JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhanced Data Sharing IoT Server Platform Using Blockchain

[1]Dr.G.Nivetha, Dr.B.Senthinayaki, B.Keerthana, D.Sowmiya

[1]Assistant Professor, [2]Teaching Fellow, [3,4]Assistant Professor
[1,3,4] Department of Electronics and Communication Engineering, [2] Department of Information Science and Technology
[1,3,4] University College of Engineering Panruti, Panruti, Tamilnadu, India, [2] College of Engineering, Guindy,Chennai,Tamilnadu, India

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 this technology remains one of the obstacles as it faces since the misuse of data leads to several damages. In this work, a proxy re-encryption approach is proposed 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, the features of information-centric networking to deliver cached content in the proxy are used. Thus improving the quality of service and making good use of the network bandwidth. Further, the proposed work 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 this scheme show the promise of proposed approach in ensuring data confidentiality, integrity, and security.

Index Terms **– Data sharing, encryption, blockchain.**

I. 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. A viable solution is to encrypt the data before outsourcing to the cloud servers. Attackers can only see the data in its encrypted form when traditional security measures fail. In data sharing, any information must be encrypted from the source and only decrypted by authorized users in order to preserve its protection. Conventional encryption techniques can be used, where the decryption key is shared among all the data users designated by the data owner. 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.

Although simple, the traditional encryption schemes involve complex key management protocols and they are not appropriate 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 delegate. 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 cipher text before sending the new cipher text 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 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 proposed work is focused on an improvement in IoT data sharing by combining PRE with Identity-Based Encryption (IBE), Information-Centric Networking (ICN), and blockchain technology.

On issues of trust a decentralized, distributed system that can smoothen secure and trusted data sharing was introduced by Nakamoto. This is the block chain technology, and it has gained much attention due to its ability to preserve data privacy. Although there exist optimization issues when storing vast sizes of data, emerging system applications have used the blockchain for access control in database management. Data confidentiality and user revocation and also be achieved using blockchain.PRE, together with IBE and the features of ICN and blockchain, will enhance security and privacy in data- sharing systems. PRE and IBE will be ensured 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 block chain is optimized to prevent storage and data- sharing overheads and also to ensure a trusted system among entities on the network. In this article, the data owner propagates an access control list which is stored on the block chain. Only the authorized users are able to access the data. The contributions of this article are summarized as follows.

1. This proposes a secured access control framework to realize data confidentiality and fine-grained access to data are achieved. This will also guarantee data owners complete control over their data.
2. This project gives a detailed description of the PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.
3. To improve data delivery effectively and 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.
4. The security analysis of this scheme is presented, and this also test and compare its performance with existing schemes.

This article is structured as follows. Section II reviews some literature on PRE, IBE, ICN, and blockchain for data sharing and access control. Proposed methodology is described in section III.

II. SURVEY ON EXISTING METHODS

Al-Fuqaha et.al, proposed 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. This project starts by providing a horizontal overview of the IoT. Then, it gives an overview of some technical details that pertain to the IoT enabling technologies, protocols, and applications. Compared to other survey papers in the field, our objective is to provide a more thorough summary of the most relevant protocols and application issues to enable researchers and application developers to get up to speed quickly on how the different protocols fit together to deliver desired functionalities without having to go through RFCs and the standards specifications. It also provides an overview of some of the key IoT challenges presented in the recent literature and provide a summary of related research work. Moreover, it explores the relation between the IoT and other emerging technologies including big data analytics and cloud fog computing. This also presents the need for better horizontal integration among IoT services. Finally, these project present detailed service use-cases to illustrate how the different protocols presented in the project fit together to deliver desired IoT services.

Shamir et.al, introduced a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. This scheme assumes the existence of trusted key generation centers, whose sole purpose is to give each user a personalized smart card when he first joins the network. The information embedded in this card enables the user to sign and encrypt the messages he sends and to decrypt and verify the messages he receives in a totally independent way, regardless of the identity of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue to function in a completely decentralized way for an indefinite period. Boneh et.al, studied the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. It defines and constructs a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. It refers to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using this mechanism Alice can send the mail server a key that will enable the server to identify all messages containing some specific keyword, but learn nothing else. It defines the concept of public key encryption with keyword search and give several constructions.

Waters et.al, logs are an important part of any secure system, and they need to be carefully designed in order to give a faithful representation of past system activity. This is especially true in the presence of adversaries who might want to tamper with the audit logs. While it is important that auditors can inspect audit logs to assess past system activity, the content of an audit log may contain sensitive information, and should therefore be protected from unauthorized parties. Protecting the contents of audit logs from unauthorized parties (i.e., encrypting it), while making it efficiently searchable by authorized auditors poses a problem. It describes an approach for constructing searchable encrypted audit logs which can be combined with any number of existing approaches for creating tamper-resistant logs. In particular, it implemented an audit log for database queries that uses hash chains

for integrity protection and identity-based encryption with extracted keywords to enable searching on the encrypted log. This technique for keyword search on encrypted data has wide application beyond searchable audit logs.

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 delegate. 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. The traditional encryption schemes involve complex key management protocols and hence, are not apt for data sharing.

In the existing system, the re-encryption was performed in a lazy way and therefore, the security of that scheme was weakened. They are not suitable in the context of IoT due to the heavy computations on encryption and decryption. The existing schemes tend to be inefficient when multiple and complex data pieces are considered. There is a leakage of access policies since they are public ones and are thus visible to everyone. High cost involved in establishing more security.

III. PROPOSED SYSTEM

This system proposed (Figure 1) is 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. This proposes 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. It gives a detailed description of this PRE scheme and the actualization of a complete protocol that guarantees security and privacy of data.In this 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.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.

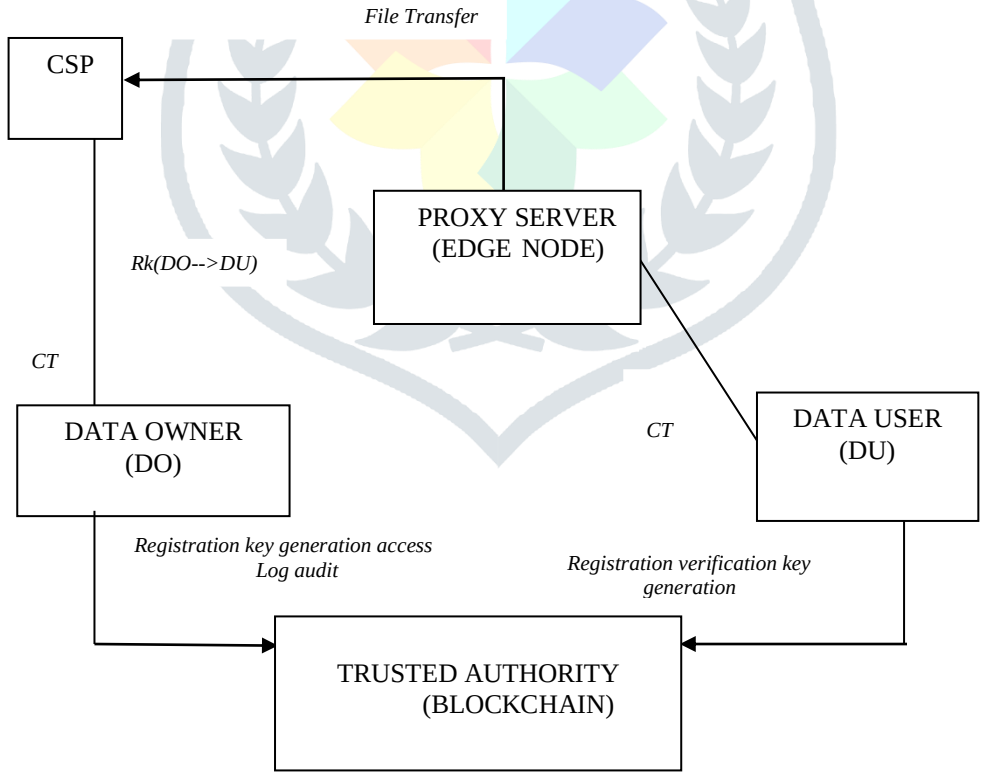

Figure 1 : Proposed Block diagram

3.1. Data Owner

In Data Owner module, Initially Data Owner must have to register their details. Then trusted authority should approve every new data owner. Only if the trusted authority approves the data owner, the data owner can able to login or else it's not

possible to login to the system. In every login the data owner should provide the private key apart from username and password. After successful registration data owner can login and upload files into cloud server with the block splitted into 3 various parts and encrypted for more security purpose. Data Owner can view the files that are uploaded in cloud. Data Owner can approve or reject the file request sent by data users. After request approval data owner will send the secret key and verification object through mail.

3.2. Data User

In this module, it develops Data User part. Where the new data user should register the details and then the trusted authority should approve the new data user. Only if the data user is approved by the trusted authority, the data user can able to get the key or login to the system, or else the data user cannot able to login into the system. In every login the data user should provide the private key apart from username and password. Once the authenticated data user logs in, the data user can able to search the available files, by entering the keyword of the file. To get the access of the file, the data user must provide the request. Only if the request is accepted, the data user can able to download the file which the data user requested. The 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.

3.3. Trusted Authority

The trusted authority is the entity which approves the new data Owner or data user in the system. The block chain serves as the trusted authority (TA) that initiates the system parameters. The TA also provides secret keys that are bound to the users' identities. By utilizing this distributed ledger, authenticity, transparency, and verifiability are achieved in the network, which enhances the security and privacy of data. Data owners are therefore able to manage their data effectively. The block chain network registers and issues membership keys to the data owner(s) and user(s). When a user requests data access, the owner generates a re-encryption key by using the identity of the user and sends it to the proxy server. Access rights and policies on the use of the data are instantiated and sent to the block chain network. A data user is verified before access is granted.

3.4. Proxy Server

In this module, it implements the Proxy server. In Proxy re-encryption a User may encrypt his file with his own public key and then store the cipher text in an honest-but-curious server. When the receiver is decided, the sender can delegate a re-encryption key associated with the receiver to the server as a proxy. Then the proxy re-encrypts the initial cipher text to the intended receiver. Finally, the receiver can decrypt the resulting cipher text with her private key. The security of PRE usually assures that,

(1) Neither the server/proxy nor non-intended receivers can learn any useful information about the (re-)encrypted file.

(2) Before receiving the re-encryption key, the proxy cannot re-encrypt the initial cipher text in a meaningful way.

3.5. CSP

In this module, it develops Cloud Service Provider (CSP). For the implementation of cloud storage, it uses DriveHQ cloud service provider where the files uploaded by the data owner are stored in the cloud service as blocks and fragments. Moreover, if an attacker is uncertain about the locations of the fragments, the probability of finding fragments on all of the nodes is very low. Therefore, the fragments in the given Data files are uploaded in the Cloud so that no attacker will obtain the data file. In cloud systems, the probability for an attacker to obtain a considerable amount of data reduces significantly. However, placing each fragment once in the system will increase the data retrieval time. The output screen shot of the proposed work is shown in Figure 2.The average encryption time and decryption time for the proposed system is shown in Figure3.

VI. CONCLUSION AND FUTURE WORK

Block chain technology creates a permanent and immutable record of every transaction. This impenetrable digital ledger makes fraud, hacking, data theft and information loss impossible. While block chain technology has reshaped and decentralized financial institution, its application possibilities are for more robust. Then, it presents 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.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. This expects 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, study more efficient and safer methods based can be proposed.

REFERENCES

[1]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, 2015, "Internet of Things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surveys Tut., vol. 17, no. 4, pp. 2347–2376.
[2]. M. Blaze, G. Bleumer, and M. Strauss, 1988, "Divertible protocols and atomic proxy cryptography," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, pp. 127–144.
[3]. A. Shamir, 1984, "Identity-based cryptosystems and signature schemes," in Proc.Workshop Theory Appl. Cryptographic Techn., Springer, pp. 47–53.
[4]. D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, 2004, "Public key encryption with keyword search," in Proc. Int. Conf. Theory Appl. Cryptographic Techn., Springer, pp. 506–522.
[5] I. Psaras,W. K. Chai, and G. Pavlou, 2012, "Probabilistic in-network caching for information-centric networks," in Proc. 2nd ed. ICN Workshop Inform.-Centric Netw., pp. 55–60.
[6] Y. Sun et al., 2014, "Trace-driven analysis of ICN caching algorithms on videoon-demand workloads," in Proc. 10th ACMInt. Conf. Emerging Netw. Exp. Technol., pp. 363–376.
[7] S. Nakamoto, 2008, Bitcoin: A Peer-to-Peer Electronic Cash System, vol. 4. Bitcoin.org, Available: https://bitcoin. org/bitcoin. pdf
[8] P. K. Tysowski and M. A. Hasan, 2013, "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.
[9] Q. Liu, G. Wang, and J. Wu, 2014, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Inform. Sci., vol. 258, pp. 355–370.
[10] J. Han, W. Susilo, and Y. Mu, 2013, "Identity-based data storage in cloud computing," Future Gener. Comput. Syst., vol. 29, no. 3, pp. 673–681.
[11] Y. Zhou et al., 2016, "Identity-based proxy re-encryption version 2: Making mobile access easy in cloud," Future Gener. Comput. Syst., vol. 62, pp. 128–139.
[12] X. A.Wang, J. Ma, F. Xhafa, M. Zhang, and X. Luo, 2017, "Cost-effective secure e-health cloud system using identity based cryptographic techniques," Future Gener. Comput. Syst., vol. 67, pp. 242–254.