International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Revocable Id-Based Authentication Proxy Re-Encryption to Secure Data Sharing Using on Blockchain

***S.Vijay*[1], *Mrs.R.Vijayalakshmi.,MCA.,M.Phil.,Ph.D*[2]**

[1]Master of Computer Application, krishnasamy college of engineering &Technology,Cuddalore

[2]Associate Professor, Master of Computer Application, krishnasamy college of engineering &Technology,Cuddalore

ABSTRACT

. The evolution of the Internet of Things has seen data sharing as one of its most useful applications in cloud computing. As eye-catching as this technology has been, data security remains one of the obstacles it faces since the wrongful use of data leads to several damages. In this article, we propose a proxy re-encryption approach to secure data sharing in cloud environments. Data owners can outsource their encrypted data to the cloud using identity-based encryption, while proxy re-encryption construction will grant legitimate users access to the data. With the Internet of Things devices being resource-constrained, an edge device acts as a proxy server to handle intensive computations. Also, we make use of the features of information-centric networking to deliver cached content in the proxy effectively, thus improving the quality of service and making good use of the network bandwidth. Further, our system model is based on blockchain, a disruptive technology that enables decentralization in data sharing. It mitigates the bottlenecks in centralized systems and achieves fine-grained access control to data. The security analysis and evaluation of our scheme show the promise of our approach in ensuring data confidentiality, integrity, and security

Keyword: Internet of Things, blockchain, secure data sharing

1.INTRODUCTION

The Internet of Things (IoT) has emerged as a technology that has great significance to the world nowadays and its utilization has given rise to an expanded growth in network traffic volumes over the years. It is expected that a lot of devices will get connected in the years ahead. Data is a central notion to the IoT paradigm as the data collected serves several purposes in applications such as healthcare, vehicular networks, smart cities, industries, and manufacturing, among others. The sensors measure a host of parameters that are very useful for stakeholders involved. Consequently, as enticing as IoT seems to be, its advancement has introduced new challenges to security and privacy. IoT needs to be secured against attacks that hinder it from providing the required services, in addition to those that pose threats to the confidentiality, integrity, and privacy of
data.

The use of symmetric encryption implies that the same key is shared between the data owner and users, or at least the participants agree on a key. This solution is very inefficient.Furthermore, the data owners do not know in advance who the intended data users are, and, therefore, the encrypted data needs to be decrypted and subsequently encrypted with a key known to both the data owner and the users. This decrypt-and-encrypt solution means the data owner has to be online all the time, which is practically not feasible. The problem becomes increasingly complex when there are multiple pieces of data and diverse data owners and users.

lthough simple, the traditional encryption schemes involve complex key management protocols and, hence, are not apt for data sharing. 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 an encryption intended for a delegatee. Let the data owner be the delegator and the data user be 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 trusted third party generates the re-encryption key. A proxy runs 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

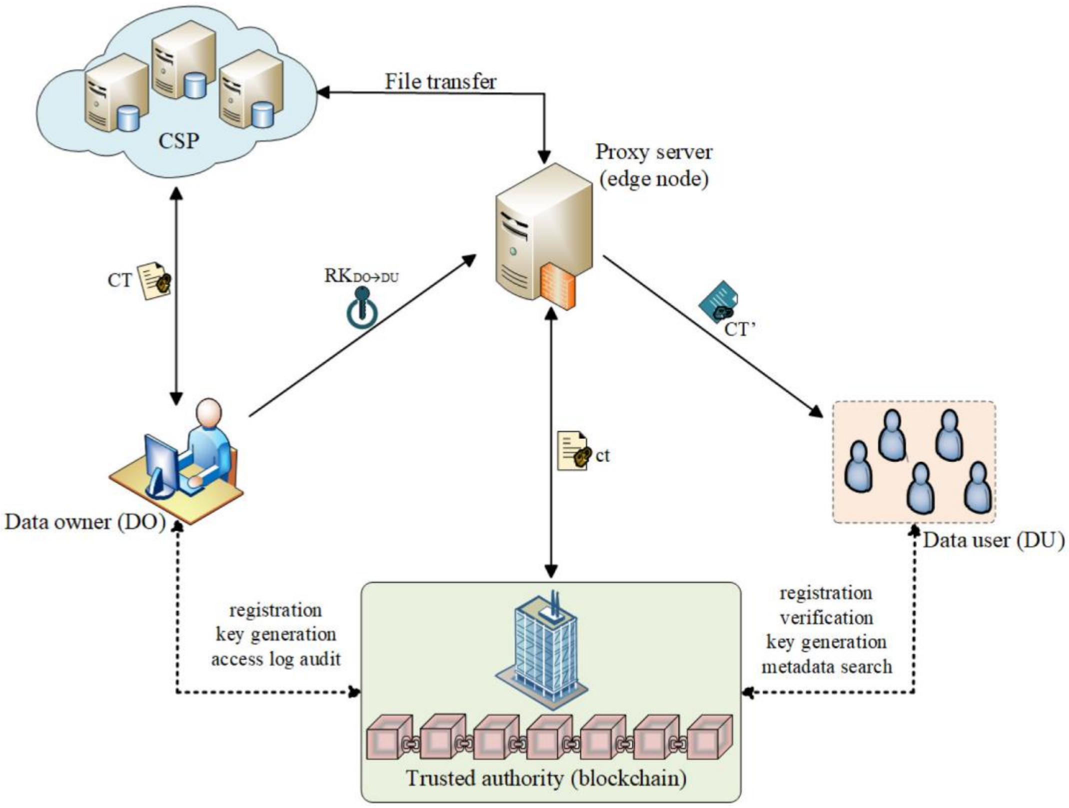
2. LITERATURE SURVEY

[1] A. Al-Fuqaha, an overview of the Internet of Things (IoT) with emphasis on enabling technologies, protocols, and application issues. The IoT is enabled by the latest developments in RFID, smart sensors, communication technologies, and Internet protocols. The basic premise is to have smart sensors collaborate directly without human involvement to deliver a new class of applications. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as the first phase of the IoT. In the coming years, the IoT is expected to bridge diverse technologies to enable new applications by connecting physical objects together in support of intelligent decision making. Finally, we present detailed service use-cases to illustrate how the different protocols presented in the paper fit together to deliver desired IoT services.

[2] M. Blaze, The notion of divertibility as a protocol property as opposed to the existing notion as a language property (see Okamoto, Ohta [OO90]). We give a definition of protocol divertibility that applies to arbitrary 2-party protocols and is compatible with Okamoto and Ohta's definition in the case of interactive zero-knowledge proofs. Other important examples falling under the new definition are blind signature protocols. We propose a sufficiency criterion for divertibility that is satisfied by many existing protocols and which, surprisingly, generalizes to cover several protocols not normally associated with divertibility (e.g., Diffie-Hellman key exchange).

3.PROPOSED SYSTEM

- This system proposes an improvement in IoT data sharing by combining PRE with ID-based encryption (IDBE), 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 the authorized users are able to access the data. 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 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.



Algorithm

- 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.
- . In addition, PRE allows for encrypted data in the cloud to be shared to authorized users while maintaining its confidentiality from illegitimate parties.Data disclosures can be minimized through the use of encryption since only users delegated by the data owner can effectively access the outsourced data.Motivated by this scenario, this article proposes an improvement in IoT data sharing by combining PRE with identity-based encryption (IBE), information-centric networking (ICN), and blockchain technology.

CONCLUSION

1`zqBlockchain technology creates a permanent and immutable record of every transaction .This impenetrable digital ledger makes fraud, hacking, data theft and information loss impossible. While blockchain technology has reshaped and decentralized financial institution, its application possibilities are for more robust. Then, we present a block chain-based system model that allows for flexible authorization on encrypted data. Fine grained access control is achieved, and it can help data owners achieve privacy preservation in an adequate way. The analysis and results of the proposed model show how efficient our scheme is, compared to existing schemes..

FUTURE ENHANCEMENTS

By enabling detailed user access control in cloud environments, sensitive information stored on cloud servers can be managed more safely. The proposed protocol provides a structure by means of which a large capacity of various data, including users' personal information requiring high confidentiality, can be accessed safely and efficiently. We expect the proposed protocol to be widely and efficiently used in the cloud computing environment. However, a disadvantage of this method is the additional computation in the polynomial equation compared to existing attribute-based encryption methods, since it provides more functions. In the future, we will study more efficient and safer methods based on the proposed method

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347–2376, Oct./Dec. 2015.

[2] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 1998, pp. 127–144.

[3] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc.Workshop Theory Appl. Cryptographic Techn., Springer, Aug. 1984, pp. 47–53.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, May 2004, pp. 506–522.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in NDSS, vol. 4. Citeseer, Feb. 2004, pp. 5–6.

[6] D. Balfanz et al., “Secret handshakes from pairing-based key agreements,” in Proc. IEEE, Symp. Secur. Privacy, 2003, pp. 180–196.

[7] R. Canetti, S. Halevi, and J. Katz, “Chosen-ciphertext security from identity-based encryption,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, 2004, pp. 207–222.

[8] T. Koponen et al., “A data-oriented (and beyond) network architecture,” in Proc. Conf. Appl., Techn., Architectures, Protoc. Comput. Commun., Aug. 2007, pp. 181–192.

[9] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, “Developing information networking further: From PSIRP to pursuit,” in Proc. Int. Conf. Broadband Commun., Netw. Syst., Springer, Oct. 2010, pp. 1–13.

[10] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, “Secure naming for a network of information,” in Proc. INFOCOM IEEE Conf. Comput. Commun. Workshops,2010, pp. 1–6.

[11] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, “A routing scheme for content-based networking,” in Proc. IEEE INFOCOM 2004, vol. 2, 2004, pp. 918–928.

[12] I. Psaras,W. K. Chai, and G. Pavlou, “Probabilistic in-network caching for information-centric networks,” in Proc. 2nd ed. ICN Workshop Inform.-Centric Netw., Aug. 2012, pp. 55–60.

[13] Y. Sun et al., “Trace-driven analysis of ICN caching algorithms on videoon-demandworkloads,” in Proc. 10th ACMInt. Conf. Emerging Netw. Exp. Technol., Dec. 2014, pp. 363–376.

[14] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, vol. 4. Bitcoin.org, 2008. Available: https://bitcoin. org/bitcoin. pdf

[15] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. IEEE

INFOCOM, Mar. 2010, pp. 1–9.

[16] N. Park, “Secure data access control scheme using type-based reencryption in cloud environment,” in Semantic Methods Knowledge Management and Communications. Berlin,Germany: Springer, 2011, pp. 319–327.

[17] G. Wang, Q. Liu, J. Wu, and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,” Comput. Secur., vol. 30, no. 5, pp. 320–331, Jul. 2011.

[18] J. Hur, “Improving security and efficiency in attribute-based data sharing,” IEEE Trans. Knowl. Data Eng., vol. 25, no. 10, pp. 2271–2282, Apr. 2011.

[19] P. K. Tysowski and M. A. Hasan, “Hybrid attribute-and re-encryption based key management for secure and scalable mobile applications in clouds,” IEEE Trans. Cloud Comput., vol. 1, no. 2, pp. 172–186, Nov. 2013.

[20] Q. Liu, G. Wang, and J. Wu, “Time-based proxy re-encryption scheme for secure data sharing in a cloud environment,” Inform. Sci., vol. 258, pp. 355–370, Feb. 2014.

[21] J. Han, W. Susilo, and Y. Mu, “Identity-based data storage in cloud computing,” Future Gener. Comput. Syst., vol. 29, no. 3, pp. 673–681, Mar. 2013.

[22] H.-Y. Lin, J.Kubiatowicz, andW.-G. Tzeng, “A secure fine-grained access control mechanism for networked storage systems,” in Proc. IEEE 6th Int. Conf. Softw. Secur. Rel., Jun. 2012, pp. 225–234.

[23] Y. Zhou et al., “Identity-based proxy re-encryption version 2: Making mobile access easy in cloud,” Future Gener. Comput. Syst., vol. 62, pp. 128–139, Sep. 2016.

[24] X. A.Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, “Cost-effective secure e-health cloud system using identity based cryptographic techniques,” Future Gener. Comput. Syst., vol. 67, pp. 242–254, Feb. 2017.

[25] J. Shao, G. Wei, Y. Ling, and M. Xie, “Identity-based conditional proxy re-encryption,” in Proc. IEEE Int. Conf. Commun., Jun. 2011, pp. 1–5.

[26] K. O. B. Obour Agyekum et al., “A secured proxy-based data sharing module in IoT environments using blockchain,” Sensors, vol. 19, no. 5, Jan. 2019, Art. no. 1235.