Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Imparting Data in Cloud Storage Using Key Revocation Process

[1]R. Subbu lakshmi, [2]R. Nirmalan

[1]PG Scholar

[2]Asst. Professor

Dept of CSE, Sri Vidya College of Engineering and Technology,
Tamil Nadu, India

Abstract- Cloud computing is ideal for places where the data remain in a fixed environment, which are unavailable. Today imparting of data with security places is a major issue in cloud computing. For security issues key aggregate place a vital role to offer secured data transfer. This paper provides the various techniques and methodologies that can be used for security in revocation process and also new method proposed for data importing in cloud computing. To provide secure data sharing in cloud storage by using Key aggregation. In order to protect the sensitive information in the cloud storage the key revocation is used.

Keywords: cloud computing, data sharing, network security, and key revocation.

I. INTRODUCTION

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources likes network, server, application and service. Data is stored at the remote location and available on demand. It allows clients to use application without installation the file at any computer with internet facility. Features of cloud computing are resource pooling, on-demand service, broad network access, measured services, rapid elasticity, reduce cost of purchasing hardware and software. Cloud model is composed of five essential characteristics, three service models and four deployment models. Service model consists of software as a service, infrastructure as a service, and platform as a service. Deployment model consists of public cloud, private cloud, hybrid cloud. Data outsourcing user can get the information from anywhere more efficiently and has no burden on data storage and avoid extra expense on software, hardware and information resources and the maintenances and usage will be more efficient. The data storage is made public by sharing it on cloud. The data stored in the cloud are accessible anywhere and security is used for data confidentiality. Cloud services are provided by different cloud providers like Google, Microsoft, IBM, Amazon etc. cloud storage is used as a core technology of many online services for personal application. Nowadays it is easy to apply for free account creation for photo album, file sharing, face book and remote access. Cloud security and privacy of data are the major issue in cloud. The data in the cloud are subjected to attacks in either by hacker and provider. Analysis of attack in cloud computing such as network level attack, language and malicious program injection based attack, web application attack. The users impart data in the cloud with a secure authentication and authorization. The imparting of data is necessary to share the sensitive information in a secured environment. Imparting data poses several problem including privacy, data misuse and uncontrolled propagation of data. The data in cloud is placed in a share pool and breaches in data are the major evolution to security. Cryptography access control is one of the most used techniques to securing data storage on entrusted servers, where sensitive data has been encrypted before outsourcing and decryption keys are given only to authorized users. Without the decryption keys even the servers are not able to decrypt the data.

II. AUTHENTICATION AND KEY GENERATION

User is asked to keep this id as a secret because it is used as a tool to authenticate him every time he logs on to the system. Authentication merely ensures that the individual is who he (or) she pretends to be but says nothing about the access rights of the individual. Authenticated user has ID/password combinations to prove identity. Password authentication protocol, secure socket layer, digital signatures, Kerberos, firewall, virtual private networks are the techniques are used in authentication.

Fingerprint, voice, face, keyboard timing are the techniques used in authentication for biometric. Cipher class consists of Data owner's id, message and the master/public key of the data owner attributes. Using the master key, public key is generated and secret key is generated by doing the logical XOR operations. Ciphering algorithms are applied using the secret key, thus secured secret key is generated by Key aggregate cryptosystem.

The author in paper [9] describes the methodology about two efficient authentication and key agreement schemes or single server, and multi server environments but both juang's schemes have no ability of anonymity for the user. The user must transmit a message of user authentication to the server, and then server must be able to verify the identity of the user and give him the right of using permitted service. The user passes a password as a secret token to the server. First server checks the user identity if the password matches. The users identify the key distribution scheme with the ability of privacy protection but it is pointed out that it is less efficient because of using public key cryptosystem. Some criteria basically on security and efficient requirements, we are using the user's authentication and key management schemes with smart cards. The outcome will be criteria such as privacy protection, freely chosen password, low computation and communication cost, mutual authentication and session key agreements. The main metrics such as the privacy of users can be ensured and a user can freely choose his own password, the computation and even the communication cost is also very low. Servers and users can authenticate each other and it's generates the session key agreed by the server and the user, the proposed schemes are novel based schemes which do not have serious synchronization problem.

This is provable secure to realize the identity authentication, session key agreement, key update with entity secrecy and perfect forward secrecy [6]. In this, the authentication of entities are implemented based on the public key cryptography and secure dynamic one way accumulator and the cross domain property is also supported. Key management is more simple, since the identity number of an entity is used as its public key. The key management function is performed by security mediator as an online service. The collusions between cloud server and revoked users can be avoided as long as the key update protocol is honestly executed. The data owner can delegate key updates to the cloud servers without disclosing the access policy information, data contents, user attributes [5]. The key generation algorithm takes as input a set of attributes S and outputs a secret key that identifies with that set. The random number r € Z_p, and then random r_i €Z_p for each attribute i €S. then computes the secret key using Diffie Hellman Key exchange.

III. KEY AGGREGATION

Aggregate key is used for the secure data sharing over the distributed data sharing in cloud environment. Aggregate key consist of various derivation of identity and attribute based classes of respective data owner in the cloud. Aggregation key is used to sharing the data between one to other. The key aggregation property is especially useful when we expect the delegation to be efficient and flexible. Key aggregation enables content provider to share other's data in a confidential and selective way, with a fixed and small cipher text expansion, by distributing to each authorized user a single and small aggregate key. Alice wants to share her data on the server. The key generation phase is provided by public key and master key pair. In this public and master key pairs are secretly done by Alice. Alice encrypts the data using public key and these data are uploaded to the server. Alice is willing to share a data to bob. Alice can compute the aggregate key for bob, it's performed by master key, and this aggregate key is sent to bob via email and this aggregation key is used to download the data and decrypt the data. Extract is executed by the data owner for delegating the decrypting power for a certain set of cipher text classes to a delegate. In this example input is master key and data and output is aggregate key. It's the primary key having more than one column. Key aggregation is group of public key and private key used for transmission of data. The combination of public and private key is known as key aggregation. Key is nothing but composite or concatenated key. Example different books may have identical title, authors. In this case we can take title, author, and publication date as the aggregate key which acts as primary key. Map reduce function is also used in key aggregation. Advantage of key aggregation is such as a secure key cryptographic derivation, higher data security, supports data integrity process, and also easy to manage all the keys. For security issues key aggregation places a vital role to offer secured data transfer.

Cheng- Kang Chu, Sherman S.M et al, describe about we can aggregates any set of secret key and make them as compact as single key and can be conveniently sent to other or be stored in a smart card with very limited secure storage. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single key and the decryption power or any subset of cipher text classes. Key-policy ABE or KP-ABE the sender has an access policy to encrypt data using the Diffie–Hellman key exchange a core cryptographic mechanism for ensuring network security [6]. The privacy-preserving authenticated DHKE protocols named deniable Internet key-exchange both in the traditional PKI setting and in the identity-based setting, for key-exchange over the Internet both security and privacy are desired. The concepts of aggregate signatures are useful for reducing the size of certificate chains by aggregating all signatures in the chain) and for reducing message size in secure routing protocols such as SBGP (Secure BGP protocol).

The security models for such signatures and give several applications for aggregate signatures. Aggregate signatures are related to multi signatures. In these multi signatures, a set of users sign the same message and the result is a single signature. Aggregate signatures allow the compression of certificate chains without any additional signatures. We propose a perfect decentralized access control scheme with aggregate key encryption for data stored in cloud. This scheme provides secure data storage and retrieval [3]. This scheme is so powerful since we use aggregate encryption and string matching algorithms in a single scheme. A decentralized access control technique with aggregate key encryption combined with string matching algorithms provides user revocation and prevents replay attacks with high security. This matching aggregate key can be easily sent to others or be stored in a storage media with very limited secure storage. The system is based on attribute based encryption for Fine-Grained Access Control of Encrypted Data. Keep sensitive user data confidential against unauthenticated servers, existing schemes usually apply cryptographic methods by disclosing data decryption keys only to authorized users [8]. Key distribution is done in a decentralized way so that the keys can be managed easily with perfect security. The secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage.

IV. ENCRYPTION AND DECRYPTION PROCESS

Encryption process is define by plain text message is converted into cipher text message and decryption process is define by cipher text message is converted into plain text message. Various algorithms are used in encryption and decryption process such as data encryption standard (DES) and advanced encryption standard (AES), RSA algorithm.

Jin Li, Jingwei Li, Xiaoeng, Chunfu Jia and Wenjing Lou, et al, we are using the data encryption standard (DES) for encryption and decryption process. DES is also called as the data encryption algorithm. DES is a block cipher. It encrypts data in block of size 64 bits each and these 64 bits are used in input of the DES and these are produced by 64 bits of cipher text. In this algorithm we use in keys and these keys are used in encryption and decryption process. The key length is 56 bits. DES is based on the two fundamental attributes such as substitution (confusion) and transposition (diffusion). DES consists of 16 steps, each of which is called as a round. Each round performs the steps of substitution and transposition. Steps of DES, in the first step the 64 bits plain text passes through an initial permutation. The initial permutation is performed on plain text. Initial permutation produces two halves of the permuted block, such as left lain text and right plain text. Now each left plain text and right plain text goes through 16 rounds of encryption process. The outputs of last rounds are swapped to produce the preoutput. Finally the pre output is passed through a permutation that is the inverse of the initial permutation function to produce the 64 bit cipher text. There are five modes of encryption operations used. Modes of operation such as electronic code book mode, cipher block chaining mode, cipher feedback mode, output feedback mode, counter mode.

Cheng-Kang Chu, Sherman S.M, et al, [1] we use the advanced encryption standard (AES) which is a symmetric. AES is block cipher intended to replace DES for commercial applications. AES fall into three areas such as security, cost, and implementation. AES cipher is a non feistal cipher that encrypts and decrypts a data block of 128 bits. Uses 10, 12, 14 rounds, key size can be 128, 192, 256 bits, depends on the number of rounds.AES uses five units of measurement to refer to data such as bits, bytes, words, blocks and states. AES encryption and decryption process steps such as substitution bytes, shift rows, mix columns and add round key. Substitution byte, only one table is used for transformation o every byte, which means that if two bytes are the same and these transformation is also same. The transformation is defined by either a table lookup process or mathematical calculations. The sub bytes operation involves 16 independent byte to byte transformations. Mix columns operate at the column level it transforms each column of a state column by a constant square matrix. Shift rows is the another transformation used in encryption and the shifting is to the left side. The number of shifts depends on the row number(0,1,2,3) of the square matrix this means the row 0 is at all and the last row is shifted three bytes. Add round key is similar to mix columns in this respect, mix columns multiples a constant square matrix by each state column. Its add a round key with each state column matrix. It uses matrix addition.

In paper [9] we are using RSA encryption and decryption algorithm. RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number. The blocks must be less than (or) equal to $\log_2$ (n), block size is i bits, where $2^i<n<2^{i+1}$ Steps:

1. Select p, q p!=q
2. Calculate n= p*q $\Phi(n)= (p-1) (q-1)$
3. Select integer e, $\gcd(\phi(n),e)\equiv1$, $1<e<\phi(n)$
4. Calculate d, $d\equiv e^{-1}(\bmod (\phi(n)))$
5. Public key PU = {e, n} e=encryption
6. Private key PR = {d, n} d=decryption

V. KEY REVOCATION PROCESS

Revocation is an act of recall or annulment. Revocation is performed by some operation in cryptosystem such as public key infrastructure and certificate revocation list. In this certificate revocation list there will be a list of certificates that are revoked. The function of revocation is performed by identity based encryption system and using key management. In this identity based encryption can support more entities than public key infrastructure while applied to the complicated system such as the cloud computing. The authentication system can be deployed in different ways such as centralized manner and distributed manner. The Key revocation process is needed when sensitive data is placed on the cloud storage. Data retrieved process not only consist o retrieved of encrypted files from the cloud server and decrypted using respected private keys, but these data are provided to the users upon the authentication of the hierarchical access control of cloud system architecture. Key revocation refers to the task of securely removing compromised keys. Data (or) keys are revocated in the cloud frequently depending upon the kinds of data owner's identity and the data to be stored on the cloud. Revocation event occurs the data owner redefines the master key component and public key component corresponding to variable attribute and then re encrypt the data using the new public key component.

In paper [5] describe about the Key revocation, how to remove secrets that may have been compromised. Revocation mechanisms are known in identity based encryption such as renew their private key periodically and senders use the receivers identities concatenated with current period. In this mechanism would result in an overhead load in public key generator. Revocation scheme is based on one way accumulator tool has both the one way and quasi commutative property, based on strong RSA assumption. Modified cipher policy attribute based encryption to setup a fine grained access control method in which user revocation is achieved based on the theory of Shamir's secret sharing. User revocation is challenging issue in this attribute based encryption. To reduce the cost for secret key updates, the cloud servers perform a lazy update, which means the users' secret keys are only updated when they setup a legal request. To provide a seamless integration between the revocation and tracing so that the tracing mechanisms do not require any change to the revocation algorithm. The revocation algorithm run by public key generator takes as input, is such as a revocation list, a time list and set of identities to be revoked and its output is such as update revocation list and time list.

H. K. Maji, M. Prabhakaran, and M. Rosulek, describe about Key-policy ABE or KP-ABE the sender has an access policy to encrypt data using the Diffie–Hellman key exchange a core cryptographic mechanism for ensuring network security. Develop a family of privacy-preserving authenticated DHKE protocols named deniable Internet key-exchange both in the traditional PKI setting and in the identity-based setting. For key-exchange over the Internet both security and privacy are desired. The concepts of aggregate signatures are useful for reducing the size of certificate chains by aggregating all signatures in the chain) and for reducing message size in secure routing protocols such as SBGP (Secure BGP protocol). The privacy of users can be ensured and a user can freely choose own password and the computation and communication cost is very low. It generates a session key agreed by the server and the user.

The author in paper [13], Revocation mechanisms such as certificate revocation list, certificate revocation status, online certificate status protocol, certificate revocation tree, security mediator. The Key revocation process is needed when sensitive data is placed on the cloud storage. Data retrieved process not only consist of retrieved of encrypted files from the cloud server and decrypted using respected private keys but the data are provided to the users upon the authentication of the hierarchical access control of cloud system architecture. Revocation mechanisms are known in identity based encryption such as renew their private key periodically and senders use the receivers identities concatenated with current period. In this mechanism would result in n overhead load in public key generator.

The author in paper [9], introduced the concept of revocation. Revocation is an act of recall or annulment. Revocation list is performed by some operation in cryptosystem such as public key infrastructure and certificate revocation list. In this certificate revocation list there will be a list of certificates are revoked. Main use of revocation is unspecified, key compromise, certificate authority compromise, affiliation changed, superseded, cessation of operation, certificate hold, remove from certificate revocation list, privilege withdrawn. Main function of revocation is performed by identity based encryption system and using key management. In this identity based encryption can support more entities than public key infrastructure while applied to the complicated system such as the cloud computing. Authentication system can be deployed in different ways such as centralized manner and distributed manner.

VI. CONCLUSION

Overall we produce an aggregate key Cryptosystem which produces effective constant size private key by means of derivations of different cipher text classes. Proposed approach proves to be more secure and efficient cryptographic scheme in which we have an effective derivation of secret key generation and key management for the outsourced Cloud data. Using blowfish algorithm will certainly increase security and also provide privacy of data. This algorithm is used for user friendly process and manner. Modification of blowfish algorithm is used to make secret key in that process, and it also allows only the authorized person to access the data at correct time.

REFERENCE

[1] Cheng-Kang Chu, Sherman S.M.Chow, Wen-Guey Tzeng, jianying Zhou,"key aggregate for Scalable Data Sharing in Cloud storage ", vol 1045-92 2013.

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy Preserving Public Auditing for Secure Cloud Storage," *IEEE Trans.Computers, vol. 62, no. 2, pp. 362–375, 2013.*

[3] S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE-Simple Privacy-Preserving Identity-Management for Cloud Environment," in *Applied Cryptography and Network Security - ACNS2012, ser. LNCS, vol. 7341. Springer, 2013, pp. 526–543.*

[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.

[5] Jin Li, Jingwei Li, Xiaoeng,Chunfu Jia and Wenjing Lou," Identity based Encryption with outsourced Revocation in cloud computing", vol0018,2013

[6] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in *Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser.*LNCS, vol. 6805. Springer, 2013, pp. 442–464.

[7] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," *ACM Transactions on Information and System Security (TISSEC), vol. 12,* no. 3, 2013;.

[8] T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu, "Identity Based Encryption Resilient to Continual Auxiliary Leakage," in *Proceedings of Advances in Cryptology - EUROCRYPT '12,* ser. LNCS, vol. 7237, 2012, pp. 117–134.

[9] Jashnapreet pal kaur, rajbhupinder kaur, "security issues and use of cryptography in cloud computing", in international journal of advanced research in computer science engineering-volume 4, issue 7, july 2012.

[10] Nagamalleswara rao.dasari, vuda sreenivasaro, " performance of multi server authentication and key agreement with user protection in network security", volume 02, No. 05,2010, 1705-1712.

[11] Neha tirthani, Ganesan R,"Data security in cloud architecture based on Diffie Hellman and Elliptical Curve Cryptography", volume 8, 2010,

[12] L.Arockiam, S. Monikandan,"Data Security and Privacy in cloud storage using hybrid symmentric encryption algorithm" volume 2, issues 8, 2010;

[13] H. K. Maji, M. Prabhakaran, and M. Rosulek, ―Attribute-based signatures: Achieving attribute-privacy and collusion-resistance,‖ IACR Cryptology ePrint Archive, 2008.

[14] D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," in *Proceedings of Advances in Cryptology - CRYPTO '01*, ser. LNCS. Springer, 2001, pp. 41–62.

[15] Rashmi Nigoti, Manoj Jhuria Dr.Shailendra Singh," A survey of Cryptography algorithm for cloud computing", IJETCAS 13-123 2001.