An Approach to Secure Data Sharing in the Internet of Things Using Blockchain- Based Proxy Re-Encryption

Keshav Kumar Choudhary[1], Shreedhara N Hegde[1], C. PuiLin[2*]

[1]Dayananda Sagar Academy of Technology and Management Bangalore, Karnataka, India
[2]Faculty of Data Science & IT, INTI International University, 71800 Nilai, Malaysia

Email: choudhary1290qwnm@gmail.com, *puilin.chong@newinti.edu.my

Abstract

The prevalence of data sharing has increased with the rise in popularity of cloud computing and the Internet of Things (IoT). However, ensuring data security is difficult because of the possible negative consequences of illegal data usage. This study presents a method for ensuring the secure transmission of data in cloud environments: proxy re-encryption. The identity-based encryption method enables data owners to transfer encrypted data to the cloud. Subsequently, a proxy re-encryption framework enables authorized individuals to access the data. To surpass the limitations of IoT device resources, we utilize an edge device as a proxy server to transfer computationally intensive tasks to a separate device. By utilizing the advantages of information-centric networking, we can optimize network capacity and enhance service quality by efficiently distributing cached content across the proxy. This method decreases bottlenecks in centralized systems while providing precise control over data access. The proposed work demonstrates the effectiveness of the strategy in ensuring data security, confidentiality, and integrity through thorough security research and plan review.

Keywords

Internet of things, Blockchain, Security, Data access control, Proxy Re-Encryption

INTRODUCTION

As a result of the proliferation of cloud computing and the Internet of Things (IoT), the practice of sharing data has grown more widespread. It is becoming increasingly difficult to guarantee the safety of data because of the potential negative outcomes that could result from inappropriate data utilization. For the purpose of ensuring the safety of data transmission in cloud environments, the team devised a method that makes use of proxy re-encryption while working on this project. Through the utilization of identity-based encryption, the implementation of this technique enables data owners to safely transmit encrypted data to the cloud. After that, persons who are utilizing a proxy re-encryption architecture, as well as individuals who have the appropriate authorization, are able to retrieve the data.

The use of edge device as a proxy server to reduce the strain of computationally demanding operations. This is done to address the restricted resources that Internet of Things devices have. Through the utilization of information-centric networking capabilities, it is able to effectively distribute cached content across the proxy, hence improving the quality of service and optimizing the capacity of the network. This method makes it possible to exercise exact control over the access to data while also minimizing the impact of bottlenecks in centralized

Submission: 4 May 2024; **Acceptance:** 29 July 2024

systems. The method demonstrated is effective in maintaining the integrity, confidentiality, and security of data by completing extensive study on security and analyzing our methodology.

LITERATURE SURVEY

There has been a significant rise in the amount of academic attention that has been focused on the intersection of blockchain technology, proxy re-encryption (PRE), and the Internet of Things (IoT) in recent years. This interest has been aimed towards the junction of these three technologies. In Internet of Things situations, the need for data sharing that is both secure and efficient has been the driving force for recent interest. On the Internet of Things (IoT), various research has studied the idea of merging blockchain technology with PRE in order to increase data security and privacy. Authors X. Huang and others [X. Huang et al, 2021] present on the Internet of Things (IoT).

An approach that is worthy of mention is the utilisation of blockchain technology as a decentralised platform for the purpose of managing access control and maintaining the integrity of data that is exchanged. According to the findings of research carried out by Y. Liu and colleagues [Y. Liu et al., 2021], PRE makes it possible to safely delegate decryption rights to individuals who are permitted to receive them.

Blockchain technology, on the other hand, provides access logs with features such as transparency and immutability. In addition, academics have investigated the possibility of utilising blockchain-based PRE in conjunction with edge computing in order to address the resource limitations that are associated with devices that are connected to the Internet of Things. By offloading operations that demand a substantial amount of processing power to edge devices, it is possible to boost the efficiency and scalability of data sharing, as indicated by Zhou [J. Zhou et al., 2022]. This is something that may be done to improve the efficiency of data sharing. In addition, Information-Centric Networking (ICN) has been utilised to optimise content caching and delivery in Internet of Things (IoT) networks. This has resulted in an additional improvement in the effectiveness of data interchange, as demonstrated by T. Li and other individuals [T. Li et al., 2023]. Research that has been conducted more recently has focused on enhancing the security and confidentiality of blockchain-based PRE systems for the Internet of Things (IoT). The implementation of methods such as identity-based encryption (IBE) and attribute-based encryption (ABE) has enabled the provision of fine-grained access control as well as the safeguarding of sensitive data. Both objectives have been successfully realised.

It is written that "L. Yuan and others" [L. Yuan et al., 2023; I. Keshta et al., 2019; W. Wang et al., 2023] In addition, the utilisation of homomorphic encryption has been taken into consideration in order to enable secure calculations on encrypted data without jeopardising the security of the material concerned. , R. Zhang, and a few others [R. Zhang et.al., 2023; H. Zhao et al., 2018; K. O.-B. O. Agyekum, et al., 2022] There are still a few challenges to be conquered before blockchain-based PRE can be utilised in the Internet of Things, despite the optimistic improvements that have already taken place. There are three of the most significant issues that need to be addressed to guarantee the effective implementation of the solution. These aspects include scalability, interoperability, and energy efficiency.

METHODOLOGIES

A. Agile Methodology

With the agile methodology, projects are broken down into smaller, more manageable chunks that are referred to as "sprints." This is a way of project management that is known as the agile methodology. To achieve continuous advancement at each and every level, it is vital for all of the numerous actors to maintain constant communication with one another and work together. As soon as they start working, teams immediately begin a process that includes planning, carrying out, and evaluating the work that they have done. This process begins immediately. Now that the teams have started working, this process will get underway. To guarantee that the project will be successful, it is essential to keep the lines of communication open between the members of the team and the people who have a personal interest in participating in the project. The phrase "agile project management" is used to describe a methodology that is utilized in the field of project administration. This methodology places an emphasis on collaborative efforts and incremental progress.

The core concept underlying the agile project management methodology is that it is possible to achieve gradual and ongoing enhancements to a project by applying essential modifications as they arise. This is the fundamental principle of the strategy. This principle is the basis of the agile software development methodology. Agile project management is gaining popularity and is now one of the most often used approaches to project management. The success of agile project management may be largely attributed to its adaptability, strong client involvement, and willingness to change, which are the defining qualities of this technique. What are the specific ways in which the Scrum methodology differs from previous methodologies?

Heuristic approaches prioritize the acquisition of knowledge from past experiences and adjusting behaviour in accordance with evolving situations. Scrum is an exemplification of a heuristic framework that was formulated via practical knowledge and systematic trial and error. The team acknowledges that they will not possess complete knowledge at the beginning of a project and anticipates acquiring new information as they go towards completing the work at hand. The objective of Scrum is to facilitate teams in adapting their processes to meet evolving requirements and a diverse range of expectations.

The significance and importance of three fundamental components of a scrum team will always remain constant, demanding our unwavering attention and effort.

(i) The Product Backlog, which is the most important list of tasks that need to be completed, is managed by either the product owner or the product manager, depending on who oversees the product. This ever-evolving collection of features, requirements, upgrades, and bug fixes is what serves as the source of information for the sprint backlog. When reduced to its most basic form, the "To Do" list of a team is nothing more than a collection of things that are up to those criteria.

(ii) The sprint backlog is a collection of features, user stories, or bug fixes that the development team intends to focus on during each sprint. This list is arranged in a prioritized order. An increment is the result of a sprint that has been finished and is ready to be used.

(iii) An increment is named after the completion of a sprint. It is also possible to refer to an increment as a sprint goal. There is a possibility that you will not hear the phrase "increment" very frequently. This is since we typically use the term "done" to denote the team's definition, a milestone, the sprint objective, or even a successfully delivered completed version or epic. Because of this, we use the term "increment" less frequently. Both the definition of "done" and the sprint goal layout are crucial.

MODULE DESCRIPTION

A. Data Owner

Complete the account registration by providing the necessary information. Once the account has been authorized, the user can log in by entering the correct username and password. Subsequently, the user is required to upload the file utilizing the encryption format. Review the user's inquiry and proceed to submit your own request for re-encryption. Please check the current state and proceed to re-encrypt the key. Afterward, please log out.

B. User

Register an account and complete it by providing the required information. Once the account has been authorised, the user can access it by entering the correct username and password. They can then proceed to their profile, initiate a download request, retrieve the desired content, and subsequently log out.

.

C. Trust Authority

The Technical Assistant (TA) can access the account using the correct login credentials. As a result of this, they could observe users, authorize owners, monitor download requests, and distribute suitable keys. The teaching assistant also has the choice to terminate the programmer.

D. Proxy Server

Please provide the correct username and password in order to gain access to the account. Upon logging in, you will have the ability to see the list of downloaded files, view the graph, review any other relevant information, log out of the system, and view all uploaded files. Additionally, you have the ability to oversee re-encryption requests and provide a timely response.

E. CSP

Provide the correct username and password in order to gain access to the account. Upon logging in, you have the option to select from the following alternatives: Access all files that have been uploaded to the account. b) Access a comprehensive list of all downloaded files from the account. c) Retrieve the graph d) Terminate your account.

SYSTEM DESIGN

Engaging in control activities and establishing trustworthy connections with development executives are of utmost importance for the enhancement of the programming strategy, as is clear when seen from a more comprehensive perspective. Not only do these methods determine whether amendments to the protocol are necessary, but they also initiate subsequent improvement activities, if necessary. When it comes to programming design ideas and approaches, project managers regularly make poor choices, which can lead to unexpected complications and hinder the overall performance of the organization. When it comes to deciding where to place their money, investors that are interested in high-risk enterprises might utilize this framework as a form of guidance. To make progress towards a project's goals and objectives, "going all in" involves giving the project full attention and effort to achieve those goals. whenever there is a risk that a project will not be able to accomplish its objectives. Figure 1 below shows the proposed system for future enhancement.

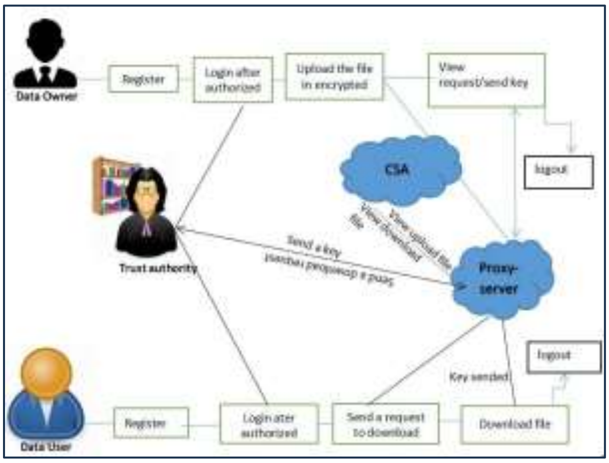

Figure 1. Proposed system for enhancement

CONCLUSION

As a result of the proliferation of connected devices, data sharing is quickly becoming one of the most well-known uses of the Internet of Things. An identity-based PRE-data-sharing system that is not only secure but also suitable for use in a cloud computing context is something that we recommend. The confidentiality, integrity, and privacy of the data will all be effectively protected because of this. IBPRE is a way that allows data owners to effectively share their encrypted data with authorized users while still maintaining their data in the cloud. This is made feasible by the approach. One of the technologies that makes this possible is called IBPRE. An edge device acts as a proxy to regulate the expensive calculations because of the limited resources that are available. In addition to this, the method also makes use of the capabilities of ICN to effectively supply cached information.

FUTURE ENHANCEMENTS

The Information-Centric Networking (ICN) system enhances the overall quality of the service and makes the most efficient use of the available bandwidth by efficiently delivering cached content. With this information in mind, we propose the creation of a system that makes use of the technology behind block chains to enable adjustable permissions for encrypted data. By combining the characteristics of ICN with those of block chain, our system provides protected and efficient access to data. Access to encrypted data is provided in line with regulations that are adaptable and customizable, and it enables granular authorization management. In addition to providing a robust framework for the management of data authorization in a secure and scalable manner, this decentralized technique helps to alleviate bottlenecks that are present in centralized systems.

References

X. Huang et al., "Blockchain-based proxy re-encryption scheme for secure IoT data sharing," IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6452-6462, 2021, 10.1109/BLOC.2019.8751336

Y. Liu et al., "Edge computing empowered blockchain-based data sharing with revocable fine-grained access control in industrial IoT," IEEE Transactions on Industrial Informatics, vol. 17, no. 4, pp. 2888-2897, 2021, 10.1109/TII.2020.3002804.

J. Zhou et al., "Secure and efficient data sharing scheme based on blockchain and proxy re-encryption for IIoT," IEEE Transactions on Industrial Informatics, vol. 18, no. 2, pp. 1426-1435, 2022, 10.1016/j.jnca.2020.102710.

T. Li et al., "Blockchain-based proxy re-encryption scheme with fine-grained access control for secure data sharing in IIoT," IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1626-1634, 2023, 10.1109/JSYST.2021.3076759

L. Yuan et al., "A secure data sharing scheme in blockchain-based IoT systems using proxy re-encryption and homomorphic encryption," in 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), pp. 1-6. 10.1016/j.phycom.2023.102048

I. Keshta et al., “Blockchain aware proxy re-encryption algorithm-based data sharing scheme,” Physical Communication, p. 102048, Mar. 2023, doi: 10.1016/j.phycom.2023.102048

W. Wang *et al.*, “A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks,” *IEEE Access*, vol. 7, pp. 22328–22370, 2019, 10.1109/access.2019.2896108.

R. Zhang et al., "A survey of blockchain-based schemes for data sharing and exchange," IEEE Network, vol. 37, no. 3, pp. 158-165, 2023, 10.1109/TBDATA.2023.3293279

H. Zhao, P. Bai, Y. Peng, and R. Xu, “Efficient key management scheme for health blockchain,” *CAAI Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 114–118, Jun. 2018, 10.1049/trit.2018.0014.

K. O.-B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia, and J. Gao, “A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain,” IEEE Systems Journal, vol. 16, no. 1, pp. 1685–1696, Mar. 2022, doi: 10.1109/jsyst.2021.3076759.