International Journal on Applications in Information and Communication Engineering
Volume 2: Issue 3: March 2016, pp 18-21. www.aetsjournal.com ISSN (Online) : 2394-6237

Secure Big Data Storage To Guarantee Confidentiality In Cipher Text Multi sharing Control

R.Ilakkiya , R.Senthamil Selvi

Abstract— The secure big data storage services are basic requirement of the service is to guarantee the confidentiality of the data. However, the anonymity of the service clients, one of the most essential aspects of privacy should be considered simultaneously. Moreover the service also should provide practical and fine-grained encrypted data sharing such that a data owner is allowed to share cipher text of data among others under some specified conditions. Propose a privacypreserving cipher text multisharing mechanism to achieve the properties. It combines the merits of proxy re-encryption with anonymous technique in which a cipher text can be securely and conditionally shared multiple times without leaking both the knowledge of underlying message and the identity information of cipher text senders/recipients.

Key Words—Data storage, Confidentiality, Big data, Data sharing, Proxy re-encryption.

I. INTRODUCTION

Big data is similar to "small data", but bigger in size. An aim to solve old problems and new problems in a better way. It refers to technologies and initiatives that involve data that is too diverse, fast changing or massive for conventional technologies. But today, new technologies make it possible to realize value from big data. Data storage configurations are used for big data analytics and what type of storage infrastructure does it require. It specifies that only the sender and intended recipients should be able to access the contents of a message. Confidentiality is roughly equivalent to privacy. It access must be restricted to those authorized to view the data in question. Data sharing is main functionality in cloud storage, but need of sharing data very securely and maintaining privacy. Solution is cryptosystem owner of data encrypt data before uploading to the cloud with its own key. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. Proxy re-encryption schemes are cryptosystems which allow third parties to alter a cipher text which has been encrypted for one party, so that it may be decrypted by another. Proxy reencryption schemes are similar to traditional symmetric or asymmetric encryption schemes. The proxy should not be able to learn the keys of the participants or the content of the messages it reencrypts. Content owners may want to use the proxy to help re-encrypt sensitive information without revealing to the proxy the identity of the recipients. It is a cryptosystem with the special property that a proxy, given special information, can efficiently convert a cipher text. The cipher text is anonymous that is, it cannot be linked to a particular public key and its owner.

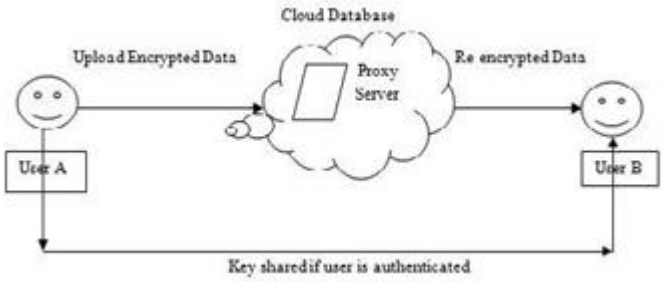

Fig. 1. Key Sharing

A. Related Works

Let us discuss some of the previous work done in this area. A cipher text policy attribute based PRE employs the PRE technology in the attribute based encryption cryptographic setting, in which the proxy is allowed to convert an encryption under an access policy to another encryption under a new access policy. The server, nevertheless, cannot learn the data during the conversion of cipher texts. The new system supports any monotonic access policy such that system users are allowed to fulfil more flexible delegation of decryption rights. Propose a new PRE systems is one for the transformation from cipher texts encrypted under a traditional certificate based public key into the cipher texts that can be decrypted by an secret key for identity based encryption, and the other one for the transformation from cipher texts that can be decrypted by the other secret key for the IBE. The system does not need additional algorithm or process for decryption re-encrypted cipher texts while it is required. The system is semantically in the standard model while previous systems are semantically secure in the random oracle model (ROM). IBE allows for a party to encrypt a message using the recipient's identity as a public key. The ability to use identities as public keys avoids the need to distribute public key certificates. This can be very useful in applications such as email where the recipient is often off-line and unable to present a public key certificate while the sender encrypts a message. The scheme can be converted to an efficient signature scheme that depends

R.Ilakkiya , M.E., Computer Science and Engineering Student, M.I.E.T Engineering College, Trichy, (Email : ilakkiyaravichandran@gmail.com)
R.Senthamil Selvi , Associate Professor, Department of CSE, M.I.E.T Engineering College, Trichy, (Email : vijai.sen@gmail.com)

only upon the computational diffie-hellman assumption in the standard model. Proposed the first anonymous

IBPRE with chosen cipher text (CCA) security in the ROM. In the context of IBE some well known systems supporting anonymity, IBPRE leveraging them may partially fulfil our goals.

B. Contributions

Introduce an algorithm for identity based proxy reencryption (IBPRE), it is a cryptographic method developed to delegate the decryption right from one party to another. It is a type of PRE scheme in the identity based public key cryptographic setting. This scheme is a natural extension of PRE. It supports oneto-many encryption. It has been used for secure cloud data sharing and related key management. The scheme is an extended IBE scheme. The first extension is an algorithm that generates re-encryption keys that can be given to the proxy. The proxy uses the second algorithm to apply these re-encryption eysto cipher texts and "atomically" reencrypt them from one identity to another. In a non interactive scheme, re-encryption keys may be generated by the delegator using only IBE secret key the IBE master secret is not required. PRE has a number of practical applications. All of these applications translate directly to the identity based setting but with some additional features. Our definitions refer to the notion of an "encryption level" as an implicit property of a cipher text. A cipher text generated directly using the encrypt algorithm is termed a "level-1" cipher text. Recently, many IBPRE schemes have been proposed. However, all of these schemes are only proved secure in the random oracle not in the standard model. This application translates naturally to the identity based setting with the additional benefit of allowing the holder of the master key to specify access control policies directly within the identity strings of the users. A reencryption key can even be generated before an individual has joined the system.

By introducing the concept of multi-hop identity based proxy re-encryption (MH-IBPRE) that maintains the cipher text size and computational complexity regardless of the number of re-encryption hops. Moreover, our scheme is bidirectional and also supports conditional re- encryption. The scheme is proven secure against identity and chosen cipher text attacks and collusion resistant in the standard model. Given a cipher text, the receiver of the cipher text can be updated in multiple times so implement to this property as "multi-hop". A cipher text can be finegrained shared with others if the pre-specified conditions are satisfied. No one knows the identity information of sender and receiver.

II. SYSTEM MODEL

System design is the process of defining the architecture, components, modules, and data for a system to satisfy specified requirements. One could see it as the application of systems theory of product development. There is some overlap with the disciplines of system analysis, systems architecture and systems engineering. If the broader topic of product development blends the perspective of marketing, design, and manufacturing into a single approach to product development, then act of taking the marketing information and creating the design of the product to be manufactured. System design is therefore the process of defining and developing systems to satisfy specified requirements if the user.

A. Encrypted Data Upload to Cloud Server

A basic security requirement of big data storage is to guarantee the confidentiality of the data. Fortunately, some existing cryptographic encryption mechanisms can be employed to fulfil the requirement. PRE allows a data sender to encrypts the data under the public key of receiver such that no one except the valid recipient can gain access to the data. Nevertheless, this does not satisfy all the requirements of users in the scenario of big data storage. Hospital stores its patient's medical records in a cloud storage system and meanwhile, the records are all encrypted so as to avoid the cloud server from accessing to any patient's medical information. After a record is encrypted and further uploaded to the cloud, only those specified doctors can gain access to the record. A huge amount of consumed data of each companies located inside the company will be automatically transferred to the authority via internet period by period. The corresponding medical record then needs to be converted to the cipher texts corresponding to various receivers so as to be shared among the departments. Therefore, the update of cipher text recipient is desirable.

B. Multiple Receiver-Anonymity

Given a cipher text, no one knows the identity information of sender and receiver. As to the security model of anonymity, it is complicated in the sense that categorize the medical departments into two sub departments. One is the anonymity for delegator the other is the anonymity of re-encryption key. The medical record owner, e.g., the patient, has rights to decide who can gain access to the record, and which kinds of data are allowed for access. The patient can choose to specify that only the medical record described with "department1" can be read by a dep1 admin only. This fine-grained control prevents a data sharing mechanism from being limited to the "all-ornothing" share mode. Moreover, a patient might be transferred to more than one medical department in different treatment phases.

C. Conditional Sharing

Cipher text can be fine-grained shared with others if the pre-specified conditions are satisfied. To hide the information leaked from re-encryption key, the notion of key privacy. To prevent a cipher text from being traced, proposed a unidirectional IBPRE scheme in which an adversary cannot identify the source from the destination cipher text. To ensure the privacy of both delegator and delegate, proposed the first Anonymous PRE (ANO-PRE) system.

D. Fine Grained Proxy Re-encryption

PRE is proposed to tackle of dilemma of data sharing. It allows a semi-trusted party, called proxy, to transform a cipher text intended for a user into a cipher text of the same message intended for another user without leaking knowledge of either the decryption keys or the message. The workload of data owner is now transferred to the proxy, and the "online all the time" requirement is unnecessary.

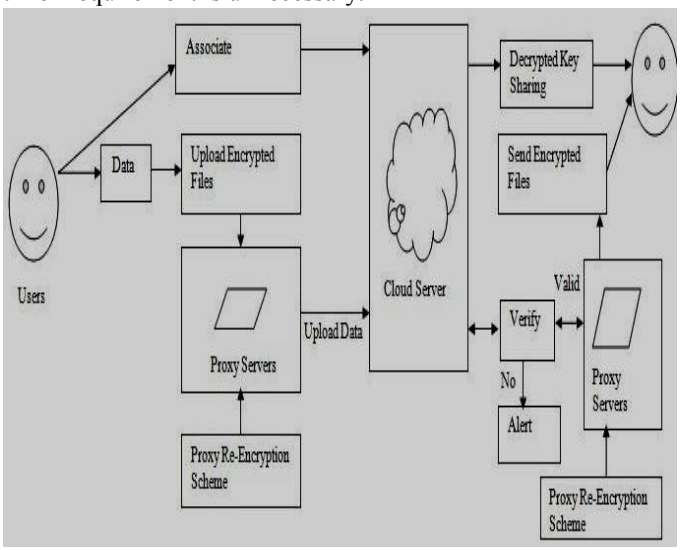

Fig. 2. System Architecture

III. ERFORMANCE EVALUATION

We proved a novel notion, anonymous multi-hop identitybased conditional proxy re-encryption to preserve the anonymity for cipher text sender/receiver, conditional data sharing and multiple recipients updates. This system satisfies the basic requirement of privacy i.e., confidentiality of data. Meanwhile, we proved the system CCA-secure in the standard model under the decisional *p*-bilinear Diffie-Hellman assumption.

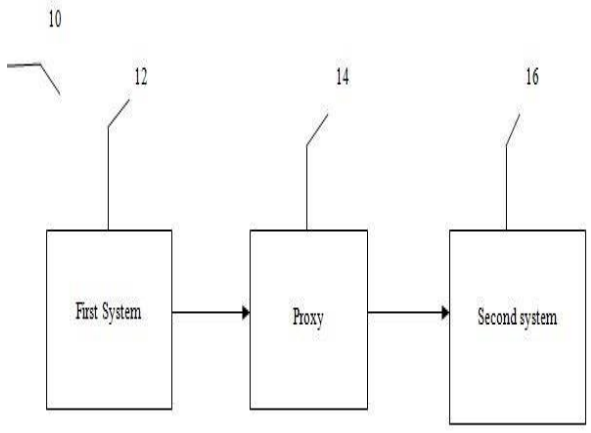

Fig. 3. Proxy Re-Encryption

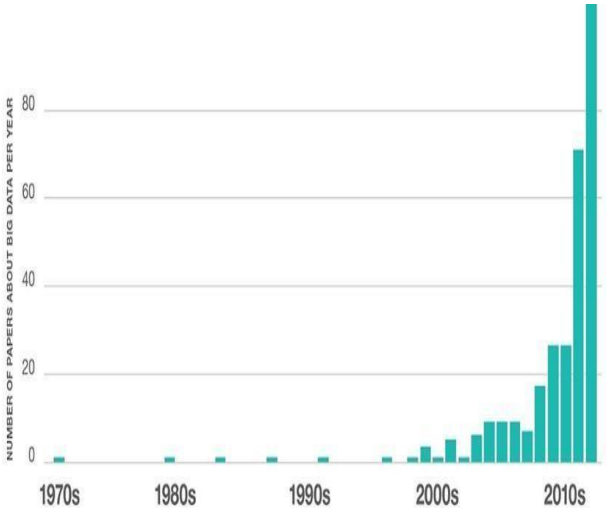

Fig. 4. Increase In Research Into Big Data

IV. CONCLUSION

Implement its patients medical records for hospital application in a cloud storage system and meanwhile, the records are all encrypted so as to avoid the cloud server from accessing to any patient's medical information. After a record is encrypted and further uploaded to the cloud, only those specified doctors can gain access to the record. This work concentrates on the identity-based cryptographic setting, and secure email with IBE. To capture privacy-preserving property and cipher text's recipient update simultaneously.

Anonymous multi-hop identity-based conditional proxy reencryption, to preserve the anonymity for cipher text sender/receiver, conditional data sharing and multiple recipients update and proposed a concrete system for the notion, proved the system under CCA-secure in the standard model the decisional. We further proposed a concrete system for the notion.

FUTURE ENHANCEMENT

Plan to future and implement real time application for hospital stores its patient's medical records in a cloud storage system after a record is encrypted and further uploaded to the cloud, only those specified doctors can gain access to the record. Analyse and overlook the practical errors and adversary collusions. The work concentrates on the identitybased cryptographic setting, and secure email with IBE. With the help of this proposed paper, we can upload large real data in the cloud with the privacy and security.

REFERENCES

[1] Ateniese G., Benson K. and Hohenberger S. CryptologyCT-RSA, vol. 5473. Berlin, (2009), 'Key-private proxy re-encryption', in Germany: SpringerVerlag, pp. 279-294.

[2] Blaze M., Bleumer G. and Strauss M. (1998), Cryptography. 'Divertible protocols and atomic proxy cryptography', in Advances in Cryptology. Berlin, Germany: Springer-Verlag,pp. 127-144.

[3] Boneh D. and Boyen X. (2004), 'Effcient selectiveID secure identity-based encryption without random oracles', in Advances in Cryptology-EUROCRYPT, vol. 3027. Berlin, Germany: Springer-Verlag, pp. 223-238.

[4] Green M. and Ateniese G. (2007), 'Identity-based proxy re-encryption', in Applied Cryptography and Network Security vol. 4521. Berlin, Germany: Springer-Verlag, pp. 288-306.

[5] Liang K., Au M.H., Susilo W., Wong D.S., Yang G. and Yu Y.(2014), 'An adaptively CCAsecure ciphertext-policy attribute-based proxy reencryption for cloud data sharing', in Information Security Practice and Experience vol. 8434. Berlin, Germany: Springer-Verlag,pp. 448-461

[6] Mambo M. and Okamoto E. (1997), 'Proxy cryptosystems: Delegation of the power to decrypt ciphertexts', IEICE Trans. Fundam. Electron., Commun., Comput. Sci., vol. E80-A, no. 1, pp. 54-89

[7] Shao J. (2012), 'Anonymous ID-based proxy reencryption', in Information Security and Privacy vol. 7372. Berlin, Germany: SpringerVela,2012,pp.364 - 375.

[8] Waters B. (2009), 'Effcient identity-based encryption without random oracles', in Advances in CryptologyEUROCRYPT vol. 3494. Berlin.

[9] Waters B. (2009), 'Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions', in Advances in Cryptology-CRYPTO vol.5677. Berlin, Germany: Springer. Libert B and Vergnaud D (2009), "Unidirectional chosen-cipher text secure proxy re-encryption".

[10] T. Matsuo,"Proxy re-encryption systems for identity based encryption," in Pairing-Based Cryptography.