e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 13, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

Enhancing Security Intelligence and Safeguarding Privacy with D. Spectre in Blockchain Technology

Dinesh Kumar[1], Dhayalan[2], Dharneesh[3] Ms. S. Queenkirubaananthy[4], Dr.V.Vijaya kumar[5]

PG Student, Department of Computer Science and Engineering,, AVS Engineering College, Tamil Nadu, India[1,2,3]

Assistant Professor, Department of Computer Science and Engineering, AVS Engineering College, Tamil Nadu, India[4]

Professor & Head, Department of Computer Science and Engineering, AVS Engineering College, Tamil Nadu, India[5]

ABSTRACT: The increasing use of mobile phones in the modern world has led to challenges for many individuals who struggle to remember their passwords, making it difficult to store and retrieve contacts. To tackle this issue, an innovative solution has been developed to facilitate the secure storage and retrieval of contacts and messages using passkeys. Passkeys are constantly evolving to keep pace with the advancements in cloud storage, which in turn enhance their reliability and accessibility for users. To ensure the highest level of security for user data, blockchain technology is employed. This technology offers key benefits such as transparency, security, and accountability. The blockchain operates as a decentralized ledger, providing a secure and transparent platform for transactions. This makes it the ideal solution for the storage and management of user data, as it leverages ECC and SHA algorithms to uphold a robust level of security.

This solution aims to provide a hassle-free and secure experience for users, with the belief that it will achieve this goal effectively. Incorporating multi-asset transactions, verification, and traceability further enhances data security. Personal Identity Security (PIS) in blockchain D.Spectre is more efficient than existing systems such as Gmail contacts, benefiting various sectors and end-users by enabling fast and secure data retrieval.

INDEX TERMS: Blockchain, fog computing, passkeys, PIS (personal identity security), ECC - Elliptic Curve Cryptography, SHA- Secure Hash Algorithm.

I. INTRODUCTION

By integrating D. Spectre into blockchain technology, businesses, and individuals can achieve a higher level of security intelligence while also addressing privacy concerns proactively. This innovative approach holds the potential to revolutionize the way security measures are implemented in the digital age.

Retrieving emergency contacts is crucial within the current system. The system currently relies on factors such as logging into the email ID, but this process often poses challenges as users struggle to remember passwords. When opting to reset the password, an OTP can be generated on other devices, complicating the contact retrieval process.
To address this issue, we have developed the D.Spectre application. This innovative tool simplifies emergency contact retrieval by securely storing data in a fog cloud, safeguarded by blockchain technology.

A key feature of the application is its intrusion detection capability, enhancing security and privacy for users. The integration of fog computing and blockchain technology has proven to be instrumental in bolstering security measures. Fog cloud technology is rapidly gaining prominence in the realm of cybersecurity. By decentralizing storage and processing capabilities for internet-connected devices, fog cloud servers offer improved latency and reduced bandwidth usage.

Sensitive user data, encrypted in traditional cloud computing systems, remain vulnerable to security breaches. FCBS (Fog Cloud Blockchain Server) presents a reliable solution to fortify security measures against potential threats.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

Blockchain technology, a cornerstone of modern security protocols, plays a vital role in authorization and authentication processes. Through the implementation of hash key algorithms, only authorized users can access the system, ensuring atmost security.

D. Spectre further enhances security with its innovative passkey system, eliminating the need to recall passwords. Users can log in using their fingerprint, facial recognition, or two-factor authentication, reducing the risk of cyber-attacks. The system validates user identity through authorization and authentication processes, utilizing the robust HASH KEY algorithm for added security.

II. RELATED WORKS

Cloud computing gained a large number of users in recent years due to the features of convenience economy and availability.

According to the **Cheng Zhang et al (2021)**. The single service provider is not enough, so he proposed the multi-cloud storage system, still the data auditing scheme is based on multi-cloud storage to confirm the integrity of outsourced data. The auditing scheme is trusted by a third-party App (TPA) and the cloud servicer. Then, they present a blockchain-based multi-cloud storage data auditing scheme. It can protect the data integrity and arbitrate service disputes. With the help of blockchain and homomorphic verifiable tags achieve low-cost batch verification without the third-party App (TPA). Theoretical experiment says the scheme is more effective in the multi-cloud and the cost is reliable.[1]cost is reliable.[1]

According **to Yang Xu et al (2020)**, the arising of the 5G technology creates a more open ecosystem in the vertical industries focusing on content-sharing services, especially mobile telemedicine. Similarly, on the other hand, side, cyber threats and vulnerabilities also increased in the 5G technology such as information leakage and privacy. It is difficult to find the information leakage based on the existing tracking system. Then, they propose the blockchain-based accountability mechanism. This mechanism works against information leakage in vertical industries. It can convert the information into vector form with the help of blockchain technology the service provider and the client can share the content safely. Last but not least, homomorphic encryption to avoid the disclosure of watermark content.[2]

To increase the availability of data in the cloud many users store their data in multiple cloud services. According to **Jiguo Li et al (2019),** the integrity of multi-copies of some provable data possession (PDP) is created. However, the (PDP) provable data possession considers all copies can be stored in a single cloud storage service. The PDP protocol can depend on the public key infrastructure (PKI). The PKI suffers many vulnerabilities and brings computational costs. To increase security intelligence, introduce a novel-based PDR scheme of multiple copies in multiple cloud storage servers. In this PDP scheme the data and stored in the different cloud storage servers. By the introduction of homomorphic key verifiable tags, the integrity of all copies can be checked. The security of the scheme is efficient and it is practice to use.[3]

The usage of cloud among the people is increasing day by day. However, security concerns such as privacy, and data integrity also increase. To solve this, the existing technique uses a public verification scheme to enable a user to employ a third party to verify the data integrity. According to **Yuan Zhang et al** (2019), this scheme is vulnerable to processing auditors and it is not verified within the time. Most of the public verification schemes work based on the public key infrastructure (PKI) and it suffers from the certificate management problem. To solve the issue, introduce the first certificateless public verification against the processing auditors (CPVPA) by using the blockchain. In this CPVPA it can check the auditors can record each verification within the time.[4]

Blockchain is an emerging technology and it creates attention in various fields. According to **Ruizhe Yang et al (2019)**, the blockchain has a limit to supporting the services with frequent transactions. Edge computing is introduced to expand cloud resources but it faces the issue of decentralized management. To solve the issue the integration of blockchain and edge computing can bring access and control of network, and storage. The main prospect of integrating blockchain and edge computing is self-organization, functions integration, and resource management, and then the security issue can be addressed [5].

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

Cloud computing is an emerging technology that makes attention among people. It is convenient data storage for individuals or organizations. According to **Xiaodong Yang et al (2020)**, still, in cloud computing, there are several issues in security concerns. The existing public scheme enables access to third-party Apps (TPA) to verify the data integrity and it is based on public key infrastructure. The existing system does not allow dynamic data storage and all data can be stored in one cloud. Once the cloud server fails there will be no retravel. To solve this introduction the certificateless multi-replica and multi-cloud data public auditing scheme based on blockchain. In this scheme, a dynamic hash table and modification record are introduced [6].

Qian Wang et al (2011), detected that cloud computing is the next-generation architecture of IT enterprise. It moves the application and database into the centralized cloud. The issue in the cloud storage is allowing the third-party auditor (TPA) on behave of the cloud client to verify the data. It eliminates the involvement of the client to verify the data stored in the cloud. This paper analyzes and identifies the difficulties and security problems with fully dynamic data updates from prior works. To achieve the data dynamically, improve the proof of storage model by manipulating the classic Merkie hash tree construction. Then further introduce the bilinear aggregate signature to extend the result [7].

The development of network computing technologies like cloud computing brought a public and economic network-based service that benefits a large number of users around the world. According to **Yang Xu et al (2020),** network storage is not reliable for keeping the user's data. This paper proposes a decentralized arbitrable remote data auditing scheme for network storage services based on blockchain techniques. Then propose an arbitrable data auditing protocol with the help of the hash technique. Additionally, the decentralized adjunction mechanism was implemented by using the smart contact technique [8].

Cloud storage services allow users can store their data in the cloud to avoid storing in local data storage and it is cost-free and low maintenance. **Wenting Shen et al (2018)** analyzed the existing system user use of the private key to data authenticators for realizing data integrity auditing. To store the private key user possesses the hardware token (smart card, USB, token) and the user needs to remember his password to activate the private key. If in some conditions the hardware token is lost or the password is forgotten the data integrity auditing scheme does not work. To solve the issue propose a new technique called data integrity auditing without private key storage. Additionally, new features use biometric data to store the data instead of hard work tokens. This scheme is effective in data integrity auditing[9].

Fu Xiang et al (2017), analyze the trend of economic globalization and its growth. The data can't be stored in a traditional single cloud provider and it does not handle the current data. The proposed JCLedger, A blockchain-based distributed ledger for joint cloud computing. It aims to improve the cooperation among the many cloud service providers. The main thing to provide is the cross-cloud service. Additionally, introduce the new method of cryptocurrency provider(CCP). The CCD function is to transfer the cryptocurrency. Further, analyzes the four most important mechanisms for JCLedger[10].

According to **Bin Liu et al (2017),** data integrity in IoT-based cloud computing is difficult. Because the iot based cloud computing is a dynamic environment. In the existing system data integrity verification with public auditory is based on the third-party auditors(TPA's). But in IoT-based cloud computing the TPA framework is difficult to use because it's dynamic. So, instead of using the TPA framework propose the blockchain-based framework to verify the data integrity storage. By using the blockchain-based framework the data is more reliable data integrity verification for both the data consumers and the data owners without using the TPA[11].

In the modern world, network storage devices are gaining a large number of users due to the low cost and the scalability of data. According to **Yang Xu et al (2020),** the security concerns and the performance affect the scalability of the network storage system. The existing system has some countermeasures such as data auditing mechanisms and the deduplication technique. The existing countermeasure cannot solve problems like cost and the data integrity verification of Third-party apps. Then it also faces issues like repeated auditing of data shared by multidentate. To solve these types of issues propose the blockchain-based de-duplicable data auditing mechanism. In this mechanism first design a client-side data deduplication scheme. This scheme is based on the bilinear pair techniques. It reduces the burden on both users and the service providers. This mechanism achieves trustworthy and efficient data auditing it can help the data integrity by using the blockchain and the bilinear pairing cryptosystems [12].

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

In recent eras, cloud computing gained a large number of users within a short period because it is dynamic, flexible, and cost-effective. **Huaqun Wang et al (2014)**, concludes research about provable data possession (PDP) as a technique cloud service providers (CSPs) to prove the client data can be integrated without downloading the client's entire data. The construction of an effect was as been proposed in 2012. In this scheme, it can store and maintain the client's data, based on the homomorphic verifiable response and hash index hierarchy. similarly proposed the cooperative PDP from the bilinear pairings. The Zhu et al CPDP cannot satisfy the property of knowledge soundness. However, the CPDP based on the bilinear pairings satisfies the property of knowledge soundness and regret that any malicious CSP can respond even if they delete all the stored data[13].

In the past years, cloud computing has become an important theme in the computer field. According to **H. Wang et al (2014),** data integrity checking is important in cloud computing. The remote data integrity can verify the client's outsourced data is kept without downloading the whole data. Sometimes the client has to store the data in the multi-cloud server. Similarly, the integrity protocol saves the user's costs. This point introduced a novel-based remote data integrity model. The model is ID-PDP (identity-based distributed provable Data possession) in multi-cloud storage. Based on the bilinear pairings a concrete ID-PDP protocol is designed. This protocol works under difficult situations like standard CDH (computational Diffie Hellman) problems. Additionally, the advantage of eliminating the certificate management the ID-PDP protocol is scalable and flexible [14].

Over the years cloud storage services have become a faster growth in technology and make more profit by providing low-cost, scalable, and platform independent for client's data. Provable data possession (PDP) technique in data integrity to store the outsourcing data for clients. **Yan Zhu et al (2012),** construct an efficient PDP scheme for distributed cloud storage. This model supports the scalability of service and data migration. The efficient cooperative PDP(CPDP) scheme. It is based on homomorphic verifiable response and hash index hierarchy. This scheme is based on the multiprover zero-knowledge proof system. Additionally, the performance is increased in this scheme [15].

III. METHODOLOGY

D.Spectre is a spectacular application designed for secure storage and access to user data on the cloud. Users can create an account by providing their mobile number as a username and utilizing passkeys as their unique passwords. Passkeys are a passwordless authentication solution, eliminating the need for users to remember multiple passwords for different accounts. The data is stored in the fog cloud, a centralized and distributed database that utilizes edge devices or distributed local databases. This innovative approach enhances scalability, reliability, and efficiency across a variety of applications. The fog cloud's distributed nature ensures data security.

Furthermore, D.Spectre leverages blockchain technology to bolster the security of end-user data. Blockchain is a decentralized and distributed ledger used to record transactions on numerous computers. It provides a secure and tamper-proof method of data storage. To access their data, users simply need to install the D.Spectre application and verify their identity by entering their user ID, passkeys, and a unique blockchain HASHKEY. The HASHKEY serves as an additional layer of security, similar to a two-step verification process. Individual HASHKEYs are generated using an algorithm specific to each user, and users must authenticate these keys whenever logging into the application.
The primary objective is to safeguard user data against cyberattacks. In today's environment, data breaches are on the rise due to inadequate security measures and mishandling of data. However, the HASHKEY algorithm ensures the generation of 128-bit keys.

The SHA algorithm, such as SHA-256, is utilized for hashing user credentials and sensitive data before transmission and storage. The SHA algorithm enhances security by producing a fixed-size hash value, ensuring data integrity and authenticity. Hashing with SHA ensures that sensitive information is transformed into a unique hash code, making it computationally infeasible to reverse-engineer the original data. The SHA algorithm is employed in conjunction with other security measures, such as two-step verification, to strengthen the protection of user data stored in fog clouds. SHA algorithms, such as SHA-256, are employed for hashing sensitive data and verifying data integrity during transmission and storage. The implementation of SHA enhances the security of end-user data by providing a robust cryptographic hash function. SHA plays a crucial role in safeguarding user information against unauthorized access and data breaches.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

Traceability within D. Spectre has been integrated to bolster cybersecurity. If a cloud server is compromised, user data is organizations can significantly enhance their cybersecurity protocols and maintain the integrity of sensitive data.The seamlessly transferred to another server in the form of an image. This image encapsulates the user's data and is subsequently forwarded to the new server, ensuring uninterrupted access to the data for the user. The confidentiality of end-user information is safeguarded through blockchain technology.Fog Server ensures rapid and efficient data processing by transferring the computational workload to the cloud. Detecting fraud through the analysis of jitter and delay metrics relies on real-time measurements. The detection and prediction of fraud should consider the Time Taken for Bytes (TTFB) as follows for delay calculation:

Delay = length / (Size of data/bandwidth of network) …… (1)

Information security, the incorporation of D. Spectre utilizing blockchain techniques represents a promising approach to reinforce security measures and address privacy concerns. By incorporating D. Spectre within the blockchain framework,

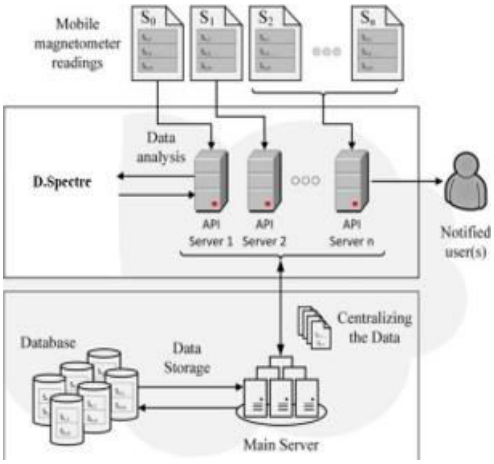

Fig 3.2 D.spectre process flow

Key benefits of leveraging D. Spectre in blockchain techniques include:

- Strengthened security measures to deter cyber threats and unauthorized access
- Improved privacy safeguards to protect personal and confidential information
- Enhanced traceability and transparency in data transactions

Mitigation of risks associated with data breaches and compromised security system

By integrating D. Spectre into blockchain technology, businesses, and individuals can enhance their security intelligence and proactively address privacy concerns. This innovative approach has the potential to revolutionize how security measures are implemented in the digital age.

The rise of cloud storage in recent years can be attributed to the growing number of users worldwide. In response, the concept of Fog Computing has emerged. Fog computing involves a cloud that stores data near end users, serving as an intermediary layer between the centralized cloud and the data-generating device.

power management enhances traceability and identifies the client entering an initial state.

Propagation Speed = 1 / Transmission Speed (Tx) …… (2)

The data may be vulnerable depending on the method of time management used. By employing the blockchain (BC) method, both the time and Authentication Center (AuC) can be simultaneously traced. AuC and Authentication Token (AuT) allow BC to authenticate a user's identity and trace a function's path in both initial and final states. The Function Centric Block Chain (FCBC) categorizes functions into three layers to safeguard data and boost security intelligence.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 11, November 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1111001 |

The banking system prevents server downtime by measuring delays (Equation 1 The BC in D.spectre has evaluated the layer convenience of the security instrument using three confirmation methods. It defaulted to PSM (pre-presented secure mode), which uses symmetric encryption to convert messages securely. Key centers have been selected to obtain a new key to verify segment consistency without the need to control messages using ASMrp (Authenticated Mode), facilitating secure message exchange and preventing no-response incidents. The attacker model introduced IPV6. The geography includes root, malicious node, and interpretation number attacks. To prevent the exploitation of the root node that cannot be identified by the ID, internal and external attackers are protected using ECC (Elliptic Curve Cryptography in 5G).

It has been communicated and noted the version number of a marker for individuals inciting or planning activities within the most secure Tx in the network across the association. This is an essential measure for identifying the root center point and validating whether a change has occurred through the established processes. The D.Spectre centers and topography play a vital role in exchanging control messages and handling root changes within the system. In the positioning system, packets are categorized based on the presence of malicious messages during transmission and reception within the network. Determining the peak and vapor, along with assessing the impact on network performance in the cloud, is crucial for detecting false positioning. Utilizing ECC in both scenarios is essential for accurate identification. The system number must be adjusted based on network flow time in each MUX.DEMUX layer during ECC modifications.

Hence, Association Rule Mining (ARM) extracts are utilized to identify data propagation and transmit data to the cloud. Equation 2 determines the speed of data transmission, which is correlated with the functionality of the Fog Server (FS). The hardware compliance of the banking system may be at risk, so FS can securely send and retrieve backup files from the Function Center (FC) without compromising the data. Analyzing data is crucial for strengthening security by monitoring the three function layers. Progress can be updated after each completed step, as this process is part of a sub-server managed by the FC.

Transmission Speed Detection = Distance between points x and y / Transmission Speed …… (3)
Equation 3 illustrates the synchronization mechanism of the FCBC in data processing and management, as it is integrated into the entire end-to-end system. The distance between interconnected endpoints is calculated as:
= 0.7 * 3 * 10^8 m/sec = 2.1 * 10^8 m/sec (Transmission speed).

IV. RESULT AND DISCUSSION

To access information stored in a fog cloud, a robust verification and authentication process is essential. This process ensures that the information is retrieved only by the intended individual.

Verification involves confirming the identity of the user attempting to access the information. This can be done through various methods such as biometric scans, passwords, or security questions. Authentication, on the other hand, is the process of validating the credentials provided during the verification stage. This step further ensures that the user is authorized to access the information stored in the fog cloud.

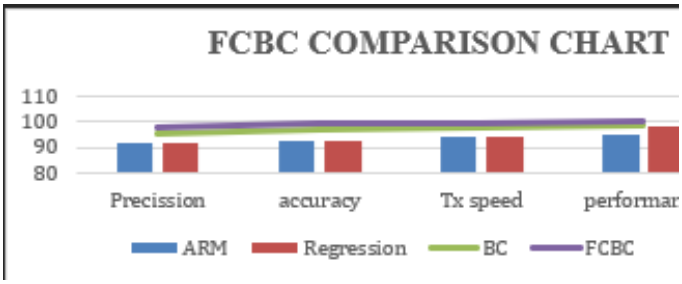

Fig 4.1 Accuracy

By implementing a comprehensive verification and authentication process within the fog cloud infrastructure, organizations can effectively uphold the security and privacy of individual data. Establishing stringent protocols is

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 11, November 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1111001 |

crucial to prevent unauthorized access to sensitive information and safeguard it from potential breaches. These protocols serve as a vital barrier that protects vulnerable data from falling into the wrong hands, thereby ensuring the confidentiality and integrity of stored information. The enforcement of these security measures is essential in mitigating risks and maintaining the trust of users whose data is stored within the fog cloud environment. By prioritizing the establishment of robust security protocols, organizations can confidently leverage the benefits of fog computing while upholding the highest standards of data protection.

V. CONCLUSION AND FUTURE ENHANCEMENT

As we navigate the ever-evolving landscape of blockchain technology, it becomes increasingly clear that the integration of D. Spectre holds immense promise in bolstering security intelligence and safeguarding privacy. By harnessing the power of decentralized networks and innovative solutions like Fog Computing, we are paving the way for a future where data protection is not just a possibility but a standard.

As we conclude our exploration into the realm of blockchain technology enhanced by D. Spectre, it is evident that the potential for greater security and privacy measures is within reach. By embracing these advancements and staying vigilant against emerging threats, we can forge a path toward a digital ecosystem that prioritizes both innovation and protection.

REFERENCES

1. Cheng Zhang, Yang Xu, Yupeng Hu, Jiajing Wu, Ju Ren and Yaoxue Zhang, Blockchain-Based Multi-Cloud Storage Data Auditing Scheme to Locate Faults, issues: The complexity and overhead introduced by blockchain-based multi-cloud storage data auditing schemes may challenge system performance and scalability, IEEE Transactions on Cloud Computing, 2021.
2. Yang Xu, Member, Cheng Zhang, Quanrun Zeng, Guojun Wang, Yaoxue Zhang, Blockchain-Enabled Accountability Mechanism Against Information Leakage in Vertical Industry Services, issues: The nonnegligible limitation in practice due to trusted third party IEEE Transactions on Network Science and Engineering,2020.
3. Jiguo Li, Hao Yan, and Yichen Zhang, Efficient Identity-based Provable Multi-Copy Data Possession in Multi-Cloud Storage, issues: Due to one cloud storage server bringing communication security vulnerabilities, IEEE Transactions on
4. Yuan Zhang, Chunxiang Xu, Xiaodong Lin, and Xuemin (Sherman) Shen, Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors, issues: CPVPA may introduce complexities in integrating with existing systems due to the adoption of blockchain technology, IEEE Transactions on Cloud Computing, 2019.
5. Ruizhe Yang, F. Richard Yu, Pengbo Si, Zhaoxin Yang, and Yanhua Zhang Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges. Issues: significant research challenges such as scalability enhancement, self-organization, and function integration, IEEE Communications Surveys & Tutorials, 2019.
6. Xiaodong Yang, Xizhen Pei, Meiding wang li, and Caifen Wang, Multi-Replica and Multi-Cloud Data Public Audit Scheme Based on Blockchain, issues: integrating blockchain introduces complexities in system implementation and management, IEEE Access, volume 8, 2020.
7. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, issues: the scheme may require significant computational resources and expertise, potentially posing challenges for adoption, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, May 2011.
8. Yang Xu, Member, Ju Ren, Yan Zhang, Cheng Zhang, Bo Shen, and Yaoxue Zhang, Blockchain Empowered Arbitrable Data Auditing Scheme for Network Storage as a Service, issues: It may require a certain level of technical expertise and familiarity with blockchain technology, IEEE Transactions on Services Computing, 2020.
9. Wenting Shen, Jing Qin, Jia Yu, Rong Hao, Jiankun Hu, and Jixin Ma, Data Integrity Auditing without Private Key Storage for Secure Cloud Storage, issues: biometric data introduces potential privacy and technical challenges related to the accuracy and reliability of biometric authentication systems, IEEE Transactions on Cloud computing, 2018.
10. Fu Xiang, Wang Huaimin, Shi Peichang, Fu Yingwei, Wang Yijie, A Blockchain-Based Distributed Ledger for JointCloud Computing, issues: introduce complexities in system implementation and management, IEEE 37th International Conference on Distributed Computing Systems Workshops,2017.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 11, Issue 11, November 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1111001 |

11. Bin Liu, Xiao Liang Yu, Shiping Chen, Xiwei Xu, and Liming Zhu, Blockchain-based Data Integrity Service Framework for IoT data, issues: introduce complexities in system integration and maintenance and could hinder widespread adoption, especially in resource-constrained IoT environments, IEEE 24th International Conference on Web Services, 2017.
12. Yang Xu, Cheng Zhang, Guojun Wang, Zheng Qin, and Quanrun Zeng, A Blockchain-enabled Deduplicatable Data Auditing Mechanism for Network Storage Services, issues: a blockchain-based solution may introduce complexities in system integration and management, IEEE Transactions on Emerging Topics in Computing,2020.
13. Huaqun Wang and Yuqing Zhang, On the Knowledge Soundness of a Cooperative Provable Data Possession Scheme in Multicloud Storage, issues: a critical flaw in the scheme's security design allows malicious CSPs, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 1, 2014.
14. H. wang, Identity-Based Distributed Provable Data Possession in Multi-Cloud Storage, issues: the reliance on bilinear pairings for security may introduce computational overhead and complexity, IEEE Transactions on Services Computing, 2014.
15. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, and Mengyang Yu, Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage, issues: The reliance on multiprover zero-knowledge proof systems for security may introduce complexity in implementation and potential overhead, IEEE Transactions on Parallel and Distributed Systems, Vol 23, No. 12, 2012.
16. Sravan Kumar R, Ashutosh Saxena, Data Integrity Proofs in Cloud Storage, issues: SLA introduces complexities in negotiation & management, 3rd Int. Conf. Commun. Netw. (COMSNETS), 2011.
17. Huaimin Wang, Peichang Shi, Yiming Zhang, JointCloud: A Cross-Cloud Cooperation Architecture for Integrated Internet Service Customization, issues: JointCloud: A Cross-Cloud Cooperation Architecture for Integrated Internet Service
18. Customization, IEEE 37th International Conference on Distributed Computing Systems, 2017

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com