IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11465

Review Paper on Secure Data Sharing Based on Blockchain in IoT

Kirti D.Singh[1], Hirendra R. Hajare[2]

M.Tech Scholar ,Computer Science & Engineering Department ,Ballarpur Institute of Technology, Ballarpur, Chandrapur, M.S,India[1]

Assistant Professor, Computer Science & Engineering Department, Ballarpur Institute of Technology, Ballarpur, Chandrapur, M.S,India[2]

Abstract-The progress of the Internet of Things has seen data sharing as one of its utmost suitable applications in cloud computing. Data security remains one of the main failures it faces since the wrongful use of data leads to several damages. In this article, security is done by hiding the proxy data. Data owners can subcontract their hidden data to the cloud using identity-based encryption, while proxy re-hiding construction will grant appropriate users access to the data. With the Internet of Things devices being resource-constrained, the main device acts as a proxy server to handle high computations. Also, we make use of the feature of information-centric networking to deliver cached content in the proxy effectively, thus improving the quality of data and making good use of network bandwidth. Additionally, our system model is built on blockchain, a technology that allows decentralization in data sharing. It moderates the bottlenecks in centralized systems and fine-grained get into control to data. The security progress and study of our scheme show the ability of our method in ensuring data confidentiality integrity, and security.

Keywords:-Blockchain, access control, identity-based encryption, data Security.

I. INTRODUCTION

Computer security is information security as useful to computers and networks. The area covers all the method and mechanisms by which computer-based tools, data and facilities are secure from unintentional or illegal access, adjustment or demolition. Computer security is provided security from unintended events and natural blows. In the computer industry, the word security or the phrase computer security states to techniques for confirming that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

II. RELATED WORK

There exist different lessons on the security and privacy of the majority. Use of blockchain to secure many IoT Platforms. The IoT devices sense, gather and share a huge amount of data, thus opening up major security and privacy concerns. This paper has reviewed different security challenges to IoT and identified the uncertain transfer of IoT data as a high-level security risk. Most of the past work partly addresses the problem of securely sharing IoT data. It is nearly impossible to come up with device-embedded security to solve all the security threats to IoT devices. Limited computing and power resources of the Internet of things make the execution of complex security algorithms tougher on the device. We offer using the mixture of a block chain and a paring free proxy re-encryption policy to provide an operating platform and to ensure the secure transfer of the sensor data to the user.

III. CONCEPT OF CLOUD COMPUTING

"The cloud" refers to servers that are accessible to over the Internet, and the databases and software packages that run on the servers' environment. Cloud servers are located in data centers all over the worldwide. By using cloud computing, companies and user do not have ability to manage physical servers themselves or run software applications on their own machines. The cloud permit users to approach the same files and applications from several devices because the computing and storage takes place on servers in a data centre, it can be placed locally on the user device. This is why a user can log in to their Twitter account on a newly purchased phone after their old phone breaks and find

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11465

their old account in place, with all their videos, photos, and brief history. It works the same way with cloud email providers like rediffmail, yahoo mail or gmails, and with cloud storage providers like Google Drive etc.

Fig . Cloud Computing

IV. CHARACTERISTICS

Unique characteristics of a Cloud Computing are:

- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service
- On demand self-service

V. EXISTING SYSTEM

Proxy re-encryption (PRE), a notion first proposed by Blaze et al., allows a proxy to transform a file computed under a delegator's public key into encryption intended for a delegate. Let the data owner be the delegator and the data user by the delegate. In such a scheme, the data owner can send encrypted messages to the user temporarily without revealing his secret key. The data owner or a reliable third-party generates the re-encryption key. A proxy goes the re-encryption algorithm with the key and revamps the ciphertext before sending the new ciphertext to the user. An intrinsic trait of a PRE scheme is that the proxy is not fully trusted (it has no idea of the data owner's secret key). This is seen as a prime candidate for delegating access to encrypted data in a secured manner, which is a crucial component in any data-sharing scenario. In addition, PRE allows for encrypted data in the cloud to be shared with authorized users while maintaining its confidentiality from illegitimate parties.

VI. DRAWBACKS OF EXISTING SYSTEM

- In the existing system, High cost is involved in establishing maximum security.
- The traditional encryption patterns involve complex key management protocols and hence, are not apt for data sharing.
- In the existing system, the re-encryption was performed idly, and, therefore, the safety of the policy was weakened.
- The existing schemes tend to be inefficient when multiple and complex data pieces are considered.
- There is a leakage of access plans since they are public ones and are thus visible to everybody.
- They are not suitable in the context of IoT due to the heavy computations on encryption and decryption.

VII. PROPOSED SYSTEM

- This system proposes an improvement in IoT data sharing by combining PRE with identity-based encryption (IBE), information-centric networking (ICN), and blockchain technology.
- In the proposed system, the data owner propagates an access control list which is stored on the blockchain. Only authorized users are able to access the data.

DOI: 10.17148/IJARCCE.2022.11465

- We propose a secure access control framework to realize data confidentiality, and fine-grained access to data is achieved. This will also guarantee data owners' complete control over their data.
- We give a detailed description of our PRE scheme and the actualization of a complete protocol that guarantees the security and privacy of data.
- In the proposed system, the data is divided into 3 different blocks and stored in the cloud for the enhanced security model and then the proxy re-encryption approach is made for securing the data in the cloud.

VIII. BENEFITS OF PROPOSED SYSTEM

- PRE, together with IBE and the features of ICN and blockchain, will enhance security and privacy in data-sharing systems.
- PRE and IBE will ensure fine-grained data access control, while the concept of ICN promises a sufficient quality of service in data delivery because the in-network caching provides efficient distribution of data.
- The blockchain is optimized to prevent storage and data-sharing overheads and also to ensure a trusted system among entities on the network.

IX. CONCLUSION

- The development of the Internet of Things has made data sharing one of its utmost projecting applications. To assure data confidentiality, reliability, and privacy, we propose a secure identity-based PRE-data-sharing scheme in a cloud computing environment.
- Secure data sharing is realized with the IBPRE technique, which allows the data owners to store their encrypted data in the cloud and share them with legitimate users efficiently. Due to resource constraints, an edge device serves as the proxy to handle the intensive computations.
- The scheme also incorporates the features of ICN to proficiently deliver cached content, thereby improving the quality of service and making great use of the network bandwidth. Then, we present a blockchain-based system model that allows for flexible authorization on encrypted data.
- Fine-grained access control is achieved, and it can help data owners adequately achieve privacy preservation.
- The analysis and results of the proposed model show how efficient our scheme is, compared to existing schemes.

REFERENCES

[1] R. S. Da Silva and S. D. Zorzo, "An access control mechanism to ensure privacy in named data networking using attribute-based encryption with immediate revocation of privileges," in Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf., Jan. 2015, pp. 128–133.

[2] B. Li, D. Huang, Z. Wang, and Y. Zhu, "Attribute-based access control for ICN naming scheme," IEEE Trans. Dependable Secure Comput., vol. 15, no. 2, pp. 194–206, Apr. 2016.

[3] S. Misra et al., "Accconf: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge," IEEE Trans. Dependable Secure Comput., vol. 16, no. 1, pp. 5–17, Feb. 2017.

[4] E. G. AbdAllah, M. Zulkernine, and H. S. Hassanein, "DACPI: A decentralized access control protocol for information centric networking," in Proc. IEEE Int. Conf. Commun., May 2016, pp. 1–6.

[5] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT," IEEE Trans. Ind. Inform., vol. 15, no. 9, pp. 5099–5108, Jan. 2019.

[6] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," IEEE Trans. Ind. Inform., vol. 14, no. 10, pp. 4519–4528, Jan. 2018.

[7 Lowlesh Nandkishor Yadav, "Predictive Acknowledgement using TRE System to reduce cost and Bandwidth"IJRECE VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) pg no 275-278

[8] Ashish B. Deharkar and H. R Hajare , "Cloud Computing Based on Predictive Acknowledgement System," International Journal of Advanced Research in Computer and Communication Engineering Vol. 11 Issue 3 March 2022 PP 90-93

[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Trans. Inform. Syst. Secur., vol. 9, no. 1, pp. 1–30, Feb. 2006.

[10] R. Pecori, "S-kademlia: A trust and reputation method to mitigate a sybil attack in Kademlia," Comput. Netw., vol. 94, pp. 205–218, Jan. 2016.