users' eligibility to access various services. Such a method defines role-based access control (RBC) architecture-based access restrictions between users and services. In RBAC, users are linked to roles through roles and role services. Within an organization, this access control is often used, but it's crucial to remember that RBAC is a flexible framework and that roles are regularly used outside of organizational bounds. In order to determine a user's eligibility to utilize a certain service, roles and titles are routinely employed. Such a technique is made possible by the role-based access management (RBAC) architecture, which describes the access management connection between users and services. In RBAC, roles and users are linked together, and roles and services are linked together. Many companies and organizations utilize these computer system frameworks to meet their internal access management needs. Communication is a crucial and unavoidable component of human life. Through digitization, communication has advanced from the past to the present on a global scale. Thanks to the vast data gathering in the communications industry, which is the focus of the centralized systems, including states and enterprises that administer the sector, our era got its name from the data. Blockchain users may share and interact with confidence and have more control over their digital identities. applications for blockchain-based communication that leverage P2P network architecture, consensus-based algorithms, and asymmetric cyphers. Thanks to cryptography, information is protected from unauthorized users and only available to those who need to comprehend it. With the use of blockchain, cryptography has been updated to safeguard user privacy and transaction information while maintaining data consistency.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205411 |

II. RELATED WORK

Brilliant Agreements [1] likewise called crypto-contract, it is a PC program utilized for moving/controlling the property or computerized flows in unambiguous gatherings. It doesn't just decide the agreements yet may likewise carry out that strategy/arrangement. These shrewd agreements are put away on block-chain and BC is an optimal innovation to store these agreements because of the equivocalness and security. At the point when an exchange is thought of, the brilliant agreement figures out where the exchange ought to be moved/returned or since the exchange really happened.

Presently CSIRRO group has proposed another way to deal with coordinate Block on IOT with [2] In its underlying undertaking, he utilizes shrewd home innovation to comprehend how IOT can be obstructed. Block wheels are particularly used to give access control framework to Shrewd Gadgets Exchanges situated on Savvy Home. Presenting BC innovation in IOT, this search again gives some extra security highlights; nonetheless, every standard BC innovation should have an idea that does exclude the idea of thorough calculations. Besides, this innovation can't give a general type of block-chain arrangement in the event of IOT usage.

As per Ilya Sukhodolski. The Al [3] framework presents a model of multi-client framework for access command over datasets put away in mind blowing cloud conditions. Like other temperamental conditions, distributed storage requires the capacity to safely share data. Our methodology gives access command over information put away in the cloud without the supplier's speculation. Access Control System The fundamental device is the powerful component-based encryption conspire, which has dynamic highlights. Utilizing Blockchain based decentralized badgers; Our frameworks give an irreversible log to availability demands for all significant security occurrences like huge funding, access strategy task, modification or undoing. We offer a bunch of cryptographic conventions that make the mystery or mystery key of cryptographic activity classified. The hash code of the sifter text is just communicated by the block on laser. Our framework has been tried on model brilliant agreements and tried on Ethereum Blockchain platforms.

As per [4] an essential IoT Blockchain combination model with four layers which contains various sorts of IoT gadgets. Appropriated document framework is viewed as in the model to store enormous measure of IoT information. Then, a contextual investigation for blockchain based IoT application, a Machine-to-Machine(M2M) independent exchanging framework, is proposed on the Ethereum blockchain. We fabricate brilliant agreements for gadget enrollment, information capacity, administration arrangement and fair installment, and the verification of idea is carried out utilizing two Raspberry Pis to cooperate with savvy contracts. The proposed framework confirms that blockchain could further develop IoT applications in straightforwardness, detectability and security.

As per [5] Edgence (EDGe + Knowledge, is proposed to act as a blockchain empowered edge-registering stage to brilliantly oversee enormous decentralized applications (dApps) in IoT usecases1. To stretch out the scope of blockchain to IoT-based dApps, Edgence takes on ace hub innovation to interface with a shut blockchain-based framework to this present reality. An expert hub contains a full hub of the blockchain and a security, and is sent on an edge haze of portable edge figuring which is helpful for the expert hub to utilize assets of the edge cloud to run IoT dApps.

As per [6] presents HCloud, a believed Joint Cloud stage for IoT frameworks utilizing server less processing model. HCloud permits an IoT server to be executed with various servers less capabilities and timetables these capabilities on various mists in view of a timetable strategy. The arrangement is determined by the client and incorporates the necessary functionalities, execution assets, dormancy, cost, etc. HCloud gathers the situation with each cloud and dispatches waiter less capabilities to the most reasonable cloud in light of the timetable approach. By utilizing the blockchain innovation, we further authorize that our framework can neither phony the cloud status nor wrongly dispatches the objective functions.

As per [7] present the idea of a decentralized gasified help trade stage where the arrangement suppliers can powerfully offer and solicitation administrations in an independent distributed style. Cost and choice to trade administrations are set during activity time in light of gasification strategies as per business objectives. The proposed idea depends on blockchain innovation to give a tokenized economy where the IoT arrangement suppliers can carry out gasification methods utilizing shrewd agreements to boost benefits during administration offering and requesting.

As per Vipul Goyalet. Al [8] grows new cryptosystems to share scrambled information appropriately, which we call key-arrangement characteristic based encryption (KPABE). In our cryptosystem, Cipher text is named with a bunch of

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205411 |

properties and controls that it associates with private key access designs that a client can decode the encryption. We show the utility of our item to share review log data and broadcast encryption. Our creation upholds private key suppliers, which buy into arranged ID based encryption (HIBE).

Hao Wang et Mate Al [9] They offer a protected electronic wellbeing record (EHR) framework in light of unique based grave co-happens and blockchain innovation. In our framework, we use quality-based encryption (ABE) and personality-based encryption (IBE) to encode clinical information and to utilize character-based signature (IBS) to apply advanced marks. To get different elements of ABI, IBE and IBS in crypto, we present another cryptographic crude, it is known as a joint component based/personality-based encryption and mark (C-Stomach muscle/IB-ES). It works on framework upkeep and doesn't need the establishment of discrete cryptographic framework for different security necessities. Moreover, we use blockconne
procedures to guarantee the trustworthiness and review of clinical information. At last, we offer a showing application for clinical protection business.

As indicated by [10] a plan to produce seed required for key age and a plan to deal with the public key utilizing blockchain. First is an irregular seed age conspire required for key age? To forestall the gamble of a man-in-the-center assault and figuring out, seeds are produced by utilizing out-of-band correspondence and equipment variety. Second is a key administration framework for the IoT utilizing blockchain? The plan we propose is to circulate the public key on the blockchain network. The public key is utilized to scramble a meeting key that will be utilized for correspondence between gadgets

III. PROBLEM STATEMENT

The combination which carried with the globalizing scene, profoundly influences the organization and the correspondence areas. Generally, shut source and unified frameworks are utilized for organization and correspondence. This goes against with the data security standards and protection. These concentrated frameworks cannot completely meet the idea of straightforward, solid, quick and continuous correspondence. Appropriated, decentralized and furthermore straightforward correspondence is conceivable with the blockchain innovation. Likewise, we involved encryption idea as cryptography assumes a fundamental part in Blockchain. In Blockchain, encryption is adjusted to guarantee the consistency of the information, monitor client security, and exchange data.

IV. SYSTEM ARCHITECTURE

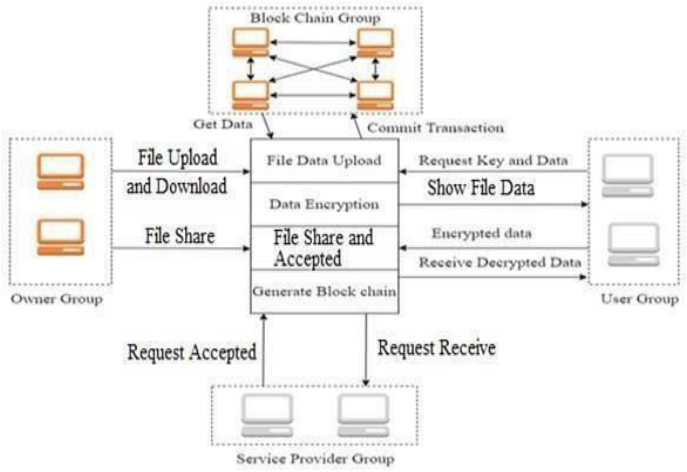


Fig. 1 Block Diagram of Proposed System

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205411 |

V. METHODOLOGY

Registration and Authentication: All entities can register during that time. Users, service providers, and data owners can all construct their own profiles.
Data Uploading: Once the file owner has uploaded it, the first phase. Data encryption, a mechanism for encrypting data, and the sending of keys to a database storage are all completed in that module.
Data Sharing: The data owner shares data during that stage; he is free to send any file to any user in the user group.
Access Control: Any user may view or access the shared file under access control. The owner of the data may deny a particular user access to a file during a revocation.
File request and download: After key verification, the user can submit a download request to databases.
Distributed Blockchain: The distributed ledger used to describe the system's current delegated access privileges is called the Blockchain. The Root User Authority and the Authorities are in charge of managing permissions to interact with the Blockchain.

Algorithm 1: Protocol for Peer Verification

Input : User get IP address, User Transaction TID, Output :

Enable IP address or current query if any connection is valid

Step 1 : User generate the any transaction DDL, DML or DCL query

Step 2 : Get current IP address If (connection(IP) equals(true)) Flag true Else Flag false End for Step 3 : if (Flag == true) Peer to Peer Verification valid Else Peer to
Peer Verification Invalid End if End for

Algorithm 2:Hash Generation

Input : Genesis block, Previous hash, data d

Output : Generated hash H according to given data Step 1 : Input data as d Step 2 : Apply SHA 256 from SHA family
Step 3 : Current Hash= SHA256(d) Step 4 : Return Current Hash

Algorithm 3: Mining Algorithm for valid hash creation

Input : Hash Validation Policy P[], Current Hash Values hash Val Output : Valid hash
Step 1 : System generate the hash Val for i th transaction using Algorithm 1 Step 2 : if (hash Val. valid with P[]) Flag =1 Else Flag=0
Step 3 : Return valid hash when flag=1

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205411 |

VI. RESULT

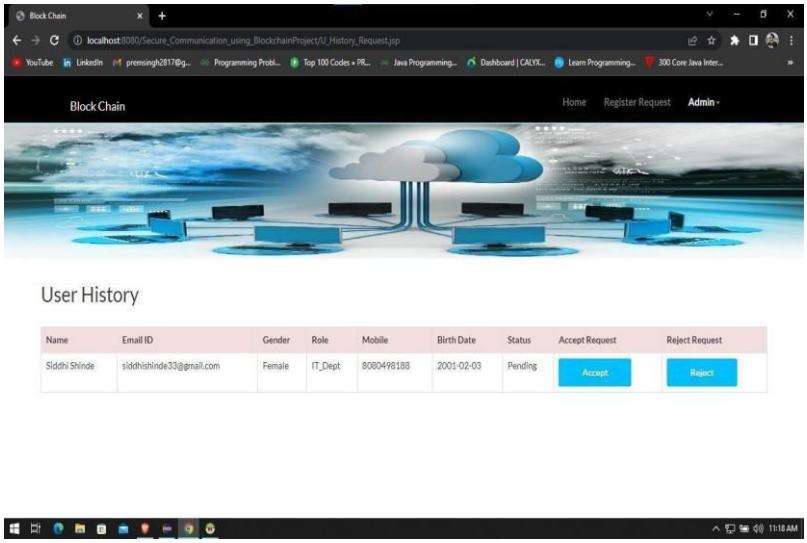


Fig: Authority Register Request Page

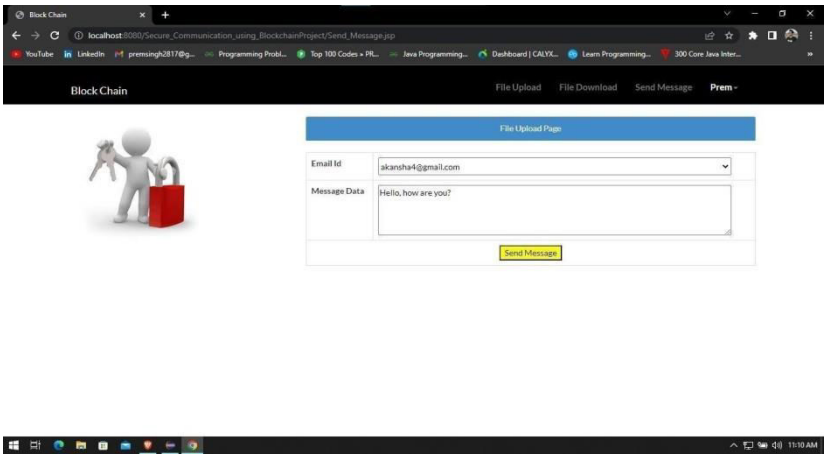


Fig: Data Owner Send Message Page

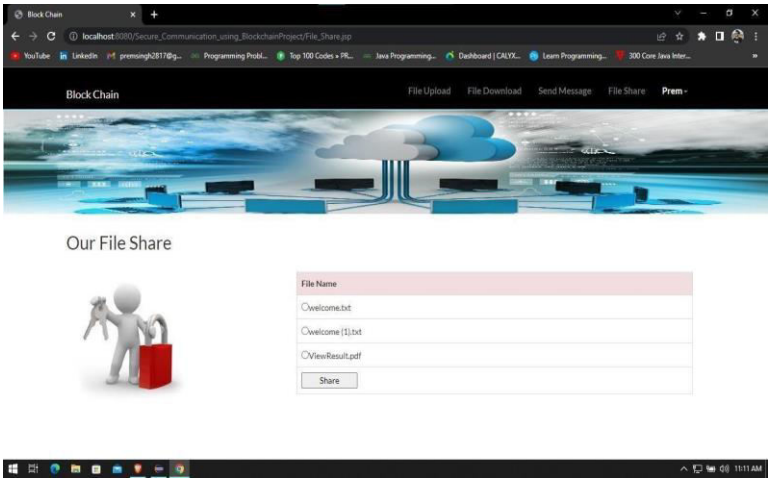


Fig: Data Owner File Share Page

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205411 |

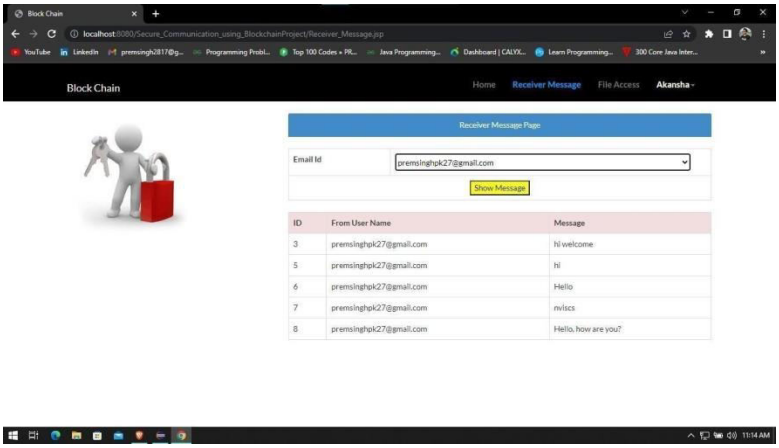


Fig: Data User Receive Message Page

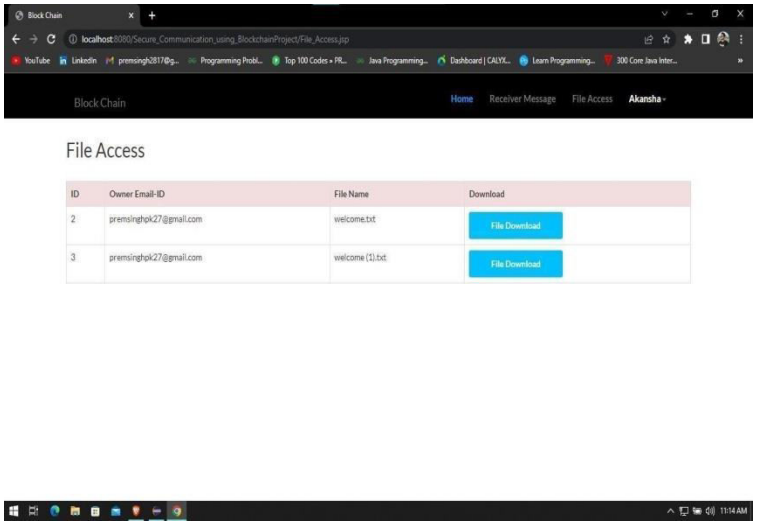
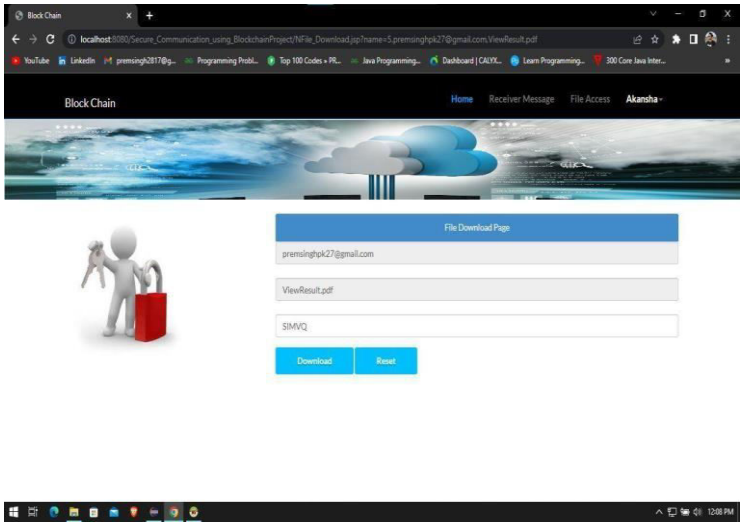


Fig: Data User File Access Page



|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205411 |

VII.CONCLUSION

Encryption and data correspondences are interesting innovative developments. The historical backdrop of encryption components and the different encryption strategies applied to blockchain innovation are introduced in this review. A conversation of Blockchain security assaults is likewise included. A conversation is given in regards to the difficulties of blockchain innovation as well as the different verification and protection security administrations accessible. The accessibility, security, and protection of the confidential information divided among clients of an association can be guaranteed with this program. Future utilizations of blockchain innovation will basically rotate around network protection. The information stays secure and evident regardless of the open and conveyed nature of the Blockchain record. To do this and forestall shortcomings like unlawful information adjustment, encryption is utilized.

VIII.ACKNOWLEDGEMENTS

This project and the research that accompanies it would not have been possible without the exceptional support of our instructor, Prof. Jyotsna A Nanaikar. He was always there to push us a little bit to get the job done on time and on time. He always gave us the freedom to do our thesis and the opportunity to work under his guidance.

We greatly appreciate the help of , HOD Prof. Balaji. Chaugule , Faculty of Information And Technology, and all staff have allowed us to continue our project work in the required university laboratories and use the necessary tools for the project judgment. We would like to express our sincere gratitude to the Principal, Dr. A. M. Kate for his invaluable support and trust in us.

REFERENCES

[1] Jiaqi Yuan, Hui Yang, Shuai Dong, Qiuyan Yao,Libin Jiao, Jie Zhang " Demonstration of Blockchainbased 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 QLearning 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 access control over encrypted spatial data," IEEE Trans. Information Forensics and Security, vol. 14, no. 4, pp. 870{885, 2019.

[9] Hagui,Masoli,Haleli “based blockchain light weight cryptography for security information” IEEE-2021

[10] Nasim Uddin, Shamima Nasrin, Shahinur alam,”secure file sharing system using blockchain,IPFS and PKI Technologies” IEEE-2

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details