IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2024

DOI: 10.17148/IJIREEICE.2024.12802

SPOC: A SECURE AND PRIVACY-PRESERVING OPPOTUNISTIC COMPUTING FRAMEWORK USING BLOCKCHAIN TECHNOLOGY

Sheethal M S[1], K M Sowmyashree[2]

Research Scholar, Dept. of MCA, P.E.S College of Engineering, Mandya, India[1]

Assistant Professor, Dept. of MCA, P.E.S College of Engineering, Mandya, India[2]

Abstract: Secure data sharing in the cloud can be a difficult challenge. There are lots of risks with keeping sensitive info in one place. But hey, blockchain technology seems like a really cool answer! It can make data safer, more reliable, and super clear in cloud systems. In this study, we're suggesting a new way to share data safely in the cloud using blockchain. What's interesting about blockchain is it's decentralized & unchangeable. This means we can create records of data transactions that can't be tampered with. This builds trust and makes everyone accountable. We also use smart contracts to set who can see what, making sure only the right people get access while keeping private and confidential. By mixing blockchain with cloud computing, we create a strong clear setup for sharing data. This helps to reduce the chances of someone accessing the data without permission or messing with it. In experiments, we show that our approach works well for secure and trackable data sharing in cloud environments. Our results point to how blockchain can really boost data security and privacy in these systems. This could lead us toward better, more trustworthy ways to share data.

Keywords: Authentication, data encryption, secure communication, security, Blockchain Technology.

I. INTRODUCTION

Data sharing is super important when it comes to cloud storage. It shows us how to do it safely, quickly, & easily with others. We talk about new public-key cryptosystems that create fixed-size cipher texts, allowing for efficient delegation of decryption rights for any set of cipher texts. The exciting part? You can combine secret keys into one compact key that holds all their power! Fundamentally, if you have the mystery key, you can discharge this minor total key for any choice of cipher content sets put away in the cloud—while keeping other scrambled records from prying eyes.

This little key can be sent out easily or kept on a smart card that doesn't have much space. We also provide a security check of our system using standard models and talk about other nifty applications of our methods. In specific, we present the exceptionally to begin with public-key patient-controlled encryption for adaptable hierarchy—something we didn't have some time recently. Now let's discuss how files are uploaded: by using clever algorithms to encrypt them so that no one person knows how they work! After uploading files, unique keys are created for each file based on those random algorithms. Those keys are special for each file and totally unique. Even when you upload many files at once (let's call it a batch), there will still be unique keys made for each file along with an aggregate key just for that batch! .But remember—the aggregate key is only for that specific batch. The user who uploaded keeps all those keys safe and sound! You can open a file by either its personal key or the aggregate key from its batch. When users want to share files with others, they just send the file and let those people know what keys go with it.

II. RELATED WORK

[1] Naveen Kumar S, M. : In this paper hyper ledger fabric frame work based permissioned block chain network is proposed and established among patents and medical institutes to achieve the secured and reliable sharing of the patient's data. Block chain reliably manage the electronic health records efficiently using Hyper ledger fabric frame work. Implementation results shows that, the hyper ledger fabric based Block chain removes the unreliability in sharing of data among health care centres, doctors, public health departments and hospitals. This network also allows the organizations to quickly and safely move medical data in a legally compliant manner as it is a transparent system. The blockchain implemented has achieved the transparent and secure transfer and also controls the access of health data of patients by user policies with smart contracts as chain code.

DOI: 10.17148/IJIREEICE.2024.12802

[2] Chaitanya Singh, Deepika Chauhan, A. Deshmukh proposed block chain based distributed authentication mechanism process and network architecture. Medi-Block presents a tamperproof and anonymous identity management model for medical record sharing for hospitals and patients, utilizing the concept of bilinear mapping for the authentication phase and eliminating third party trust issues. It implements two-way authentications between patients and the hospital. The effectiveness of the proposed authentication scheme is analysed by BAN logic, storage overhead and computing cost.

[3] Shi Wang, Jing Liu :This paper studies a data sharing scheme based on blockchain, and proposes a model that combines the Ethereum blockchain and federated learning ideas, and uses off-chain storage methods to share data. In this model, users can upload data description information to the blockchain through smart contracts, and can retrieve the required data through keywords, and then send the data identification and data processing model to the data owner in the form of transactions. The data owner can use this model to process the data, and finally return the result to the data requester..

[4] : Ye Tao, Peng Xu :Existing secure CECS schemes are secure only if all edge servers are trusted. In other words, if any edge server is compromised, all cloud data (generated by IoT devices) will be leaked. Additionally, it is costly to request expected data from the cloud, which is linear with respect to the number of edge servers. To address the above problems, we propose a new secure data search and sharing scheme for CECS. Our scheme improves the existing secure CECS scheme in the following two ways. First, it enables users to generate a public-and-private key pair and manage private keys by themselves. In contrast, the existing solution requires edge servers to manage users' private keys. Second, it uses searchable public-key encryption to achieve more secure, efficient, and flexible data searching. In terms of security, our scheme ensures the confidentiality of cloud data and secure data sharing and searching and avoids a single point of breakthrough.

[5] Altaf Khan, Alexander G. :_This paper presents a model of the Graphical password scheme under the impact of security and ease of use for user authentication. We combine the idea of recognition with recall and cu-recall methods to enhanced security in comparison to current systems.

III. METHODOLOGY

Existing System

When it comes to data sequestration, a common system is counting on the garçon to apply access controls after a person has logged in. This means that if someone suddenly gets further boons, all the data could be exposed. effects get trickier in a participated- residency pall computing terrain. Now, about train vacuity – there are several cryptographic styles out there. These allow a third- party adjudicator to check if lines are available for the data proprietor without oohing any word about the factual data or compromising that proprietor's obscurity. But let's be real, pall druggies might not completely trust the pall garçon to keep their stuff nonpublic. Whenever druggies are not super confident about trusting the security of the virtual machine or the honesty of the tech staff, they tend to lean towards a robust cryptographic result with proven security grounded on number-theoretic hypotheticals.

DISADVANTAGES OF EXISTING SYSTEM

- Costs & complications go up as the number of decryption keys increase.
- In public key encryption, the encryption key & decryption key are different.

Proposed System

The proposed system highlights how to make a decryption crucial much more important. It allows decryption of multiple ciphertexts without making it bigger. The main idea is "To produce an effective public- crucial encryption scheme that supports flexible delegation. " This is a group of ciphertexts can be deciphered using a constant- size crucial created by the proprietor of the master-secret key. To attack this, we are introducing a special kind of public- crucial encryption called crucial- aggregate cryptosystem (DATA SHARING).

In DATA SHARING, dispatches are translated not just under one public- key but also under commodity called a class identifier. So principally, ciphertexts get sorted into different classes. The crucial proper known as a master-secret key. They can use this key to pull out secret keys for colorful classes. More yet, these up rooted keys can be an aggregate key. This total key is compact like a riddle key for one course but holds the control of multitudinous keys. This means it can decipher any subset of ciphertext classes.

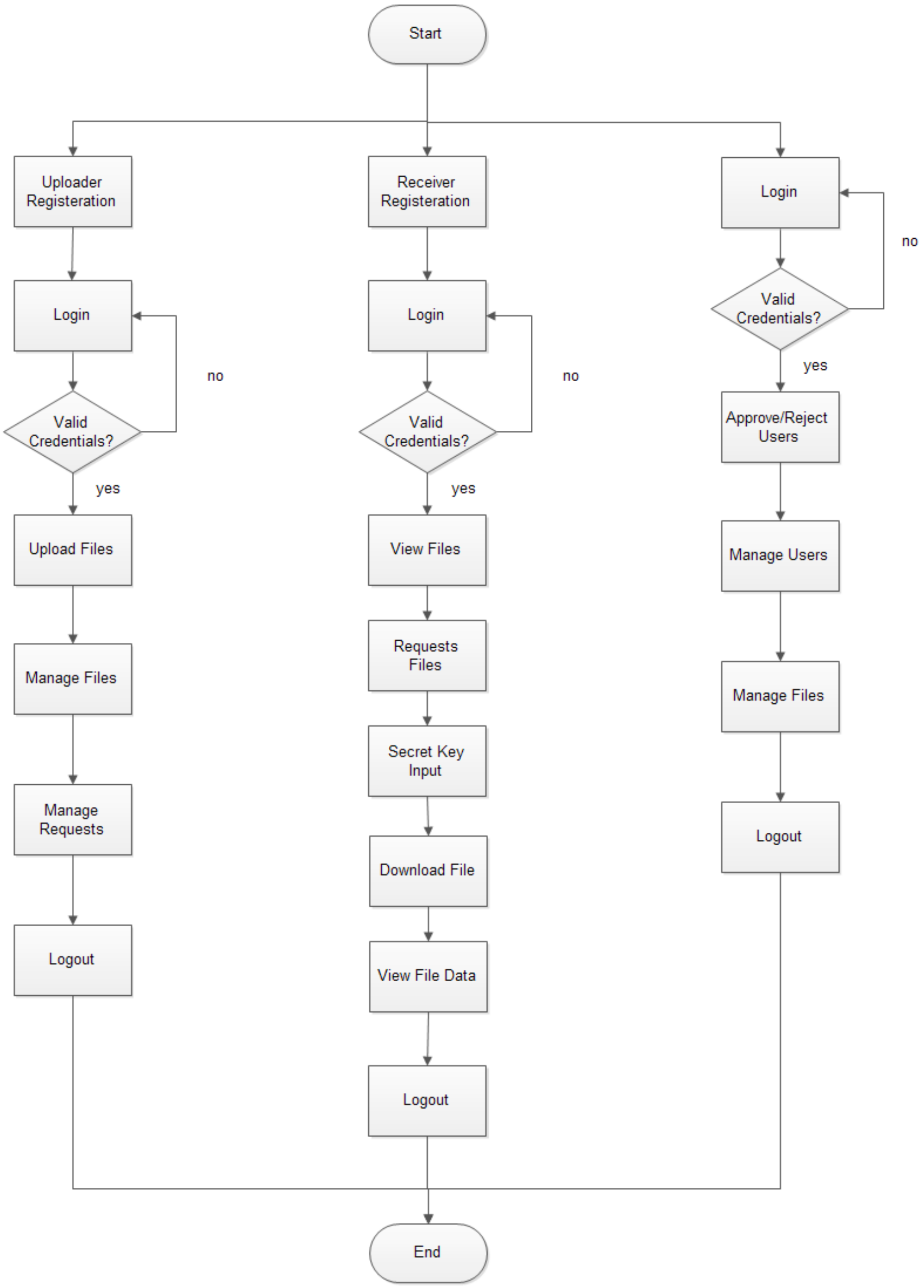
DOI: 10.17148/IJIREEICE.2024.12802

ADVANTAGES OF PROPOSED SYSTEM

- The uprooted key can be an aggregate key that is as compact as a regular secret key.
- You can efficiently delegate decryption with this aggregate key

IMPLEMENTAION

Implementation is the process of transforming a new or updated system design into a fully operational system. The primary goal is to deploy the new system while minimizing costs, risks, and disruptions to ongoing operations. This phase is crucial for ensuring that the system operates smoothly and effectively, without interrupting the organization's workflow. A key aspect of the implementation process is conducting thorough testing to avoid any issues. This involves creating test cases and using sample data to validate that the new system performs as expected. Before transitioning to live data, it is essential to test the system with data from the old system, ensuring that all functions work correctly in the new environment.



FLOW OF IMPLEMENTATION

DOI: 10.17148/IJIREEICE.2024.12802

IV. CONCLUSION

How to secure users' information security is a central address of cloud capacity. With more numerical apparatuses, cryptographic plans are getting more flexible and regularly include different keys for a single application. It consider how to "compress" mystery keys in public-key cryptosystems which back assignment of mystery keys for diverse ciphertext classes in cloud capacity. No matter which one among the control set of classes, the delegate can continuously get an total key of consistent estimate. It is more adaptable than various leveled key task which can as it were spare spaces if all key-holders share a comparable set of benefits. A impediment in a work is the predefined bound of the number of greatest ciphertext classes. In cloud capacity, the number of ciphertexts more often than not develops

quickly. So have to save sufficient ciphertext classes for the future expansion. In spite of the fact that the parameter can be downloaded with ciphertexts, it would be way better if its estimate is free of the greatest number of ciphertext classes. It is more versatile than dynamic key errand which can as it were save spaces if all key-holders share a comparative set of benefits. A control in a work is the predefined bound of the number of most prominent ciphertext classes.

REFERENCES

[1] Hanshu Hong and Zhixin Sun, "Towards secure data sharing in cloud computing using attribute based proxy re-encryption with keyword search," 2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), 2018,

[2] A. Michalas, "Sharing in the rain: Secure and efficient data sharing for the Cloud," 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2019.

[3] J. Zhang and Z. Zhang, "Secure and Efficient Data-Sharing in Clouds," 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, 2019.

[4] A. Razaque et al., "Secure data sharing in multi-clouds," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2018.

[5] S. Nalajala, K. Akhil, V. Sai, D. C. Shekhar and P. Tumuluru, "Light Weight Secure Data Sharing Scheme for Mobile Cloud Computing," 2019 Third International conference on ISMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019.

[6] Y. Tao, P. Xu and H. Jin, "Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage," in IEEE Access, vol. 8, pp. 15963-15972, 2020 .

[7] X. Qiu and S. Ji, "Research On Mine Data Sharing Scheme Based On Blockchain," 2020 International Conference on Computer Engineering and Application (ICCEA), 2020.

[8] N. Kumar S. and M. Dakshayini, "Secure Sharing of Health Data Using Hyperledger Fabric Based on Blockchain Technology," 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), 2020.

[9] S. Wang and J. Liu, "Blockchain based Secure Data Sharing Model," 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 2021 .

[10] Chaitanya Singh, Deepika Chauhan , Sushama A. Deshmukh, Medi-Block record: Secure data sharing using block chain technology, 2021.

[11] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," Proc. Information Security and Cryptology (Inscrypt '07), vol. 4990, pp. 384-398, 2017.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2016.

[13] S.G. Akl and P.D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Trans. Computer Systems, vol. 1, no. 3, pp. 239-248, 2019.

[14] G.C. Chick and S.E. Tavares, "Flexible Access Control with Master Keys," Proc. Advances in Cryptology (CRYPTO '89), vol. 435, pp. 316-322, 2019.

[15] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Trans. Knowledge and Data Eng., vol. 14, no. 1, pp. 182-188, Jan./Feb. 2022.

[16] Y. Sun and K.J.R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," Proc. IEEE INFOCOM '04, 2024.