An Efficient And Secure Data Sharing In Iot Based On Blockchain

T.Dhurga Devi[1], Mr. U. Sundhar, M.E.[2]
[2] Professor
[1, 2] Thiruvalluvar College Of Engineering And Technology, Vandavasi – 604 505.

Abstract- *Due to the evolution of Internet of Things, data sharing is seen as one of the most useful applications in cloud computing. In data sharing, data security has become one of the obstacles, since the wrongful use of data leads to several damages. In this paper, a proxy re-encryption approach to secure data sharing in cloud environments proposed. Identity-based encryption is used by data owners to outsource their encrypted data to the cloud, where proxy re-encryption construction will grant legitimate users access to the data. With the IoT devices being resource-constrained, for handling intensive computation an edge device acts as a proxy server. Also, this system makes 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, the proposed system is based on blockchain, a disruptive technology that enables decentralization in data sharing. It achieves fine-grained access control to data by mitigating the bottlenecks in centralized systems. The security analysis and evaluation shows that proxy re-encryption approach ensures data confidentiality, integrity, and security.*

Keywords- Access control, Blockchain, Data Security, Identity Based Proxy Re-Encryption, Information-Centric Network (ICN), Internet of Things (IoT).

I. INTRODUCTION

The internet of things is a system of interrelated computing device, mechanical and digital machines or objects which are provided with unique intensifiers (UIDs) and ability to transfer the data through a network without the requirement humans. The IoT provides businesses with a real-time look into their systems really work, delivering insights into everything from a performance of machines to supply chain and logistics operations. Increasingly, organizations in a variety of the industries are used IoT to operate more efficient, better understand customers to delivered enhanced customer service, improve decision-making and increase the value of business. An IoT ecosystem consists of web-enabled smart devices that used embedded systems, such as processors, sensors and communication hardware, to collect, send and act on data they acquire from their environments. IoT devices share the sensor data they collect by connecting to an IoT gateway or other edge device where data sent to the cloud to be analyzed locally. The devices communicate with other related devices and act on the information they get from one from another. The devices almost of the work without human intervention, although people can interact with the devices for instance, to set them up, give them instructions or access the data.

A viable solution is to encrypt the data before outsourcing to the cloud servers. Attackers can be only see the data in its encrypted form when traditional security measures fail. In data sharing, any information must be encrypt from the source and only decrypt by authorized user in order to the preserve its protection. Conventional encrypt technique can be used, where the decrypt key is a shared large among of the data users designated by the data owner. The use of symmetric encrypt implies that a same keys is share between the data owner to users, or at least the participants agree on a key.This solution that very inefficient. Furthermore, the data owners do not know the advance who the intended of the data users are, and, therefore, the encrypted data needs to be decrypt and subsequently encrypt with a key known to both the data owner and the users. This decrypt-and-encrypt solution means that the data owner has been online all the time, which is practically not feasible. The problem becomes an increasing complex when there are multiple pieces of the data, diverse data owners and users

II. RELATED WORK

A. PRE Data Sharing

The data was encrypted used KP-ABE meant that only an appropriate collection of the attribute secret keys can make decrypted possible. The encrypted data, the cloud also managed all the attribute secret keys except one special secret key in order to handle revocation of users. When user are revoked, new keys are distributed to the remaining users by the data owner and the encrypted data had to be re-encrypted. Although the scheme was efficient, the re-encryption is performed in a lazy way, and, the security of the scheme a weakened. The service provide and revoke users is avoided.

Their scheme is basically to replace the service provide with a trust third party, which implies that should be reliance on stronger trust assumption. The proposed a time-constrained access control scheme based on PRE and ABE. ABE is used to design time-based access control policies while PRE was used to update the time attribute, they are not suitable in the context of IoT due to the heavy computation on encrypted and decrypted.

An identity-based PRE (IBPRE) scheme for accessing health record. The scheme achieved coarse-grained access control. If the proxy receive the re-encrypted key from the data owner, re-encrypted and accessible to the ciphertext can be either all the intended users or none at all. In the, proposed an IBE PRE scheme based on conditions. In their proposal, the proxy could transform a subset of the ciphertext under an identity to other ciphertext under another identity. The decrypted rights to a group of user could not be authorized. In above to the addition is PRE has been used to mitigate security problems in an IoT.

B. Blockchain-Based Access Control and Data Sharing

In used blockchain to provide distributed the ensure privacy and personal data management as well. The blockchain is utilized as automatic access to the control manager, and, hence, no third party was required. The data address stored on the blockchain and a distributed hash table was used as the implementation of the data storage. This reduced the risk of data leakage. However, no specific access to the control model was proposed in their scheme. The blockchain-based on access to the control scheme where the data owner the policies data and stores them on the blockchain. The policies are then assign to the users as access to the rights. The encrypted data is uploaded to the cloud and access to the policies on the data are stored on the blockchain as transactions. Although these two schemes achieve to tamper-proof systems and easy auditing, there is a leakageof access to the policies since the blockchains used to public ones and are thus visible to everyone. In presented a blockchain-based model for sharing data in the vehicular networks and enable secure communication among vehicles. A public blockchain does not work well in peer-to-peer (P2P) data sharing among the vehicles due to the high cost involved in establish a public blockchain in resource-constrained of the vehicles.

C. Access Control Schemes for ICN

In order to control content in ICN frameworks, several centralized and decentralized access to the control mechanisms have been proposed in literature. The presented an access to the control system on the data networking which relied on an ABE scheme and a proxy server. Before the content is publish, the data owner can be encrypts the content and generates an access to the policy that binds it. The encrypt data to be stored in the immediate routers while the access to the policy is stored on the server. When a user wants to access to the content, the user retrieves the content from a router, the access policy from a proxy server, and then decrypts the data. Their scheme enables user revocation; it suffers from a single point of failure if a proxy server to be fails the work because to the proxy server takes a part of the each content access. The designed a privacy enhancing scheme using ABE for access to the control in ICN, and a trusted third party is deployed to manage attributes. A content publisher generates an access to the policy based on the attributes defined by the third party uses a random symmetric key to be encrypt the data. The publisher then hides the random key and the access to the policy in the content name and only authorized users can gain access to the content. The proposed scheme achieve a privacy by hiding the access to the policy in the content name, but user revocation is not guaranteed. For decentralized access control systems,the proposed a secure content delivery ICN framework using Shamir's threshold secret sharing scheme of the broadcast encryption but without the services of a third party.

A symmetric key is used to encrypt the content which is a broadcast to the network along with the key of generation materials. Only authorized user can be use these keying materials and decrypt the encrypt data using their individual keys. The scheme provides user revocation services, but an account of each content to the access or the history of keying materials' update is not kept. This makes auditing difficult. The Diffie–Hellman (DH) protocol in the process of content to be publishing to achieve decentralized access to the control. After going the various stages of the Diffie–Hellman key exchange protocol, the ICN verifies the metadata and sends the encrypt data together with the shared key. There is no single point of the failure in this scheme; the cached to the content in the ICN is in the plaintext form which makes it vulnerable to attacks

III. PROPOSED SYSTEM

In this subsection, we analyze the attacks that our proposed system mitigates.

Methodology

In this project a secure access control framework is proposed to realize data confidentiality, and fine-grained access to data are achieved and this will also guarantee data owners' complete control over their data. The PRE scheme actualize a complete protocol that guarantees security and privacy of data. To improve data delivery and effectively utilize the network bandwidth, edge devices serve as proxy nodes and perform re-encryption on the cached data. The edge devices are assumed to have enough computation capabilities than the IoT devices and as such provide high performance networking. A consortium blockchain is adopted due to its suitability to access control and privacy preservation. Only authorized user can be have access to the data.

Data owners can effectively manage their data and audit logs. Consortium blockchains provide a high level of security. IoT security concerns that are addressed by the blockchain network include verifying the identity of the connected users or devices, their account information, and also preventing cached data from being misused. Because edge devices have enough computing resources and storage, they act as proxy servers to provide re-encryption services and other computations for the resource-constrained IoT devices. It is, therefore, easy to cache data at these edge of the nodes. Retrieving data via high-speed networks, the user can make requests for data access, thus providing a smooth user experience. In this proposed system, the following modules such as data owner, data user, proxy server, cloud service provider and trusted authority are used.

DATA OWNER

The data owners are the entities that they generate the data. Normally data owners can participate in data protection from the onset by encrypting the data and outsourcing it to the cloud service providers (CSPs) themselves. In this proposed model data owner generate the data and store in the CSP in chipertext form. Data owner need to register in this web application. The data owner need private key which will receive when the data owner sign-in with trusted authority. More protection is needed to the data. When the user request to access the data, data owner will receive the approval request through the proxy server. Then by approving the request, user can decrypt the chipertext and download the original data and can access it.

DATA USER

The data user domain consists of legitimate recipients of the information that is shared by the owners. These data users must access the shared data from the CSP which is a semi-trusted party that offers storage services to the data. It houses the encrypted data from the owner and the data is received through a secure communication channel. They provide data-sharing services without being able to learn anything about the plaintext. The data user need to register in this application and also sign-in with trusted authority to receive the private key, which help to search the data and download it. The data user search the data that the data user needed and send the request to access the data. Once the request is approved, the user can now decrypt the ciphertext with his private key and download the data and access it.

PROXY SERVER

The edge devices serve as proxy nodes and provide re-encryption services to the authorized user(s). When the data is cached at the edge of the network, the edge devices provide services to users with high availability and performance. When the user request for the approval that will send to data owner though the proxy server. And the proxy server can see the data owners list and their registered details. Proxy server help the data owner and the user to secure the data and provide the secured data access framework

CLOUD SERVICE PROVIDER

The cloud service provider plays an important role in this models, CSP keeps the data that stored by data owners. The ciphertext is then outsourced to the CSP and the keyword for the data is stored on the trusted authority. The related information on the data is fetched from the cache, while the associated ciphertext is also retrieved from the CSP. Retrieving data via high-speed networks, the user can make requests for data access, thus providing a smooth user experience. The CSP also have login and the access to see the stored partial details of the data by data owners.

TRUSTED AUTHORITY

The blockchain is acting as a trusted authority, which verify the data owner and the data user. In blockchain-based systems and applications, forks become important with every chance of the evolution of a malicious purpose. The data owner and the data user need to sign-in with this trusted authority to receive the private key. With the help of the private key that issued by trusted authority, data owner can upload the chipertext of the data needed to store in CSP. And data user can send request and decrypt chipertext and download the data to access. This is like the trusted authority issue the access permission to the data user and the data owner, so that the data will stored and protected. The verification is important in the access control, the trusted authority is also very important model in this proposed system.

System Architecture

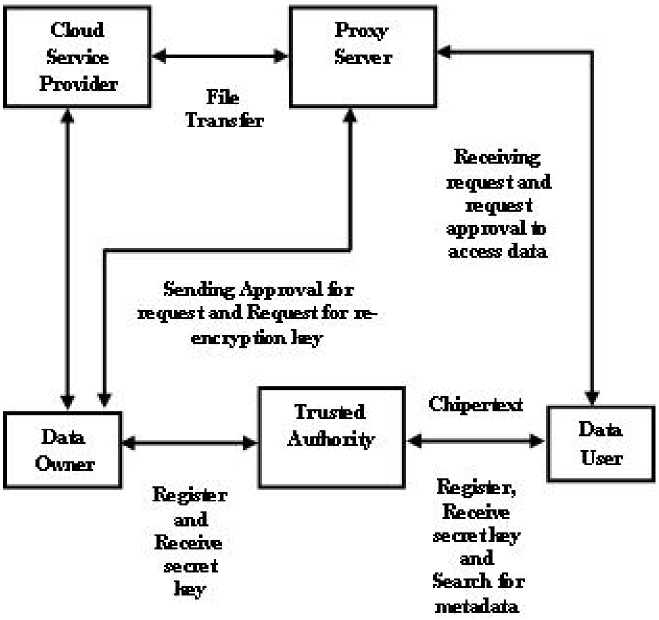
Cloud Service Provider
Proxy Server
File Transfer
Receiving request and request approval to access data
Sending Approval for request and Request for re-encryption key
Data Owner
Trusted Authority
Chipertext
Data User
Register and Receive secret key
Register, Receive secret key and Search for metadata

Fig: System Architecture

IV. CONCLUSION

The emergence of the IoT has made data sharing one of its most prominent applications. To guarantee data confidentiality, integrity, and privacy, a secure identity-based PRE data-sharing scheme is proposed in a cloud computing environment. Secure data sharing is realized with 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, a blockchain-based system model is presented that allows flexible authorization on encrypted data. Finegrained access control is achieved, and it can help data owners achieve privacy preservation in an adequate way.

REFERENCES

[1] 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., 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.

[10] 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.

[11] 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.

[12] Y. Sun et al., “Trace-driven analysis of ICN caching algorithms on video on-demand workloads,” in Proc. 10th ACM Int. Conf. Emerging Netw. Exp. Technol., Dec. 2014, pp. 363–376.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] H.-Y. Lin, J. Kubiatowicz, and W.-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.

[22] 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.

[23] 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.

[24] 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

[25] 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.