International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 11 | Nov 2022 www.irjet.net p-ISSN: 2395-0072

An interactive Study on secure data sharing in the IOT through Blockchain

Shinde Tanmay Balkrushna[1], Thorat Swastik Jaysing[2], Dahatonde Mangesh Ramesh[3], Prof. A. S. Dumbre[4]

[1, 2, 3] Student, Department of Computer Engineering, Jaihind College of Engineering, Pune, Maharashtra, India
[4]Guide, Department of Computer Engineering, Jaihind College of Engineering, Pune, Maharashtra, India

---

Abstract - *At the same time as the information age is growing exponentially, the amount of data produced by users is growing at an equally rapid pace. It is obvious that the storage space on the desktop device is insufficient. Cloud services are becoming more popular as a means for users to archive, analyze, and administer their data. Peoples' lives are improved in several ways by cloud - based solutions, yet these alternatives also pose significant threats to consumers' confidentiality. As soon as data is uploaded to a cloud server through the internet, the data's owner has no further say over the content and therefore must depend on the server to perform any required computations or processing. As a consequence, cloud data protection has taken on new challenges, such as figuring out how to effectively ensure user privacy and fine-grained access control as well as authorization control. Our approach, which will be detailed in more depth in the subsequent volume of this study, has relied heavily on the findings of these studies. The proposed approach for proxy re-encryption secures the Internet of Medical Things data on a public cloud through the use of Blockchain distributed framework. This approach will be further elaborated in the upcoming editions of this research.*

Key Words: Internet of Medical Things, Public Cloud, Medical Health Records, Cryptography, Search over encrypted data.

1. INTRODUCTION

Users' information provided is expanding at an exponential rate along with the expansion of the age of information. It's clear that the user's computer's storage device isn't enough. Users are increasingly turning to cloud services for data storage, processing, and management. Although cloud solutions improve users' lives in many different ways, there are also serious risks to their privacy and security. Once data is sent to the cloud across a network, the data holder loses control on the information and must rely on the cloud server to do any necessary calculations or processing. As a result, new difficulties have emerged in cloud data security, such as how to guarantee the confidentiality of information and the efficacy of user fine - grained access control and permission management.

In contrast, the majority of the currently available cloud storage solutions are centralized, with data management handled by a single authority. Both the transmission and calculation costs associated with this method are substantial. Therefore, it is important to provide a user-friendly, secure, and effective cloud storage sharing solution. Cloud ciphertext authorization technique is presented as a solution to the issue of data privacy protection. The privacy is maintained by encrypting the information key as well as maintaining the encrypted message in the cloud. Additionally, the data owner controls the user's key and hence the access privileges.

Conventional research proposes a participation encryption methodology that takes the role into account as a decryption criterion. It was suggested to use attribute encryption as the basis for a composite cloud re-encryption information sharing framework. This strategy not only facilitates versatile ciphertext identity management but then also simplifies management for data owners. An adaptive and intelligent proxy re-encryption technique is devised. Using this method, the data owner may provide access to the plaintext message by authorizing the designated user to decode any re encrypted ciphertext using the user's component. Individuality, certifications, and environments were subsequently suggested as important components in a proxy re-encryption system.

Confidential information is adequately ensured by the aforementioned methods; yet, users are hampered in their ability to swiftly locate the data and information they want throughout the data exchange operation. A characteristic proxy re-encryption system using cryptographically searchable terms is proposed to enhance access efficiency during information sharing. However, a practical ciphertext decryption technique cannot be designed using this method. The traditional research solves this through a key-based attribute proxy re-encryption technique to facilitate keyword retrieval, and demonstrated the system's viability inside a randomly generated oracle model.

Unfortunately, the scheme's computational complexity cost makes it impractical for widespread practical application, according to performance studies. The majority of the following methods also include outsourcing the administration of user data to remote cloud storage facilities. In the event of an assault on the administrators of

third-party cloud services, sensitive customer data may be compromised or perhaps even deleted forever.

The development of Blockchain technologies has resulted in a decentralized, non-tamper able, unforgeable, and communally administered system of administration. What we possess with Blockchain is simply a distributed database. Also, Bitcoin's core technology is a series of cryptographically created data blocks. Bitcoin blockchain transactions are grouped together in blocks. Data needed to ensure the integrity of the previous block's data and create the following one. To begin, decentralization is a key feature of the blockchain. Distributed ledger technology operates independently of centralized authorities and physical servers. Due to decentralized ledgers and databases, the Blockchain operates autonomously. Data self-verification, transmission, and administration are all implemented by networks. The Blockchain's primary value and main attraction is its decentralized nature. On top of all that, the Blockchain is decentralized, accessible, private, and confidential.

Jingwei Liu [1] proposes a consortia blockchain-based system for exchanging medical records that protects patient confidentiality. To safeguard patients' confidentiality, we offer a conditionally anonymous tracking technique that may identify bad actors when unlawful activity is detected. When dealing with enormous amounts of health information, the on chain off-chain warehouse architecture may significantly decrease blockchain's memory load. Aside from that, the enhanced proxy re-encryption strategy may withstand a collaboration assault that involves a third-party cloud as well as the authorized data requester. This means that the plan is more secure and faster than similar projects. It is the authors' intention to employ smart contracts as the basis for a tool to track down rogue users.

[2] Xiaoyu Zhang proposes two asynchronously deep learning techniques that are secure and don't interfere with users' confidentiality. Together, several users may train the same model in concurrently and asynchronously whilst maintaining the secrecy of their input data and the information contained within it. Depending on proxy re-encryption, DeepPAR allows for guidelines outlined secrecy to be maintained while still protecting the privacy of individual participants' inputs. In addition, DeepDPA's lightweight dynamic participation notification is only affected by its immediate two neighbors thanks to the group key administration system on which it is built. Furthermore, DeepDPA provides retroactive anonymity in adaptive privacy-preserving machine learning.

This literature review paper divides section 2 into an assessment of prior work in the form of a review of literature, and section 3 concludes with recommendations for future research.

2. RELATED WORKS

In order to offer effective and private security controls for media distribution in V-NDN, Shunrong Jiang [3] reveals the security problems when deploying NDN to VANETs and proposes appropriate solutions (ESAC). To begin, researchers construct a proxy re-encryption method that works in the absence of a trustworthy source to provide identity management, revocation, and updating. Researchers use pseudonyms and an identifier-based signature to solve the problem of anonymous authentication and validity checking. To assure NDN's usefulness in VANETs, researchers provide an incentive technique using a hashed certificate. According to the results of the security study, ESAC is capable of providing the necessary level of security for use in V-NDN. The simulated outcomes further demonstrate that the suggested secure strategy has a negligible impact on the efficiency of the network.

To ensure the immutability, auditability, trustworthiness, and security of log events pertaining to access/permissions, Ammar Ayman Battah [4] presented a completely decentralized blockchain-based multi-party authorization (MPA) system. Proxy re-encryption with multiple oracles was suggested to provide accessibility to protected shared data on a community and decentralized storage network like IPFS. The researchers designed the suggested smart contracts with reputational algorithms that assign oracles scores based on their record of malevolent and benign actions. To construct the procedures, variables, and trigger events, the researchers used smart contracts on the Ethereum platform. The smart contract implementation is published on GitHub and is flexible enough to be used with little adjustments for use on either permissionless or anonymous public blockchains, depending on the requirements of certain sectors. The researchers detailed the development, evaluation, and verification of the suggested algorithms as well as the elements of the system.

In order to overcome the drawback of conventional intelligent transportation's centralized data administration and to focus on ensuring the anonymity and safety in the data engagement process, Di Wang [5] proposed a unique strategy of secure information posting and customized service providers for transportation engineering predicated on the consortium blockchain. By splitting the key through into attribute key and also the search key, the suggested policy attribute - based proxy re-encryption method enables both word search as well as proxy re-encryption, as well as safe data exchange and the prevention of OBU privacy information leaks. Afterwards when, the smart contract may be used by the hospitality industry to give accurate and personalized services like insurance premiums and auto repairs. This approach provides clear benefits in terms of confidentiality, computing cost, communication cost, and latency, as shown by the security study and performance assessment.

In order to safely store and transmit PHRs to the appropriate parties in the cloud, Mazhar Ali [6] devised an approach. This approach ensures that protected health information (PHI) is kept private and secure by enforcing granular, patient-centric controls over who has access to what parts of PHI. By implementing a fine-grained accessibility control technique, the authors ensure that none of the legitimate network operators may see protected health information (PHI) that they have been not permitted to view. Owners of protected health records (PHRs) secure their data and keep it on the cloud; only those with appropriate re-encryption keys supplied by such a semi-trusted proxy may access the PHRs. Users' private and public keys pairs inside the system will be generated and stored by the semi-trusted proxy. By contrast to safeguarding patient privacy and ensuring PHRs are managed in a patient-centric manner, the approach also manages both forward backwards access controls for individuals who are leaving and entering the system.

Utilizing proxy re-encryption technologies and Blockchains, Yanfang Lei [7] creates a system for updating authorization to retrieve data in the cloud, with capability for search retrieval. At the outset, the reader is provided with some introductory material to the situation. Second, the system architecture and methodology of the approach are outlined in great depth. The scheme's accuracy and security are next analyzed. The scheme's effectiveness is then analyzed, and the algorithm's efficacy is tested using numerical trials. One positive aspect of this technique is that it uses ciphertext segregation and preservation to significantly lower the possibility of informational cooperation. However, if the major parameters of the proxy re-encryption are really only modified whenever the access permissions are modified, then the objective of a deterministic authorization upgrade is best served.

The Web 3.0 structure was created by Koushik Bhargav Muthe [8]. Humans, as a species, have the potential to unite as one, linked organism, powered by a decentralized Internet. This study analyzed the existing state of the web and recommended a mechanism for its full decentralization. The suggested Decentranet protocol must be employed for experimental purposes since it is still in the proof-of-concept phase. The limitations of the present Network infrastructure make scalability a manufacturing problem. Motivating the intermediaries to take an interest in the network is an important step in expanding the system's design. Ethereum 1.0, the foundation of the present protocol is focused, has a Proof of Work-based agreement method, which isn't optimal for truly decentralized systems.

To ensure that third party candidates (first responders) may have immediate or subsequent accessibility to movies captured by drones without jeopardizing the confidentiality of the material, Khaled Rabieh [9] presented a privacy-preserving yet effective sharing method. Users' privacy is protected when watching these films since they are encrypted and stored in the cloud. For reasons of data security, emergency rescuers are never given a copy of the initial private key being used encode drone footage. Alternatively, a proxy re-encryption is used to facilitate re-encryption through the CC upon that cloud server. To initiate the re-encryption procedure, a new key is produced and uploaded to the cloud. Authors used ns-3 simulator as well as OpenCV framework to create working model.

Conditional identity-based broadcasting proxy re-encryption was described by Chunpeng Ge [10], a practical implementation was presented under this specification, and it was shown that our method is CPA reliable in the randomized oracle scenario. Comparing properties and effectiveness also shows that their suggested approach is economical and usable in the real world. In addition, the RIB-BPRE method can elegantly handle key revocation for a data-sensitive platform in a cloud - based environment, such as a volunteer-based genomic research process. Although this research has addressed the issue of revoked keys for data sharing, it has also inspired some intriguing open issues, such as building a RIB-BPRE strategy requiring random oracles and figuring out ways to enable more expressiveness on identification.

To get a (single-hop directional) semantic proxy key re-encapsulation technique out of a linear predicate key abstraction strategy, Yi-Fan Tseng [11] presents a unique general construction. It is possible to achieve a (single-hop unidirectional) conditional proxy re-encryption process by integrating with a trustworthy symmetric key encryption. As a consequence, the result offers a novel approach to building a semantic proxy re-encryption that works with any predicate functions, addressing the issue that the existing predicate proxy re-encryption exclusively works with the kernel function predicate feature.

In the context of substantial data, Kun Wang [12] implements multi-sharing, anonymous, and CCA-secure transmission of data. In addition, researchers suggest a novel concept termed pre for usage in the proxy re-encryption scheme that might guarantee that only individuals for whom the credentials have been confirmed are authorized to get the information and provide effective security for the private variables. User demands are considerably reduced by the pre-authentication feature. Researchers also show that the pre-authentication procedure improves the system's integrity by keeping users' information, credentials, and other properties safe. Authors believe their idea of pre-authentication will be the first of its kind in this context.

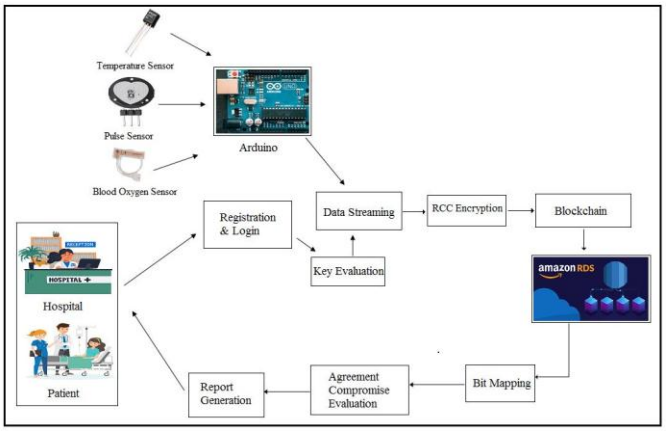

Fig. System Overview Diagram

3. CONCLUSION

Proxy re-encryption may prohibit a proxy that cannot be entirely authorized from gaining any insight into the actual plaintext whilst re-encrypting a ciphertext. Proxy re-encryption has seen widespread application due to the flexibility it affords. Unsurprisingly, the computational complexity overhead renders it impossible for extensive operational implementation, as per performance benchmarks. The bulk of the following strategies also require delegating the management of user information to remote cloud infrastructures. In the case of an attack on the operators of third-party cloud storage, critical client data may be jeopardized or possibly even wiped permanently. Diverse academics came up with numerous approaches to deal with the security breaches that spring up in various application contexts, and they have all been properly assessed to help us arrive at our strategy. Protecting IoMT data in the cloud using a distributed ledger like Blockchain is the goal of the suggested proxy re-encryption method. In subsequent iterations of this study, this method will be developed in more depth.

REFERENCES

[1] J. Liu, T. Liang, R. Sun, X. Du and M. Guizani, "A Privacy-Preserving Medical Data Sharing Scheme Based on Consortium Blockchain," GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 2020, pp. 1-6, doi: 10.1109/GLOBECOM42002.2020.9348251.

[2] X. Zhang, X. Chen, J. K. Liu and Y. Xiang, "DeepPAR and DeepDPA: Privacy Preserving and Asynchronous Deep Learning for Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2081-2090, March 2020, doi: 10.1109/TII.2019.2941244.

[3] S. Jiang, J. Liu, L. Wang, Y. Zhou and Y. Fang, "ESAC: An Efficient and Secure Access Control Scheme in Vehicular Named Data Networking," in IEEE Transactions on Vehicular Technology, vol. 69, no. 9, pp. 10252-10263, Sept. 2020, doi: 10.1109/TVT.2020.3004459.

[4] A. A. Battah, M. M. Madine, H. Alzaabi, I. Yaqoob, K. Salah and R. Jayaraman, "Blockchain-Based Multi-Party Authorization for Accessing IPFS Encrypted Data," in IEEE Access, vol. 8, pp. 196813-196825, 2020, doi: 10.1109/ACCESS.2020.3034260.

[5] D. Wang and X. Zhang, "Secure Data Sharing and Customized Services for Intelligent Transportation Based on a Consortium Blockchain," in IEEE Access, vol. 8, pp. 56045-56059, 2020, doi: 10.1109/ACCESS.2020.2981945.

[6] M. Ali, A. Abbas, M. U. S. Khan and S. U. Khan, "SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud," in IEEE Transactions on Cloud Computing, vol. 9, no. 1, pp. 347-359, 1 Jan.-March 2021, doi: 10.1109/TCC.2018.2854790.

[7] Y. Lei, Z. Jia, Y. Yang, Y. Cheng and J. Fu, "A Cloud Data Access Authorization Update Scheme Based on Blockchain," 2020 3rd International Conference on Smart BlockChain (SmartBlock), 2020, pp. 33-38, doi: 10.1109/SmartBlock52591.2020.00014.

[8] K. B. Muthe, T. S. T. Vemuru, K. Sharma and N. S. Mohammad, "Decentranet - An Ethereum, Proxy Re-Encryption and IPFS Based Decentralized Internet," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp. 1-5, doi: 10.1109/ICCCNT49239.2020.9225483.

[9] K. Rabieh, S. Mercan, K. Akkaya, V. Baboolal and R. S. Aygun, "Privacy-Preserving and Efficient Sharing of Drone Videos in Public Safety Scenarios using Proxy Re-encryption," 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), 2020, pp. 45-52, doi: 10.1109/IRI49571.2020.00015.

[10] C. Ge, Z. Liu, J. Xia and L. Fang, "Revocable Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 3, pp. 1214-1226, 1 May-June 2021, doi: 10.1109/TDSC.2019.2899300.

[11] Y. -F. Tseng, Z. -Y. Liu and R. Tso, "A Generic Construction of Predicate Proxy Key Re-encapsulation Mechanism," 2020 15th Asia Joint Conference on Information Security (AsiaJCIS), 2020, pp. 1-8, doi: 10.1109/AsiaJCIS50894.2020.00013.

[12] K. Wang, J. Yu, X. Liu and S. Guo, "A Pre-Authentication Approach to Proxy Re-Encryption in Big Data Context," in IEEE Transactions on Big Data, vol. 7, no. 4, pp. 657-667, 1 Oct. 2021, doi: 10.1109/TBDATA.2017.2702176.