ISSN:0975-9646

Survey on Cryptographic Schemes for Security in Cloud Data Storage

Mounesh[#1], Pandurang.D.R[#2], Basavaprabhu[#3], Sagar V[#4] ,Shyamala G[#5]

Department of Computer Science and Engineering,
BMS College of Engineering, VTU University,Basavanagudi, Bangalore, India

***Abstract*—A Cloud data storage system consists of collection of storage servers over the internet which provides long term storage services. The data stored in a third party's cloud system may cause serious concern over data confidentiality. To keep sensitive user data confidential against un-trusted servers and to provide security, access control in cloud there are some cryptographic techniques specially used for secure cloud storage. The data shared over network need to be encrypted. To provide security and access control over the network there are many encryption schemes. In this paper, we analyze and explore the different type of data encryption techniques available for cloud security such as identity proxy re-encryption, Key private proxy re-encryption, Attribute based proxy re-encryption, Type based proxy re-encryption. Identity based proxy re-encryption and Threshold proxy re-encryption.**

***Keywords*— cloud security, proxy re-encryption,_identity Based Proxy Re-encryption Scheme, MH-IBPRE**

I. INTRODUCTION

Cloud computing is a kind of internet based computing, where shared resources, data and information are provided to computers. Over the network the cloud computing resources (hardware, software) are delivered as service. Users can access the information and resources when a network connection is available. All data and business information are stored on distributed servers at remote location in cloud computing. The remote locations are data centers. The client can purchase or he can rent, such as processing time, network bandwidth, disk storage and memory. The data owners can remotely store their data in the cloud and no longer posses the data locally. Cloud computing moves the application software and database to the large data centre, where the data management and services may not fully trustworthy. A cloud storage system is consists of many independent storage servers because of distributed storage system. These independent storage servers can store data over long periods of time. The stored data can be accessed a large number of times and it may be chances to changes. The main factor of cloud storage servers is that, it rises to a number of security threats. Cloud applications may require all standard security functions including data confidentiality, integrity, privacy, robustness and access control. To providing security to the cloud is the challenging. There are several cryptographic techniques to secure the data stored in cloud storage. In this paper different encryption technique are proposed.

II. IDENTITY-BASED ENCRYPTION

The concept of IBE (identity-based encryption) proposed was by Shamir [1]. In this new type of cryptography, user identifier information can be email or IP addresses. Instead of digital certificates email or IP addresses can be used as public key of the user, using this as identity of the user PKG(Private key Generator) is called as trusted third party. The PKG can generate private key of the user using identity of the user. The receiver can use this private key to decrypt. PKG generate private key with corresponding public key. The identity based encryption is promising for overcoming issues like symmetric and asymmetric key scheme and IBE has some issue revocation problem. The essential property of IBE is that the user encrypt using their email address as public key but there is a potential issue if the private key is compromised. This means a user cannot use their email address as public key any longer. The Identity Based Encryption scheme is very promising for overcoming issue associated with symmetric and asymmetric key management schemes.

III. PROXY RE ENCRYPTION SCHEME

The proxy re-encryption scheme is proposed by mambo [2] and blaze et al.[3]. Proxy re-encryptions is another cryptographic scheme which translate the one encryption key to another encryption key of cipher text. Proxy re-encryption is be used to send messages (cipher text) without having to expose the plain text to the potential users. The re-encryption should be key independent because to avoid compromising the private key of sender and the receiver. The main advantage of proxy re encryption[4] is that they are unidirectional and don't require delegators to reveal entire secret to anymore (i.e. A can delegate to B without B having to delegate to her). A proxy re encryption algorithm transforms the cipher text under public key pk1 to cipher text pk2 by using re encryption scheme RK12, so the server does not know the corresponding text, where pk1 and pk2 can only be decrypted by different key K1 and K2 respectively and it is very secure against plain text attack. The proxy re encryption schemes has many applications like email forwarding, secure network file storage, etc. The advantage of PRE is it provides security against plain text attack. The disadvantage of this scheme is that it has collusion problem, means PRE allows a proxy to convert a cipher text encrypted for delegator into a cipher text for delegatee by sing re encryption generated by sender. Non transferability is a desirable property of PRE that colluding proxies and delegatees cannot re-delegate decryption rights to a malicious user.

IV. IDENTITY BASED PROXY RE-ENCRYPTION SCHEME

Identity Based Proxy Re-encryption Scheme was first proposed by Shamir [5]. In this identity based PRE scheme, user identity such as email addresses or the IP address can be used to create public keys for users (sender and receiver). In identity based encryption, the senders can encrypt messages by using the receiver identity (string) as used as public key. For example, A (sender) could encrypt a message for B (receiver) by just using his email address [6]. Here in this scheme the proxy can transform the message with proxy key or re encryption key. And it performs the translation without knowing the plaintext. This scheme allows translating an encryption under receiver identity into one computed under sender identity

V. ATTRIBUTE BASED PROXY RE-ENCRYPTION SCHEME

Sahai and Waters [7] introduced the attribute based proxy re-encryption scheme. In this proxy re encryption scheme, a semi trusted proxy server with some additional information can transform a cipher text under a some set of attributes into a new cipher text under a set of attributes into a new cipher text under another set of attributes on the same message. This encryption scheme, allows us to fine-grained access control on encrypted data. Attribute based encryption is a generalization of Identity Based Encryption. Goyal [8] introduced the two kinds of ABE one is cipher text policy attribute based encryption (CP-ABE) and another one is key policy attribute based encryption (KP-ABE). This scheme provides fine-grained access control on encrypted data. But it has Average efficiency and flexibility.

VI. TIME BASED PROXY RE-ENCRYPTION SCHEME

Qin Liu, Guojun Wang, Jie Wu, proposed the Time based Proxy Re Encryption scheme to provide fine-grained access control and scalable user revocation in cloud data storage [9]. This scheme allows every user's access right to be in a pre determined time period, and enables the (cryptographic service provider) CSP to re-encrypt the cipher text automatically, based on its own time. This scheme don't allow data owner to be every time online in the process of user revocations. Disadvantage of this scheme is that, it requires the time periods to be the same for all the attributes associated with a user.

VII. KEY PRIVATE PROXY RE-ENCRYPTION SCHEME

The Ateniese et al. [4] was proposed the key private proxy re-encryption scheme. In a key private proxy re-encryption it is not possible for the proxy and a set of colluding users to derive the recipient of a message from the cipher text and the set of public keys. To Achieve the key private proxy re-encryption[11] is only possible when the underlying encryption scheme is key-private and the key privacy encryption also provides privacy of the key under which the encryption scheme was performed. It is a very efficient, simple, and also secure under basic assumptions of bilinear groups in the standard model. But In this they didn't consider about the key privacy. For that types of collusions and interactions may appear to break the security of the construction

VIII. TYPE BASED PROXY RE-ENCRYPTION SCHEME

The type based proxy re-encryption schemes are proposed by Tang[12]. The type based proxy re-encryption scheme is to implement the fine grained policies with one key pair without any additional trust on the proxy. Some properties of KP-PRE scheme are below given. The delegator only needs one key pair so that key management problem can be simplified. The receiver can choose the particular proxy for a specific delegate, which might be based on the sensitiveness of the delegation. The advantages of KP-PRE is Semantic security and cipher text Privacy Control but encoding operations over encrypted messages is not possible

IX. CONDITIONAL PROXY RE-ENCRYPTION SCHEME

The Conditional proxy re-encryption (C-PRE) was proposed by Jean Weng and others [13]. The Conditional -PRE scheme has three principles: a Delegator, a Proxy and a Delegatee. A message was sent to delegator (receiver) with a condition w is encrypted by the sender using both delegator (receiver) public key and condition w. To re-encrypt the message to delegate the proxy is given the re-encryption key and also the condition key (cki, w) corresponding to w. Both the keys can be generated only by delegator. So these two keys form the secret trapdoor used by the proxy to perform cipher text translation of encryption. Conditional Proxy Re-encryption Scheme is very secure against chosen cipher textattack (CCA).But it is difficult to design CCA secure conditional proxy re-encryption.

X. THRESHOLD PROXY RE-ENCRYPTION SCHEME

The main approach of the threshold Proxy Re-Encryption scheme is [14] for secure computation. It has a multiplicative homomorphic property. This property is supports the encoding operation over encrypted messages. And forwarding operation over encrypted messages and encoded messages. Threshold PRE scheme has a three properties, Homomorphism, Proxy re-encryption, Threshold decryption Homomorphism means if Given two cipher texts c1 and c2 on plaintexts p1 and p2 respectively, one can obtain the cipher text on the plaintext p1+p2 and/or p1, p2 by evaluating c1 and c2 without decrypting Cipher texts. Proxy re-encryption means Transforming encrypted data of one user to encrypted data of target user. Threshold decryption means by dividing the private key into several pieces of secret shares, all clients can work together to decrypt the cipher text – the output of the function. Advantage of this scheme is data forwarding. But it has very high access control

XI. IMPROVED PROXY RE-ENCRYPTION SCHEMES WITH APPLICATIONS TO SECURE DISTRIBUTED STORAGE

The proposed application is called atomic proxy re-encryption, in which a semi-trusted proxy without seeing the underlying plaintext converts a cipher text for delegator into a cipher text for delegatee. We predict that fast and secure encryption will become increasingly popular for managing encrypted file systems. Although efficiently computable, BBS re-encryption is wide-spread adoption

that has been hindered by considerable security risks. G. Ateniese, K. Fu, M. Green, and S. Hohenberger [15], present new re-encryption schemes Improved proxy re-encryption schemes with applications to secure distributed storage, that provide a stronger notion of security and a method of adding access control to a secure file system it is demonstrate the usefulness of proxy re-encryption. Advantages are, they use a centralized access control server to manage access to encrypted content stored on distributed, un trusted replicas, they use proxy re-encryption to allow for centrally-managed access control without granting full decryption rights to the access control server. The Disadvantages are, secure even when the proxy publishes all the re-encryption information it knows, the main drawback of the process is it would not be practical if the proxy needed to be fully trusted.

XII. EFFICIENT SELECTIVE-ID SECURE IDENTITY-BASED ENCRYPTION WITHOUT RANDOM ORACLES

In this, they construct two efficient Identity Based Encryption systems that are selective identity secure without the random oracle model[16] in groups equipped with a bilinear map and Selective identity secure IBE is a slightly weaker security model The first system is based on the decisional bilinear Diffie-Hellman assumption, and extends to show selective identity Hierarchical secure without random oracles. Advantages are IBE systems that are secure against selective identity attacks ,it is a selective-ID secure IBE system implies a fully secure IBE system the resulting security reduction is not polynomial. And the disadvantages are in this they use selective identity IBE, is a weaker security model, in this identity it intends to attack., and Selective- ID secure IBE can be turned into a fully secure IBE in the standard model.

XIII. IDENTITY-BASED ENCRYPTION FROM THE WEIL-PAIRING

Boneh and Franklin [11] were proposed the first secure and practical identity-base encryption (IBE) scheme based on pairing. They proposed a scheme with full functional identity based encryption scheme. This scheme had chosen cipher text security in random oracle model using the Diff-Hellman problem. Advantages is this scheme was a Very basic encrypting scheme and also this scheme was a first practical identity based encrypting scheme. But this scheme provides only encryption.

XIV. IDENTITY BASED SECURE DISTRIBUTED DATA STORAGE SCHEMES

Jinguang Han, Willy Susilo, and Yi Mu [16] proposed the Identity-Based Secure Distributed Data Storage Schemes. In previous scheme intra domain proxy cryptosystem was used which is the cloud based system. In this system users identity is string and there is two parties communicate with each other without checking public key. The advantages of this scheme is, the file owner can create the re-encryption key independently without interacting with packet key generator after authentication of user, this scheme provides collusion safe, collusion attack does not occur in this system and for one query user could get only one file, user can download one file for one request. It has also disadvantages like in this scheme, for providing better security, the owner of the data must have to be online for all the time to check the authenticated user and generate access permission for them.

XV. MULTI-USE UNIDIRECTIONAL IDENTITY-BASED PROXY RE-ENCRYPTION FROM HIERARCHICAL IDENTITY-BASED ENCRYPTION

Ateniese and Green proposed identity based proxy re-encryption (IBPRE), where a semi-trusted proxy with some information (re-encryption key), can transform a cipher text under an identity to another cipher text under another identity with the same plaintext. But the proxy cannot obtain plaintext. So Blaze et al. gave some methods to distinguish proxy re encryption schemes. The first one is according to the allowed times of transformation. If the encrypted message can be transformed from A to B, then from B to C, and so on, then the proxy re-encryption scheme is called multi use otherwise it is called single use. Another method is according to the allowed direction of transformation. If the re-encryption key can be used to transform the encrypted message from A to B, and also B to A then the proxy re encryption scheme is called bidirectional, otherwise, it is called unidirectional. Sometime the unidirectional is better than bidirectional PRE scheme. Example the delegator delegates his decryption rights to the delegatee; the delegatee does not always want to do the reverse delegation.In multi use identity based proxy re-encryption there are two security notions 1) CCA security and 2) collusion resistance.

XVI. RECIPIENT ANONYMOUS CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION

Attribute based encryption is a promising and increasingly versatile paradigm. given the many potential uses of ABE schemes constructing efficient schemes that provides recipient anonymity via policy hiding while ensuring constant size secret key and cipher text with strong security notion is a challenging task. ciphertext-policy(CP-ABE)scheme [18] using and AND-gate access policy. The secret key size, ciphertext size and computation costs are all constant in this scheme. This work proposes the first fully secure recipient anonymous CP-ABE scheme whose secret key size, ciphertext size and computation cost are all constant regardless of the number of underlying attributes

XVII. CHOSEN-CIPHER TEXT SECURE MULTI-HOP IDENTITY-BASED CONDITIONAL PROXY RE-ENCRYPTION

Public Key Encryption (PKE) is one of the useful cryptographic primitive, where it allows a user to encrypt the data under the public key of a receiver such that only the authorized receiver with the respective private key can be used to access the data. In some social networks, a data is often shared among different users. For example a user A can share a data, like audio, video or picture with his friend say B without the loss of confidentiality by using PKE. Sometimes, B might choose to further share the same data with another user, say C. In the context of PKE, B should

first decrypt the cipher text of the data sent by A, and next re-encrypt the data to C, so as to finish data sharing. But this is does not scale well when B is off-line or unavailable. PRE comes to two kinds: The first one is single-hop PRE, and the second one is multiple-hop PRE. If a encrypted message can be re-encrypted from A to B and we cannot be further converted, the scheme is called single hop. But in multi-hop scheme a encrypted message can be re-encrypted from A to B and to C, and so on. So it provides the flexibility of re-delegation, i.e., the receiver can re-delegate the cipher texts to another users. Green and Ateniese [17] proposed the multi-hop identity-based proxy re-encryption (MH-IBPRE), in Proxy re-encryption scheme. The applications are group data sharing and multi device data sharing.

The proxy re-encryption scheme is proposed by mambo [2] and blaze et al.[3]. Proxy re-encryptions is another cryptographic scheme which translate the one encryption key to another encryption key of cipher text. Proxy re-encryption is be used to send messages (cipher text) without having to expose the plain text to the potential users. The re-encryption should be key independent because to avoid compromising the private key of sender and the receiver. The main advantage of proxy re encryption [4] is that they are unidirectional and don't require delegators to reveal entire secret to anymore (i.e. A can delegate to B without B having to delegate to her). A proxy re encryption algorithm transforms the cipher text under public key pk1 to cipher text pk2 by using re encryption scheme RK12, so the server does not know the corresponding text, where pk1 and pk2 can only be decrypted by different key K1 and K2 respectively. And it is very secure against plain text attack. The proxy re encryption schemes has many applications like email forwarding, secure network file storage, etc. The advantage of PRE is it provides security against plain text attack. The disadvantage of this scheme is that it has collusion problem, means PRE allows a proxy to convert a cipher text encrypted for delegator into a cipher text for delegatee by sing re encryption generated by sender. Non transferability is a desirable property of PRE that colluding proxies and delegatees cannot re-delegate decryption rights to a malicious user.

BRIEF REVIEW OF ENCRYPTION SCHEMES

Encryption Scheme	Advantages	Disadvantages
1. Identity based encryption	No certificates needed. A recipient's public key is derived from his identity .No pre enrollment required.	Requires a centralized server. Requires a secure channel between a sender or recipient and the IBE server for transmitting the private key.
2. Proxy re encryption scheme	PRE is secure against plain text attack	Collusion problem and Plaintext attack
3. Identity based proxy re encryption scheme	Secure against an adaptive Chosen cipher text attack.	Difficult to find efficient Constructions for multiuse CCA-secure IBE-PRE.
4. Attribute proxy re encryption scheme	Fine-grained access control on encrypted data	Average efficiency and Flexibility.
5. Time based proxy re encryption	Reduce the workload of the data owner.	Requires effective time period to be the same for all attributes associated with the user.
6. Key private proxy re encryption scheme	Provides CCA security.	The key privacy proof is more difficult than that of CPA security.
7. Type based proxy re encryption scheme	Semantic security and Cipher text Privacy Control.	Encoding operations over encrypted messages is not possible.
8. Conditional proxy re encryption	Security against chosen Cipher text attack.	It is difficult to design CCA secure C-PRE scheme.
9. Threshold proxy re encryption scheme	Data Forwarding.	High access control.
10. Improved proxy re encryption scheme with applicants to secure distributed storage	They use proxy re Encryption to allow for centrally-managed access control without granting full decryption rights to the access control server.	The main drawback of the process is it would not be practical if the Proxy needed to be fully trusted.
11. Efficient selective-ID secure identity based encryption without random oracles.	This system implies a fully secure IBE system and secures against selective identity attacks.	Selective –ID secure can be turned into fully secure IBE in the standard model, at the cost of an inefficient security reduction.
12. Identity based encryption from the weil-pairing.	This was a Very basic encrypting scheme And this was a first practical identity based encrypting scheme.	This scheme was provides only encryption.
13. Identity based secure Distributed data storage scheme.	This scheme is collusion safe, collusion attack in not possible in this system. The file owner generates the re-encryption key independently without interaction with PKG after authentication of user.	In this scheme, for providing better security to the system, the data owner must have to be online for all the time to check the authenticated user and generate access permission for them.
14. Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption.	It is including efficient forward secure encryption.	There is a large time taken for encryption and decryption.
15.Recipient anonymous cipher text policy attribute based encryption	It is more efficient anonymous identity based encryption scheme with more light weight key derivation protocols would translate directly into highly efficient PEOKS.	It is a weaker security model for generating the keys.

XVIII. CONCLUSIONS

Security in cloud computing is an important aspect of quality of service. To keep the sensitive user data confidential against un-trusted servers several proxy re-encryption techniques are used. This paper reviews different proxy re-encryption schemes used in cloud storage system. The merits and demerits of the algorithms have been studied. The future work will be concerned with the development of better PRE schemes which works in distributed environment and efficient utilization of these schemes to provide more security to the large data stored on the cloud network.

ACKNOWLEDGEMENTS

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES

[1] A. Shamir, Identity-based Cryptosystems and Signature Schemes, Proceedings of CRYPTO

[2] M. Mambo and E. Okamoto, "Proxy Cryptosystems: Delegation of the Power to Decrypt Cipher texts", IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, 1997, pp. 54-63.

[3] M. Blaze, G. Bleumer, and M. Strauss,"Divertible Protocols and Atomic Proxy Cryptography", Proc. Int'l Conf. Theory and Application of Cryptographic Techniques ,1998, pp. 127-144.

[4] G. Ateniese, K. Benson, and S. Hohenberger, "Key- Private Proxy Re-Encryption", Proc. Topics in Cryptology, 2009, pp. 279-294.

[5] Shamir, "A Identity-based cryptosystems and signatures schemes", In Advances in Cryptology, 1984, pp. 47-53.

[6] Matthew Green and Giuseppe Ateniese, "Identity- Based Proxy Re-Encryption", ACNS 2007, pp. 288-306.

[7] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption", Springer, 2005, pp. 457–473.6

[8] Goyal V, Pandey O, Sahai A, and Waters B , "Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data", In: ACM conference on Computer and Communications Security, 2006.

[9] Matt Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography", In Proceedings of Eurocrypt, 1998, pp. 127–144.

[10] MihirBellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval, "Key-privacy in public-key encryption", In ASIACRYPT, 2001, pp. 566-582.

[11] Q. Tang, "Type-Based Proxy Re-Encryption and Its Construction", Proc. Ninth Int'l Conf. Cryptology in India, 2008, pp. 130-144.

[12] JianWeng, Robert H. Deng, Xuhua Ding, Cheng- Kang Chu, and Junzuo Lai, " Conditional proxy reencryption secure against chosen-ciphertext attack", In ASIACCS,2009,pp. 322−332.

[13] GiladAsharov, Abhishek Jain, Adriana Lopez-Alt, EranTromer, VinodVaikuntanathan, and Daniel Wichs, "Multiparty computation with low communication, computation and interaction via threshold FHE", Proceeding EUROCRYPT'12, Springer, 2012,pp. 483-501.

[14] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed

[15] storage," in Network and Distributed System Security. Berlin, Germany: Springer-Verlag, 2005, pp. 29–43.

[16] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in Advances in Cryptology–EUROCRYPT (Lecture Notes in Computer Science), vol. 3027. Berlin, Germany: Springer-Verlag, 2004, pp. 223–238

[17] K. Liang, C.-K.Chu, X. Tan, D. S. Wong, C. Tang, and J. Zhou, "Chosen-ciphertext secure multi-hop identity-based conditional proxy re-encryption with constant-size ciphertexts," Theoretical Comput. Sci., vol. 539, pp. 87–105, Jun. 2014.

[18] Y. S. Rao and R. Dutta, "Recipient anonymous ciphertext-policy attribute based encryption," in Information Systems Security (Lecture Notes in Computer Science), vol. 8303. Berlin, Germany: Springer-Verlag, 2013, pp. 329–344.