International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1
Article Received: *25 November 2021* ***Revised:*** *12 December 2021* ***Accepted:*** *10 January 2022*

A Novel Security Mechanism for Cloud based System using Blockchain Technology

Harmandeep Singh

Assistant Professor, Department of computer science & Engineering, Punjabi university,Patiala, India

Abstract:

Different techniques are available to preserve data safety and privacy. Every program's goal should be to obtain confidentially, Integrity, and availability (CIA). The existing centralized cloud services, on the other hand, of CIA qualities. Distributed system archiving should be used in conjunction with blockchain systems to improve data safety and management approaches. It efficiently aids in the protection of data against manipulation and the deletion of a sample of data. A chain of blocks connects that hold data in a blockchain. Every block contains a hash function that would be recorded in the successive stages. After the decryption technique is applied, the information is transformed into an unintelligible form. To recover the original comment, the targeted user must know the secret that was used during the encryption algorithm. As a result, the odds of information alteration were reduced. The SHA-512 Hashing technique should be used in an application. The method exploits were utilized in a variety of applications to data protection was necessary, such as text digests, passcode validation, key exchange, but also blockchains. Information becomes safer and more dependable when various methodologies are combined. Nevertheless, the information's safety could be improved with the use of several techniques. Dueto the major properties of the technique, Advance Encryption Standard (AES) was utilized to encrypt and decrypt the information.

Keywords: Cloud based security system, Blockchain technology, Encryption standard.

Introduction

A blockchain should be essentially a database that is maintained among internet network elements. A blockchain maintains data electronically to compact representation as a data system [1]. Blockchains were highly regarded as preserving a safe and decentralized ledger of events in financial systems. A blockchain's originality would be that it ensures the accuracy of information of a data file while generating confidence to the requirement of a trusted third party [2]. The architecture of the information on a blockchain differs from that of a special database.

The need to obtain information quickly expects critical information of retrieved effectively but also reliably. As a result, decentralized cloud infrastructure [3] should be established. It's also saved in multiple locations to decentralized cloud services that reduce the likelihood of data breaches. Information was achieved to multiple locations, it should be secure in terms of data loss; however, to prevent information from hackers, a decryption technique is needed [4]. Even an individual data document could be kept in different locations using small data pieces, but the little block of knowledge includes vital information [5] Distributed cloud computing was considered safe to centralized cloud services in terms of information security because it should blockchain technology. Although the Blockchain to combat data security issues appears to be an obvious option, its existing constraints of limited throughput, lower bandwidth, and poor stability to the Blockchain approach are impractical [6].

Related Works

Technological improvements through Geospatial Information Systems (GIS) as well as the internet the procedure easier and appropriate to express the fact that hard and time-consuming strategic planning could be a higher degree of reliability [7]. the development of IT indicated the preservation, administration, integration. It would be vital to protect geographic information collected in the corporate network to verify who has control over the data to mitigate errors for data protection, public safety, purposes.

A sequence of blocks connects the information recorded in the blockchain. Every block contains a hash code stored in the following block. As a result, the odds of information alteration are reduced. The SHA-512 Clustering technique should be used for this. The analysis calculation was utilized in a variety of applications where data protection was necessary, including message digest, passcode validation, key exchange, and blockchain. Information becomes safe and trustworthy to various optimization techniques were combined [9]. Nevertheless, the information's safety could be improved with the use of several techniques. Due to the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1
Article Received: *25 November 2021* ***Revised:*** *12 December 2021* ***Accepted:*** *10 January 2022*

major properties of this technique, the Advanced Encryption Standard (AES) should be utilized to encrypt messages.

Proposed System

In UML diagrams, utilization scenario illustrations were a means to represent the proposed solution and needs. It records a live program's dynamic characteristics [10]. A sequence diagrams of two parts: a use scenario and an operator. Here, the data controller and customer to membership and password, that the data controllers would submit a textual content and decrypt the sensor information with asymmetric cryptography.

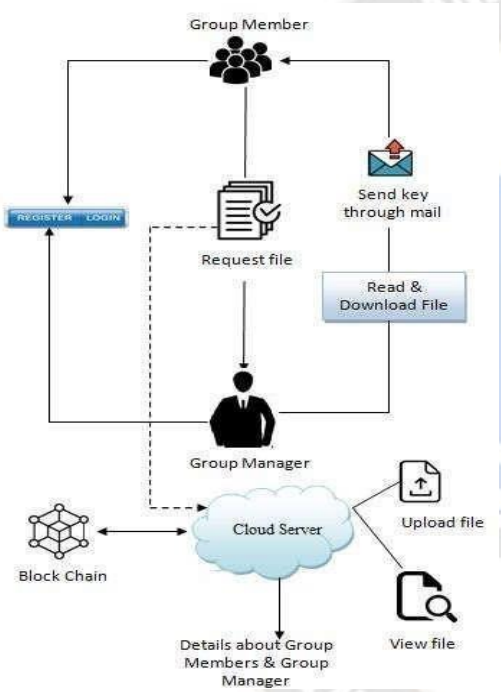


Figure 1 The proposed System

Implementation

We would utilize Eclipse to perform the programming portion of the project. The programming that would be utilized to construct the area component of Cloud Computing was listed. A smart city application owner or a consumer seeking a big volume of data service from an information owner are examples of information consumers. Figure 2 depicts the service scenario of the proposed architecture from the perspective of the information consumer. Figure 2 depicts the proposed architectural functionality as a step-by-step functionality of the service scenario. It explains how to leverage Blockchain technology at the cloud layer to collaborate with cloud service providers, as well as how to consume and store data at the cloud layer.

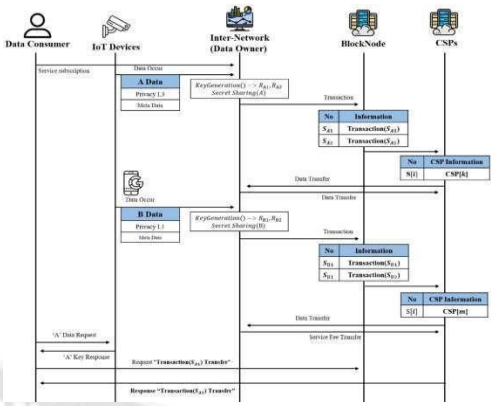


Figure 2: sequence diagram of proposed system

The testbed goal is to analyze the SSA-1 and SSA-2 calculations with the AES-128 encryption innovation that was utilized in the past review. For secret circulation to two CSPs and secret rebuilding using scrambled information from both CSPs, SSA-1 is a proposed effectiveness instrument. To strengthen security confirmation over SSA-1, SSA-2 appropriates data to three CSPs; For reclamation, encoded information with no less than two CSPs is required. A correlation of the non-disseminated free encryption information AES-128, SSA-1, and SSA-2 is displayed in Figure 3.

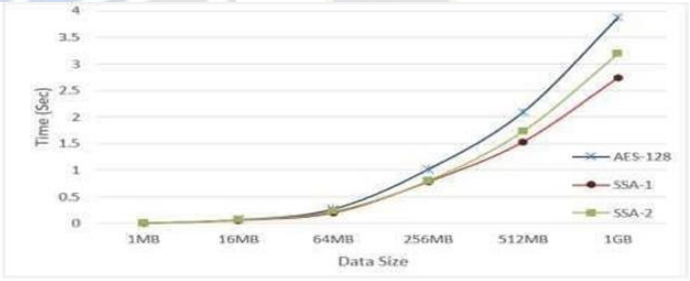


Figure 3: proposed system vs existing system

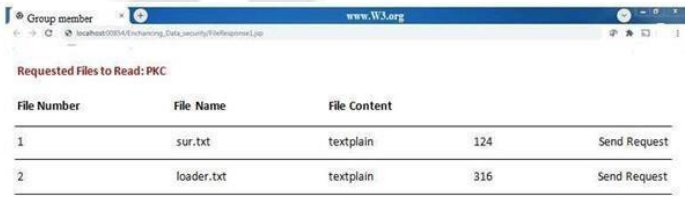
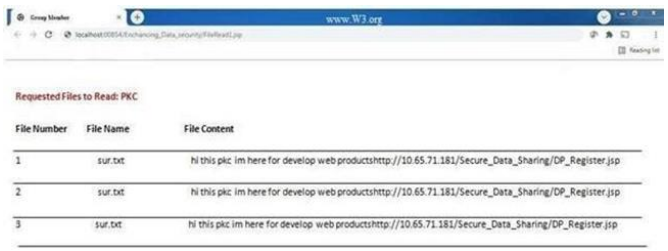


Figure 4: Implementation 1



International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1
Article Received: *25 November 2021* ***Revised:*** *12 December 2021* ***Accepted:*** *10 January 2022*

Figure 5: Implementation 2

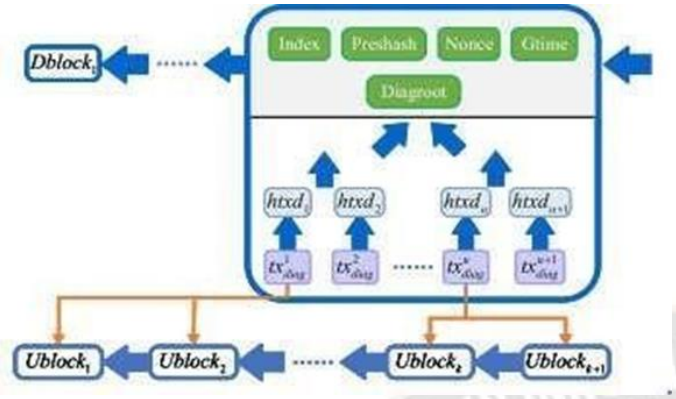


Figure 6: Structure of proposed system

Software Testing

The testing phase begins with the creation of a detailed strategy to evaluate the general functioning and particular specifications of the product across a multitude of system configurations shown in Figure 6. There are strict quality assurance measures in place. The procedure ensures that the product satisfies the technical specifications article's specifications and is bug-free. The following are the objectives that were considered to create the architecture of experimenting.

Operational results suggest that the operations being evaluated were accessible by the business and technical requirements, requirements specification, and customer guides. Quality assurance ensures that the entire integrated software maintenance meets the criteria. It examines a configuration to ensure that the outcomes were recognised and predictable. System evaluation would be a configurations-focused system implementation assessment. In the testing phase, procedure definitions and processes are employed, with an emphasis on predriven procedure links and integration points. Any work could be broken down into smaller components that could then be handled in more depth. Finally, in these units, a validation technique is implemented. Tests performed aids in the identification of potential flaws in independent parts, allowing the element of problems to be discovered as well as corrected.

Conclusion

Humans could conclude to the literature and studies that centralized archiving was a disadvantage. As a result, specialists could leverage decentralized cloud services to improve datasafety. This article suggests a safe and effective method to store data in the cloud. Data protection in a decentralized organization is provided via blockchain cloud computing to encrypt data. The proposed approach was suitable for implementing the blockchain architecture. The techniques utilized to construct the prototype system are efficient, take little work, and provide great protection of data kept on the internet. This technique made the system more secure and resilient to various security assaults carried out through unauthorized users' attempts to destroy and release information of customer data documents to gain.

References

1. Purnama, S., Aini, Q., Rahardja, U., Santoso, N. P. L., & Millah, S. (2021). Design of Educational Learning Management Cloud Process with Blockchain 4.0 based E- Portfolio. Journal of Education Technology, 5(4), 628-635.
2. A. Abdelmaboud et al., "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions," Electronics, vol. 11, no. 4. MDPI AG, p. 630, Feb. 18, 2022. doi: 10.3390/electronics11040630.
3. Liu, S., Dai, Y., Cai, Z., Pan, X., & Li, C. (2021). Construction of double-precision wisdom teaching framework based on blockchain technology in the cloud platform. Ieee Access,9, 11823-11834.
4. K. Hameed, M. Barika, S. Garg, M. B. Amin, and B. Kang, "A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues," Journal of Industrial Information Integration, vol. 26. Elsevier BV, p. 100312, Mar. 2022. doi:10.1016/j.jii.2021.100312.
5. Abunadi, A. Rehman, K. Haseeb, L. Parra, and J. Lloret, "Traffic-Aware Secured Cooperative Framework for IoT-Based Smart Monitoring in Precision Agriculture," Sensors, vol. 22, no. 17. MDPI AG, p. 6676, Sep. 03, 2022. doi: 10.3390/s22176676.
6. T. Chen, L. Zhang, K.-K. R. Choo, R. Zhang, and X. Meng, "Blockchain-Based Key Management Scheme in Fog-Enabled IoT Systems," IEEE Internet of Things Journal, vol. 8, no. 13. Institute of Electrical and Electronics Engineers (IEEE), pp. 10766–10778, Jul. 01, 2021. doi: 10.1109/jiot.2021.3050562.
7. Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 17(2s), 1-17.
8. O. Daramola et al., "Towards AI-Enabled Multimodal Diagnostics and Management of COVID-19 and Comorbidities in Resource-Limited Settings," Informatics, vol. 8, no. 4. MDPI AG, p. 63, Sep. 23, 2021. doi: 10.3390/informatics8040063.
9. R. Gupta, A. Kumari, and S. Tanwar, "Fusion of

blockchain and artificial intelligence for secure drone networking underlying 5G communications," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1. Wiley, Nov. 24, 2020. doi: 10.1002/ett.4176.

10. M. A. Bazel, F. Mohammed, and M. Ahmed, "Blockchain Technology in Healthcare Big Data Management: Benefits, Applications and Challenges," 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA). IEEE, Aug. 10, 2021. doi: 10.1109/esmarta52612.2021.9515747.