International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

FINANCIAL DATA SECURITY USING BLOCK CHAIN AND PROXY RE ENCRYPTION

Chenna Rao.B[1] , Roshith.ch[1] ,Rajesh.G[1]
Mrs.Siva Sakthi k[2], G.Victo Sudha George[2,] J.Jayaprakash[2]
[1] IVYear B.Tech, Dept of CSE, [2] Professor,Dept of CSE
[1]bolligorlachennarao@gmail.com,[1]roshithchennam2002@gmail.com,[1]rajeshgolla54@gmail.com
[1,2] DR. M.G.R EDUCATIONAL AND RESEARCH INSTITUTE,Maduravoyal, Chennai-95, Tamil Nadu,India

ABSTRACT: A significant amount of data is currently preserved via the cloud. A few cryptography is used by Third Party Auditors (TPAs).frequently employed to verify data. more focused methods for requesting cloud data. The goal is to address the privacy and security declaration. By doing this, you may access information via the internet without having to deal with the hassle of web software. cloud-based storage It supports safe data storage on the cloud. Clouds are networked collections of data and mobile applications running on cloud platforms. We will have access to any record, including consumer records, from anywhere in the globe owing to cloud computing. on essence, it may be on the cloud. Used for large parking space, great scalability, and significant financial savings. Security is a problem with cloud computing.

Keywords : Financial, Data Security, Block Chain, Proxy Encryption,

1. INTRODUCRTION

Cloud carrier providers (CSPs) are offering an increasing range of statistics storage options. ensuring the security of data. Any information pertaining to assets, obligations, financial transactions, or other monetary activity is referred to as financial data. Account balances, transaction histories, market prices, investment portfolios, and other data can be included in this blockchain is a distributed, decentralized ledger system that maintains the security, integrity, and openness of data transmitted by recording transactions across several computers. A transparent and impenetrable record of transactions is produced by each block in the chain including a timestamped transaction record, a cryptographic hash of the preceding block, and a unique identifier A cryptographic technique known as "proxy re-encryption" enables a proxy entity to use a single key to re-encrypt ciphertext that has already been encrypted. without first decrypting the original ciphertext, encrypted using a different key. This preserves confidentiality and integrity while enabling safe data transfer between many parties. It is frequently employed in situations when users with different encryption keys need to safely exchange data. For reasons of confidentiality and factual integrity Transfer data across locations using the cloud administrator, malware, rogue cloud providers, or other enemies. The data could be tainted by it. Thus, periodically review the saved modifications. Time intervals At the moment, distant (cloud) record authentication is done via encryption. With Third Party Auditors' assistance (TPAs).

2. LITERATURE SURVEY

[1] Cloud statistics technology that acknowledges protection and privacy: These days, cloud provider carriers store enormous amounts of records. Cryptography is a common tool used by third-party auditors (TPAs). Examine these figures. However, cloud users' information is not protected by maximum auditing software. An overview of the country's research and artwork related to cloud data auditing from TPA The issues of systemic integrity and privacy are urgent, with modern remedies and future research objectives.[2] examinations of laptop systems one of the most crucial features of cloud computing is the protection of data privacy is making sure that data kept there is safe. Facts that are encrypted are kept on cloud servers. seen or altered by the cloud carrier provider. Numerous approaches have been developed to address this issue, although they cannot guarantee correctness security of data storage. This documents any changes made throughout the service; the developer or another individual should give credit to the information owner. Data tagging techniques can be used to audit information for this purpose. Third Party Auditor (TPA) listening is used to do that. TPA is made up of owner information and data. calls sent to the cloud server mostly in response to the statistics that the grasp requests. As though The cloud server and the owner of the records can both be charged by the TPA using such a technique.[3] Request cloud computing services using OpenStack: You will see in this presentation how to integrate audio features with the environment. Everything from the Cloud Audit Data Framework (CADF) is discussed; what are the issues with a distributed cloud platform such as OpenStack and how they're being resolved? Effective application of CADF.[4] protection against cloud audits: issues and novel approaches; IT auditors collect information on IT policies and procedures, analyze key data, and identify areas for improvement. One An IT audit's main goal is to ascertain whether the information device complies with all legal

requirements for protecting client data and for the company to get financial data on standards and other security features. Dangers These needs are much more relevant in the context of modern cloud computing. Business model, but it has to be developed. There is a clear difference between traditional IT protection audits and cloud-based ones. The newsletter's writers examine aptitude issues particular to cloud protection audits and also identify unique to particular cloud computing domains, such as Reliance, the general and medical sectors, and a brand-new protective cloud He offers feedback and listens.[5] Public auditing for comfortable cloud storage using dynamic hash tables: One more and more well-liked use of cloud computing is cloud garage. Both companies are able to provide outsourcing services upon request. Despite this, customers still rely significantly on cloud service providers (CSPs). Determining if carrier providers are living up to their expectations is a challenging task. for the security of statistics. Consequently, it is sense to develop effective accounting techniques that bolster data owners' trust in cloud storage. This newsletter introduces a new public audit tool for safe cloud storage that is based mostly on dynamics. A recently developed two-dimensional facts structure of Facts and data will be reported by 3 Peer Auditor (DPA) to Dynamic Auditor. In contrast to present positions, a proposal delegated power As a result, the computational cost and verbal interchange overhead of data from CSP to TPA are significantly decreased. Despite the fact that they could be very exorbitant, our machine can achieve a superior optimization fee performance than state-of-the-art methods because to the benefits of the DHT architecture.Formally speaking, the purpose of an audit is to show the organization and its efficacy through independent examinations and business-to-business comparisons. Situation Show This method offers auditing that is relaxed. In terms of processing complexity, storage costs, and connectivity overhead, Cloud Garage surpasses earlier plans.[6] Safe Data Exchange on the Internet of Things Through Blockchain-Based Proxy Re-Encryption The efficiency of the proposed system in terms of computation and communication overhead, as well as the security assurances offered by the method, are among the performance metrics assessed in the article.

3. EXISTING SYSTEM

These benefits are now much more alluring because to cloud computing, which also poses novel and intricate security risks to user data that is outsourced. The ordinary person is essentially given control over their own riches through information outsourcing as cloud service providers (CSPs) are distinct management organizations. For the following reasons, the cloud of justice created by this purpose threatens information. Even though cloud computing has more reliable and accurate infrastructure than personal computers, there are still many internal and external dangers that compromise the data's integrity. In terms of the standing of their information that was outsourced, these additional incentives for CSPs are unjust to cloud customers. A CSP, for instance, can ship storage. To reduce financial obligations by the removal of facts that are rarely or never used, or instances of records being withheld in order to preserve popularity. Lastly, even though it may be more cost-effective in the long run, storing data in the cloud no longer guarantees its integrity, and if this issue is not well managed, it may even prohibit fulfilment. Drawbacks of the Current System: Misuse and abuse of the cloud IaaS providers provide their clients the illusion of having infinite networks, computing resources, etc. And garage ability, which is frequently "coupled" with a "seamless" recording method that enables anybody to quickly join up and begin using the cloud with a valid payment card. Certain providers of services also provide free, limited trials. Spammers who exploit these information and use patterns are incredibly anonymous; those who create harmful programs and collaborate with other criminals face the death penalty. behaves comparatively unpunished. PaaS providers have historically taken the brunt of this attack; however, recent data indicates that hackers have initially only been a small number of Iaas. IaaS. The password and key are the fields that make up the future query.

4. PROPOSED SYSTEM

We urge public businesses to examine the security of the cloud-based information storage facility. Compiling and providing our computing, that is, our schema, using a privacy-preserving protocol. helps an outside auditor confirm cloud uploads made without user records by being aware of the developer's resources. Supporting scalability to the caliber of our knowledge is our primary goal. beneficial for the field of public cloud computing. In particular, with our guidance, it offers block auditing, in which many auditing responsibilities are fulfilled by separate individuals Users can be deployed while using TPA simultaneously. We disclose and substantiate the suggested projects' safe overall performance. via certain tests and comparisons with a generation that is at the forefront.

Proposed Objective: The primary intention of this apparatus is to present a dynamically modified protocol; This procedure 1. A cost that indicates how long it will take to verify the accuracy of the information. 2. Tables List dynamic mastery of information. This device has four modules. 1. Several cloud garages 2. Adapted Dynamic Audit 3. Third-Party Auditor and Data Integrity 4. Dynamic Audit.

Proposed Algorithm: The suggested algorithm AES using SHA key To encrypt document metadata, we employ the AES encryption set of principles. Across the key, the

encryption method generates a symmetric key. This key is subjected to SHA-I, which generates a block of records kept in a degree array—a collection of facts. The data encryption technique known as Data Encryption Standard (DES) is antiquated and uses symmetric keys. A Feistel cipher is implemented by DES.

5. METHODOLOGY USED

Initialization Phases: To enable tracking, create a public key that is only used on the blockchain and cannot be altered or erased. Give instructions to the smart contracts to enforce access control and authentication rules as well as permissions throughout the blockchain's ecosystem of the users. Proxy Re-Encryption Integration: Establish a proxy re-encryption function integrated into the blockchain infrastructure that will empower the curious parties to enter into data sharing agreement in a privacy preserving manner. Create a special proxy architecture for the financial sector that has a peculiar component of the cryptographic directions like the access control and high performance. Dynamic Key Generation and Distribution: Formulate a smart process employing keys encryption transmission for knowledge sharing and also exchange possibility to the users, doing dependent on their access level to DKMS and also the data they need to access. Make use of consensus methods based on blockchain. Decentralized Access Control Enforcement: Use smart contracts that have been proved time and again to include the verification and authorization components having fine-grained access permissions which fit any access policy. Source access requests validation using trusted gatekeepers through a consensual mechanism like the evidence of power and the proof of stake. Also, enforce that the access control decisions made are enforced. Auditability and Accountability: The digital footprints and tracking that can be used for audit, as well as logging on the blockchain are ways to follow any changes on the data beside the modification of the financial information. Use the immutable ledger of blockchain for a tamper-proof audit trail of compliance and to satisfy regulatory requirements.

6. SYSTEM ARCHITECTURE

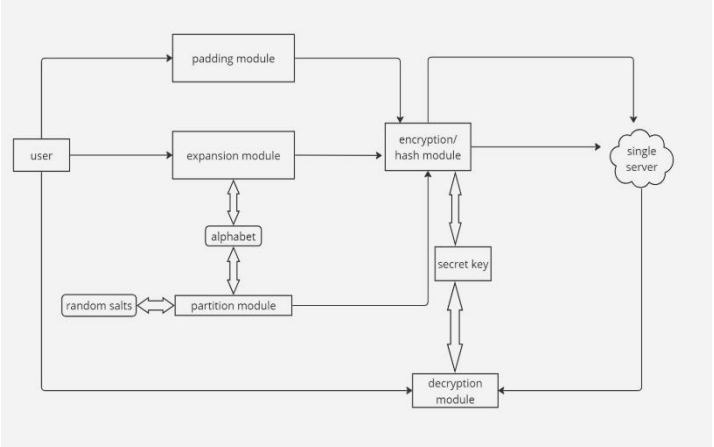
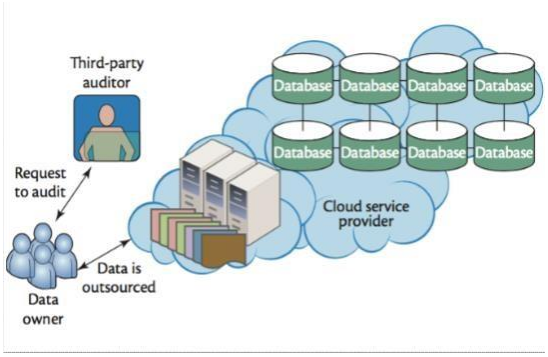


Fig 1 Proposed System Architecture

The fig 1 represents Component's relationship on the whole system will be illustrated with system architecture diagram. In most cases, these are for systems with a combination of hardware and software, where the direction for their interactions is displayed.

Fig 2



Block Diagram

The fig 2 represents proposed structure is platform non-preferential and has its own correct hardware . It is no more done by means of special encryption or storage systems' authorization credentials. While this may not be the most permissible courses of action, Grantly is the most appropriate situation. This task could be assigned to the recipient after they had read the content.

7. MODULES

The following modules are suggested to be included in the system: Block Insertion, Block Deletion, Block Verification, TPA, and User modules.

Admin Module : Admin is the governing force in the data management procedures of the financial data security system using blockchain and proxy re-encryption system. Such an activity includes checking the information saved in the cloud area and relating everything to those that are registered. The administrator part (of the system) acts as the central power that is responsible for making and

maintaining the governance rules on data access for in the system. Administrators can define granular access control policies via a set of networking modules as part of the system..

TPA Module: TPA verify whether the data crafted or not, if yes, then the created information transmit to the user. The TPA module acts as a neutral stakeholder that views the transactions, controls key operations and eventually implements corrective decisions in cases of security flaws such as conflicts and disputes. Within the hierarchy of the key management system (DKMS), the TPA module has a slew of responsibilities that include the generation, distribution, and revocation of key in compliance with data access control policies and regulatory mandates.

User Module: He will be able to create his account Now he has the opportunity to upload the file to the website after providing his user name and password to get in. move the data from the space area to the cloud region. In our financial data security project's user interface module, the blockchain prototype and proxy re-encryption, we would like to make an easily-accessible service, in which the owners of information assets may have the full control of their data and consequently to say who they share their information with and who has the access to this data.

Block Verification Module: A user could easily review to see whether the document has been modified my personal or someone else (e.g. Server United States of America). This module is like a gatekeeper, which is responsive by selecting the permitted stuff to be added or not in the blockchain. Using this framework, the block verification module involves some combination of cryptographic technologies and consensus algorithms to approve transactions and check which of them are valid/ false in the block.

Block Insertion Module: In this insert module simply plug in a newest module. It provides a mechanism for infusing new data records into the chain, in a secure way to be validated at each operation or update. The block spinning module which employs Crypto graphical techniques and consensus mechanisms becomes a cracker jacker in making sure that the data insertion takes place successfully while keeping the decentralization and immutability principles in mind..

Block Deletion Module : During the trash mode, in particular, the user can remove the module out of the block chain system. The Block Deletion Module is an essential component in the ongoing development and improvement of our encryption and data security protocol for the block chain-based system. This module is working dynamically, while assessing the relevance and importance of the blocks being added to the network frequently. By leveraging the best in terms of algorithms along with well-defined specific criteria, it can identify obsolete and redundant blocks which might include spending in outdated encryption keys or access control policies. The module enables the process whereby blocks that serve the purpose of overriding the blocks already saved in the block chain will be deleted to ensure no data is corrupted

8. IMPLEMENTATION

We are basing our solution on a highly detailed architecture that is a result of a uniform application of cryptographic protocols with distributed ledger techniques. This is aimed to enhance the security of the personalized financial transactions. Using pure mathematical functions like elliptic curve cryptography and homomorphic encryption, we meticulous develop a solid encryption scheme that will secure data send and storage via the cloud network. Additionally, the incorporation of proxy re-encryption algorithms plays a vital role in facilitating data availability while ensuring the continuity of the enforceable access control decisions Our plan is to naviagate intricacely the profundities associated with bockchain consensus mechanisms through hybrid of blockchain consensus model. Besides, we inventive develop smart contracts that govern access permissions & keys managing; their enforcement policies are set across the network. The testing approach of our implementation consists of the simulation of the attacks and the usage of the device in the real-world, which serves as a validation process of the efficiency and security of the solution under the whole spectrum of cyber attacks. The system requirements are Hardware and Software Requirements,Database: MySQL,Operating,System:,Windows95/98/2000/XP,Processor Pentium 4 CPU, 80 GB of hard disk space, and 1 GB of RAM

9.RESULT AND DISSCUSION

Fig 3 TPA Login

Above Fig 3 represents that client can login through his registration details in TPA(Third Party Auditor) login. Whenever client forgets his user id and password details client can check the details in their database

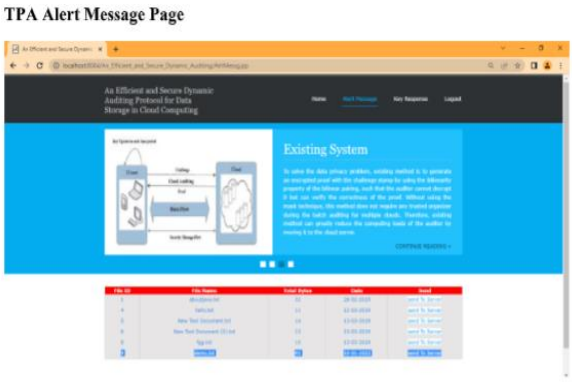


Fig 4 Pass Key Generator

This fig 4 represents , After successful registration client uses to get the pass key to secure their financial data using the pass keys.

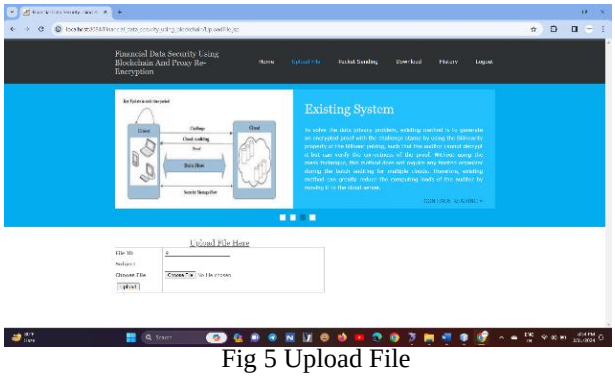


Fig 5 Upload File

This fig 5 represents to upload a client's file which contains sensitive information. Often used to validate the statistics.The intention is to provide remedy to the privateness and safety and declare

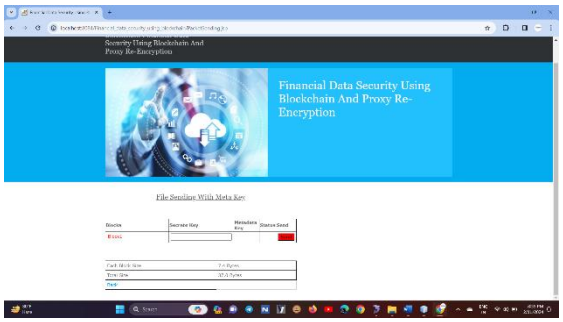


Fig 6 Blocks

Above fig 6 represents group of blocks and going For walks computer apllications on the cloud platform. It could be within the cloud used for fee financial savings.

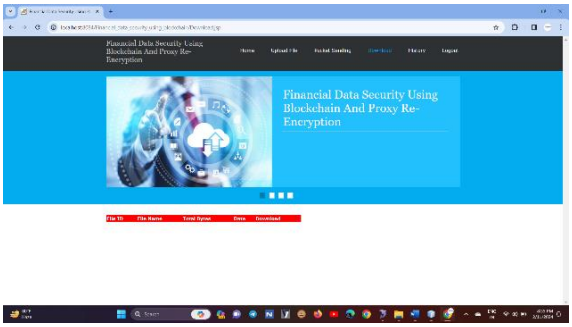


Fig 7 Download File

This fig 7 represents the client can download their's financial data securely.

CONCLUSION

Thus, cloud based data backup for file safety was our mission of which it was our above. There is a tendency that cloud computing is going to play an even more important role and affect everyone in the future. We employ on-the-fly encryption that is hidden through the randomized linear homomorphism Technique in an autonomous process. Through doing so, the server is blinded and the only entity that has knowledge about what the user has stored is the cloud. The server has no visibility. Intermediates cannot intercept the information in transit because it is on a non-human route. The cloud has full sovereignty, and this also If TPA does a couple of examinations at the same time there will be many audits possibly, and, as someone keeps their data outsourced, our privacy will be increasing, and a new audit protocol would be efficient i.e. an audit system for TPA may well be implemented to make multiple audits in one cycle. This thoroughness shows, that our packages have everything needed for you to reach the new level with no harm to your health and improvement in your performance.

REFERENCES

[1] P. K. Tysowski and M. A. Hasan, "Hybrid attribute-and re-encryptionbased key management for secure and scalable mobile applications in clouds," IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172–186, Nov. 2013.

[2] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inform. Sci., vol. 258, pp. 355–370, Feb. 2014.

[3] J. Han, W. Susilo, and Y. Mu, "Identity-based data storage in cloud computing," Future Gener. Comput. Syst., vol. 29, no. 3, pp. 673–681, Mar. 2013.

[4] H.-Y. Lin, J. Kubiatowicz, and W.-G. Tzeng, "A secure fine-grained access control mechanism for networked storage systems," in Proc. IEEE 6th Int. Conf. Softw. Secur. Rel., Jun. 2012, pp. 225–234.

[5] Y. Zhou et al., "Identity-based proxy re-encryption version 2: Making mobile access easy in cloud," Future Gener. Comput. Syst., vol. 62, pp. 128–139, Sep. 2016.

[6] X. A. Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, "Cost-effective secure e-health cloud system using identity based cryptographic techniques," Future Gener. Comput. Syst., vol. 67, pp. 242–254, Feb. 2017.

[7] K. O. B. Obour Agyekum et al., "A secured proxy-based data sharing module in IoT environments using blockchain," Sensors, vol. 19, no. 5, Jan. 2019, Art. no. 1235.

[8] G. Zyskind et al., "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Secur. Privacy Workshops, May 2015, pp. 180–184.

[9] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in Proc. IFIP Int. Conf. Distributed Appl. Interoperable Syst., Springer, Jun. 2017, pp. 206–220.

[10] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," IET Commun., vol. 12, no. 5, pp. 527–532, Mar. 2018.