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 13, Issue 5, May 2024

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 & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305488 |

A Comprehensive Survey on Blockchain Based Security in Cloud Computing Architecture

Haseeba Mahek, Sheema Fatima, Zufesha Sharmeen, Asma Begum

B.E, Department of CME, SCETW, OU Hyderabad, Telangana, India

Assistant Professor, ADCE, SCETW, OU Hyderabad, Telangana, India

ABSTRACT: Cloud services are vulnerable to assaults due to their widespread use and accessibility by both individuals and corporations. Malicious users may alter data and utilize it for their own gain. Data manipulation, which is a possibility in cloud computing, can also result in the loss of data integrity. Clients using cloud computing across a range of application domains want to know that their data is reliable and correct. However, Blockchain has become a disruptive technology for the future generation of many industrial applications because of its decentralized, transparent, and secure nature. In order to create a tamper-proof cloud computing environment, blockchain—a tamper-proof digital ledger—can be utilized in conjunction with cloud technologies, as discussed in this paper.

In this research, a blockchain-based cloud computing method that guarantees data integrity for all homomorphic encryption techniques is proposed. The suggested system builds a distributed network of processing cloud service providers (CSPs) based on the client requirements, leveraging the Byzantine Fault Tolerance consensus to overcome the CSP's ultimate control over the data. CSPs create master hash values, which are then stored in blockchain networks.

KEYWORDS: Cloud Computing Security, Cloud Service Providers, Cryptography, Blockchain, ,Byzantine Fault Tolerance, Homomorphic Encryption, Crypto currency , Bitcoin, Ethereum.

I. INTRODUCTION

Data security threats are oftentimes what define data security. Cloud computing is vulnerable to a variety of risks, just like any other industry. This is primarily because cloud computing operates by fusing together a wide range of technologies. It is crucial to weigh the advantages of cloud computing and security threats using the risk management approach.

Cloud security, also known as cloud computing security, is an umbrella term for a group of policies, procedures, and technological tools that cooperate to protect cloud-based infrastructure, data, and systems. To safeguard cloud data, adhere to legal requirements, and preserve user privacy, these safeguards are in place. Cloud security can be customized to meet a company's specific demands by building distinct authentication procedures for individuals and devices in addition to offering access to traffic filtering. Furthermore, administrative costs are decreased, enabling IT teams to focus on other aspects of the business, and these policies can be created and maintained in a single location. Either the cloud security solutions already in place or the cloud provider will offer cloud security. Conversely, the solution provider and the business owner ought to work together on cloud security protocols. Even though cloud computing has been around for a while, cluster and grid computing were discovered before it.

It speaks of the techniques and equipment employed to defend cloud computing infrastructures against intrusions from the outside world as well as from within. Cloud computing, or the internet-based delivery of IT services, has become essential for governments and businesses seeking to foster innovation and collaboration. Cloud security and security management best practices for preventing unauthorized access are essential for protecting data and apps in the cloud from current and future cyber security threats.

Cloud Scheduling: - "Scheduling" in cloud computing refers to assigning virtual machines (VMs) to work on available resources or mapping a set of workloads to a set of VMs in order to satisfy user demands. Using cloud scheduling algorithms aims to minimize processing time, maximize resource utilization, optimize system throughput and load balancing, and save energy and money. Thus, to provide appropriate job-to-resource matching, the scheduler needs to consider both user-specified constraints and displayed resources.

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 & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305488 |

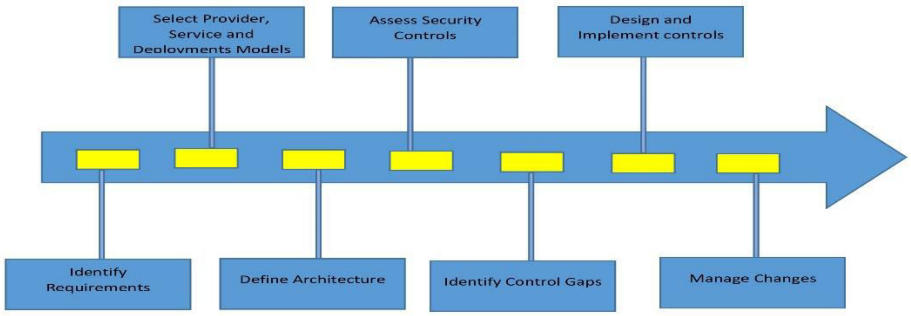

FIGURE 1. CSA Process model for cloud security management

In order to reduce the dangers connected with cloud computing, the Cloud Security Alliance (CSA) has outlined crucial shared obligations for cloud service providers (CSPs) and their clients. Recording, designing, and implementing internal and client security controls are the responsibilities of the CSP. The Consensus Assessments Initiative Questionnaire (CAIQ) is a tool used in the design and implementation process. A Cloud Control Matrix (CCM) is a tool that cloud consumers use to record who is responsible for putting particular controls into place and how they go about doing so. Additionally, as shown in Fig. 1, a high-level process model for cloud security management has been created to accommodate the substantial modifications in the process model that are anticipated to arise throughout the construction of a cloud project.

The key is to outline the prerequisites, organize the architecture, and fill in any gaps based on the capabilities of the cloud platform that underpins it. Even while the CSP makes an effort to build a solid security foundation, such agreements are rarely significant in the eyes of the data owner, particularly when it comes to having faith in the CSP. This is made worse by the fact that new security flaws being created and old ones are exacerbated by the development of cloud computing technology.

II. BITCOIN AND BLOCKCHAIN TECHNOLOGY

A. Fundamentals of Bitcoin

Satoshi Nakamoto addressed the issues with the adoption and usefulness of digital currency, particularly the double-spending issue, in his now-famous paper. Though suspicions abound over Nakamoto's true identity, what is known is that he worked on the Bitcoin project actively until 2010, at which point he stood back and turned the project over to the community for continued development.

He suggested a system that functions as a generator of the computational evidence of the transactional chronological orders and includes a P2P distributed timestamp server. An electronic chain of signatures is called an electronic coin. A set of digitally signed hashes of the preceding transaction and the public key of the subsequent owner constitute each transaction. As seen in Fig. 2, the public key is utilized for transaction verification while the private key is used for transaction signing. The wallet, which can be used online, with hardware, or through software, stores the public key.

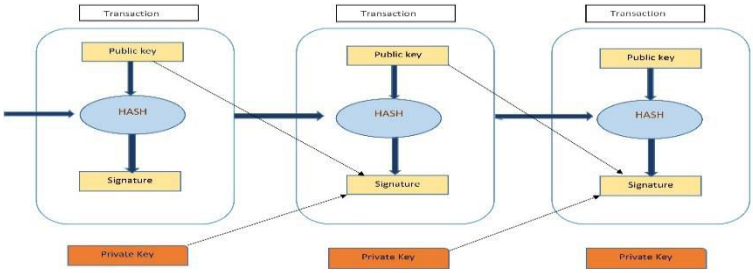

FIGURE 2. Structure of transaction in a Bitcoin blockchain

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

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305488 |

The definition of the Bitcoin ledger is a state transition system made up of a transaction-based state transition function and a state that displays the ownership status of all currently circulating bit coins. A new state is the result of the state transition function. If the sender has sufficient bit coins to complete a transaction, the procedure will result in a state change for both the sender and the recipient; if not, an error will occur.

B. Transactions using Bitcoin

Every transaction is identified by its hash value, which also serves as a collection of inputs and outputs. A transaction's output can only be utilized once throughout the blockchain as an input. It is not permitted in the network to attempt to reference the same output twice as this causes the double-spending issue. The transaction's output is referred to as an unspent transaction output (UTXO) if it hasn't been referenced previously and as a spent transaction output (STXO) if it has. A transaction may have two or more outputs, but it may also have several inputs. Smaller sums of coins can be sent using several inputs, and the outputs can be an amount paid to the recipient or change returned to the sender. The distributed ledger of Bitcoin lists every ownership and transaction within the network. This P2P network maintains a copy of the ledger record on each node. The network is responsible for confirming the accuracy of any transaction made by a user sending a certain quantity of coins to another user.

Nonetheless, an individual may attempt to influence the network by sending several transactions using the same currency to various users (a problem known as double-spending). Additionally, the same user can create multiple instances in order to carry out a Sybil assault and validate his original intent.

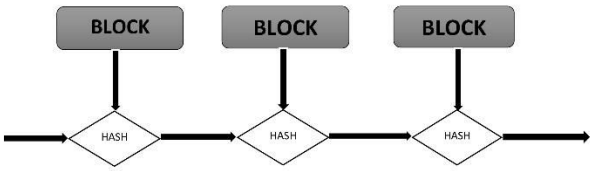

FIGURE 3. The blockchain scheme

C. Blockchain and proof-of-work

In the Bitcoin network, these kinds of scenarios are avoided, or at least reduced, by requiring a proof-of-work from every node that confirms the transaction. To demonstrate that they are legitimate members of the network, the nodes must perform a number of complex calculations. The system will stay consistent and all legitimate transactions will go place as long as the combined processing power of the honest nodes exceeds the computational power of the attacker. A block is declared by a collection of transactions, a nonce, and the hash of the preceding block. A timestamp server proves that the data within a block must have existed at the moment of hashing by creating a hash of the block and making it publicly known. The timestamp server must confirm that the block's timestamp is less than two hours in the future and greater than the timestamp of the block before it in the chain. As seen in Fig. 3, these hashes are connected to form a chain that is known as a blockchain. The ability to track transactions back through time is a key feature of the blockchain. Based on the SHA-256 hash function, Bitcoin's proof-of-work hashing algorithm is comparable to that of Hash Cash. In order to demonstrate proof-of-work, a nonce in the block is increased until a value is generated at the start of the block hash that has the necessary number of zero bits. Once completed, it cannot be undone without starting the calculations over again. Should a malevolent actor manage to alter it in any way, the hashes of every subsequent block would be erroneous. The attacker must have sufficient processing power to override the majority of honest nodes' vote in order to alter a block, which brings up the race problem. The rule is that the longest chain with the majority consensus in the network is the correct one.

III. ETHERUM

The blockchains of Ethereum and Bitcoin are comparable. The primary distinction is that Ethereum blocks include the transaction list and the most current state in addition to the block number, difficulty, nonce, etc. The previous state is applied to construct the new state for each transaction in the transaction list. The Ethereum blockchain's block header comprises the Keccak 256-bit hash of the parent block's header, the recipient's address for the mining fee, hashes of the transaction and receipt attempts, the difficulty, the block's current gas limit, a number that indicates the total amount of gas used in all block transactions, a timestamp, a nonce, and multiple additional hashes for verification.

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

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305488 |

The network's largest issue with Bitcoin is its eligibility for ASIC mining. Ethereum employs the memory-intensive Ethash proof-of-work method, making it less appropriate for ASIC mining. The modified version of the Dagger-Hashimoto algorithm is known as Ethash.

Every Ethereum network node operates under the EVM and carries out its commands. The nodes then translate the smart contracts into EVM code and carry them out. Solidity is one of the most widely used programming languages for creating smart contracts.

The average Ethereum block duration is 15 seconds, while there have been occasional surges of up to 30 seconds. As of January 29, 2018, the Ethereum blockchain size, using the Geth blockchain client with rapid sync, is 47.43GB. The Ethereum network was able to handle over a million unique transactions in a single day, averaging roughly 11 transactions per second, despite worries regarding Ethereum's scalability. The Ethereum platform's "Serenity" prototype, which is based on the Casper consensus algorithm and is slated for later deployment, is meant to facilitate the shift to the proof-of-stake mining paradigm, in which miners are rewarded based on their coin holdings rather than their computations (the more coins a user has, the higher the reward). Token systems, financial derivatives, identity and reputation systems, file storage, insurance, cloud computing, prediction markets, and other applications are listed as possible uses for Ethereum. Decentralized applications are Ethereum's most significant use case (Dapps). Several companies have managed to raise sufficient funds through Initial Coin Offerings (ICOs) to be represented on the cryptocurrency market. These include Golem, which specializes in supercomputing; Augur, which offers prediction markets; Civic, which verifies and protects identity; OmiseGO, which offers exchanges on a public blockchain; Storj, which rents out hard drive space; and many more.

IV. AN OUTLINE OF THE PBFT ALGORITHM

The Byzantine problem consensus algorithm known as the PBFT algorithm was first put forth by Miguel Castro and Barbara Liskov in 1999. The Byzantine problem can be resolved by reducing the temporal complexity of the original Byzantine method from an exponential level to a polynomial level. From a theoretical to a practical application level, the issue has evolved. The distributed scenario's consistency of state machine copies is resolved using the PBFT algorithm.
The three components of the PBFT algorithm's fundamental idea are view, replica, and role. The picture depicts the current system's overall condition. The system's participating nodes split into duplicates. The roles in replicas are separated into two groups in every view. The other clones act as backups, with one replica functioning as the primary. The three primary protocols that make up the PBFT consensus algorithm are the checkpoint, view replacement, and consensus protocols. The checkpoint protocol is used for routine cleaning; the view replacement protocol is used to replace the malfunctioning node to ensure normal system operation; and the consistency protocol is used to ensure that the data saved by all nodes in the entire network is consistent, which is realized through mutual communication between the three-stage nodes. Expired interactive data synchronizes inconsistent nodes, periodically verifies if the system is unified, and relieves load on node storage. The fundamental protocol that the PBFT algorithm uses to finish the consensus process is known as the consensus protocol. The execution process is displayed. The following three procedures make up the majority of the consensus protocol:

(1) Pre-prepare: The master node creates a pre-prepare message in accordance with the service request message and broadcasts it to the slave nodes after receiving the service request message and confirming that it is accurate.

(2) Get ready: The slave node checks to see if the message content has been altered after receiving the pre-prepare message from the master node. Following accurate content verification, the slave node will broadcast a prepare message to all replica nodes in accordance with the pre-prepare message.

(3) Commit: Consensus has been obtained after receiving $2Z + 1$ commit messages (including themselves), at which point the nodes will carry out the request and write data.

V. ENCRYPTION USING HOMOMORPHISM

With homomorphic encryption, the person holding the decryption key can obtain the result of the encryption process without needing to be aware of the contents of each cipher text at all times. Semihomeomorphic encryption, homomorphic-like encryption, and complete homomorphic encryption are the three categories of homomorphic encryption techniques. There are three types of encryption algorithms: semi-homeomorphic, which can only perform

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

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305488 |

one of the three algebraic operations—or, addition, and multiplication—at the same time; homomorphic, which can perform a limited number of additive and multiplicative operations simultaneously; and full homomorphic, which can perform a combination of additive and multiplicative operations at any given time.

VI. LITERATURE SURVEY

Year	Reference Paper Title	Methodology and Modules	Dataset Used	Result	Limitations
2020	A Review Paper on Security Concerns in Cloud Computing and Proposed Security Model.	Security Access Control Service Model (SACS) Data Security susing Encryption and Steganography Enhanced Data Security model Cloud Security Service using Data mining	H.K and Usma (2015) Data Security in Cloud Computing using international journal of Encryption and Steganography	Threats identified Proposed Modes (SACS) Performance Evaluation Research need Security Model Refinement	Issues rule as multi-tendancy , IP Spoofing, DNS poisoning, Address additional security challenges
2022	.Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing	Blockchain Evolution Security services Future Direction and challenges Bitcoin, Crypto currency.	Data heterogeneity Data de-duplication techniques	Blockchain Evolution Various platforms of Blockchain Technology	Lack of detailed analysis Limited discussion on scalability and hardware issues.
2019	Blockchain Technology, Bitcoin, Ethereum: A Brief Overview.	Bitcoin Essential Bitcoin transaction Proof of work and Blockchain Bitcoin Network and mining Segwet and Lightning Ethereum	There is no data set used specifically	Bitcoin Ethereum Crypto currencies	Numerous crypto currencies, hashing algorithms, and consensus agreements in the networks
2022	Survey on Cloud Computing Security And Scheduling.	Security Concerns in cloud computing Cloud Security Threats: DOS attack, SQL injection, Phishing attacks.	Specifically no data set is used	Two step authentication system Cloud Computing Security Robust Security measures	Paper does not extensively address all potential security threats and challenges in cloud computing
2020	Research on Practical Byzantine Fault Tolerant Consensus Algorithm Based on Blockchain	Consensus Algorithm PBFT Algorithm	Blockchain Classification and Comparing	PBFT Algorithm execution process Zyzzyva execution process Hybrid consensus algorithm	Combining the Blockchain consensus algorithm improvement theory can be done in further researches.

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

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305488 |

Year	Reference Paper Title	Methodology and Modules	Dataset Used	Result	Limitation
2020	Review Of Cryptography in Cloud Computing	RSA(Rivest-Shamir-Adleman) ElGamal Symmetric Key Cryptography(AES,DES,BLOWFISH,RC5,3DES) Hashing Key Cryptography Homomorphic Encryption	There is no specific dataset used.	Symmetric Cryptography(AES,DES,BLOWFISH,RC5,3DES)	The topics are not specifically explained in depth
2022	The Blockchain and Homomorphic Encryption Data Sharing Method in Privacy Preserving Computing	Homomorphic Encryption Traceability Privacy-Preserving Asymmetric Encryption	Comparative Analysis Of Data sharing accuracy Comparative Analysis of data transfer time	In-depth Examination of Cryptographic Algorithms Transmission techniques based on homomorphic encryption.	Other data sets should have be used to explain more about the topics
2020	Cloud Service Providers : An Analysis of Some Emerging Organisations and Industries	Cloud service providers SaaS PaaS Modern Cloud Services	No specific dataset	Cloudways Digitaloceans Kamatera Rackspace Massive grid Alibaba Liquid Web Azure Vmware Oracle	Government rules, regulations, and norms are most vital in this context as well.
2019	Application of Cloud Computing in Blockchain.	Theoretical framework and algorithms in the context of blockchain technology and cloud computing frameworks Evaluating digital brand marketing strategies, identifying the scope of blockchain technology	No Specific dataset It focuses on prior papers	Review of Blockchain Technology in Cloud Computing Systems Advantages and Disadvantages of Blockchain and Cloud Computing Prior Papers and Research Gaps in the Field Significance of Blockchain Technology in Cloud Computing Insights into Potential Threats and Challenges Assistance for Upcoming Researchers in Designing Secured Models	Development process of blockchain-based cloud systems. It highlights issues such as access control, communication disruptions, unexpected financial loss, and scalability degradation due to the creation of fake accounts.

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

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305488 |

VII.CONCLUSION

The paper delves into the critical aspects of cloud computing security and the integration of blockchain technology, shedding light on the vulnerabilities and challenges faced in cloud services. It extensively discusses the benefits and applications of blockchain technology in enhancing cloud security measures. The study underscores the necessity for robust security protocols to mitigate potential threats effectively. Furthermore, it emphasizes the importance of ongoing research to address emerging security challenges in cloud computing and blockchain integration. The findings underscore the significance of implementing advanced security measures to safeguard data and ensure the integrity of cloud-based services.

REFERENCES

[1] T. Kavitha, S. Hemalatha, T. M. Saravanan, A. K. Singh, M. I. Alam and S. Warshi, "Survey on Cloud Computing Security and Scheduling," , 2022, pp. 1-4, doi: 10.1109/ICCCI54379.2022.9740932. https://ieeexplore.ieee.org/document/9740932

[2] Ergashev Nuriddin G‘ayratovich. (2022). “The Theory of the Use of Cloud Technologies in the Implementation of Hierarchical Preparation of Engineers”. Eurasian Research Bulletin, 7, 18–21. Retrieved from https://www.geniusjournals.org/index.php/erb/article/view/1009

[3] Habib G, Sharma S, Ibrahim S, Ahmad I, Qureshi S, Ishfaq M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. Future Internet. 2022; 14(11):341. https://doi.org/10.3390/fi14110341

[4] R. Doshi and V. Kute, "A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1-4, doi: 10.1109/ic-ETITE47903.2020.37. https://ieeexplore.ieee.org/document/9077910

[5] Kavuri, S.K.S.V.A. & Kancherla, Gangadhara & Brao, Bobba. (2017). “An Improved Integrated Hash and Attributed based Encryption Model on High Dimensional Data in Cloud Environment. International Journal of Electrical and Computer Engineering”. 7. 950-960. 10.11591/ijece.v7i2.pp950-960. https://www.researchgate.net/publication/318092280_An_Improved_Integrated_Hash_and_Attributed_based_Encryption_Model_on_High_Dimensional_Data_in_Cloud_Environment

[6] He, Ningyu & Wu, Lei & Wang, Haoyu & Guo, Yao & Jiang, Xuxian. (2019). “Characterizing Code Clones in the Ethereum Smart Contract Ecosystem”. https://www.researchgate.net/publication/332799463_Characterizing_Code_Clones_in_the_Ethereum_Smart_Contract_Ecosystem

[7] Di Angelo, Monika & Salzer, Gernot. (2020). “Wallet Contracts on Ethereum”. 1-2. 10.1109/ICBC48266.2020.9169467. https://www.researchgate.net/publication/343704204_Wallet_Contracts_on_Ethereum

[8] Sehgal, Naresh & Bhatt, Pramod & Acken, John. (2020). “Foundations of Cloud Computing and Information Security”. 10.1007/978-3-030-24612-9_2. https://www.researchgate.net/publication/335636398_Foundations_of_Cloud_Computing_and_Information_Security

[9] Zaineldeen, Samar & Ate, Abdelrahim. (2020). “Review of Cryptography in Cloud Computing”. 9. 211-220. https://www.researchgate.net/publication/340435364_Review_of_Cryptography_in_Cloud_Computing

[10] Vujičić, Dejan & Jagodic, Dijana & Ranđić, Siniša. (2018). “Blockchain technology, bitcoin, and Ethereum: A brief overview”. 1-6. 10.1109/INFOTEH.2018.8345547. https://www.researchgate.net/publication/324791073_Blockchain_technology_bitcoin_and_Ethereum_A_brief_overview

[11] K. Gai, Y. Wu, L. Zhu, L. Xu and Y. Zhang, "Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7992-8004, Oct. 2019, doi: 10.1109/JIOT.2019.2904303 https://ieeexplore.ieee.org/document/8664577

[12] M. S. Chishti, F. Sufyan and A. Banerjee, "Decentralized On-Chain Data Access via Smart Contracts in Ethereum Blockchain," in IEEE Transactions on Network and Service Management, vol. 19, no. 1, pp. 174-187, March 2022, doi: 10.1109/TNSM.2021.3120912. https://ieeexplore.ieee.org/document/9577210

[13] Zheng, Xiandong & Feng, Wenlong. (2021). Research on Practical Byzantine Fault Tolerant Consensus Algorithm Based on Blockchain. Journal of Physics: Conference Series. 1802. 032022. 10.1088/1742-6596/1802/3/032022. https://www.researchgate.net/publication/349940360_Research_on_Practical_Byzantine_Fault_Tolerant_Consensus_Algorithm_Based_on_Blockchain

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

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