IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.
www.ijiset.com
ISSN 2348 - 7968

Amalgam Attribute Based Encryption Scheme over the Cloud Data for Secure Access in the Hybrid Cloud

Raj Priyadarshini. R[1] and Kanchanadevi. P[2]

[1] **Department Of Computer Science and Engineering, Alpha college of Engineering & Technology, Pondicherry, Pondicherry, India**

[2] **Department Of Computer Science and Engineering, Alpha college of Engineering & Technology, Pondicherry, Pondicherry, India**

Abstract

In the emergence of cloud computing, data owners are aggravated to outsource their complex data management system from local site to commercial cloud for great flexibility and economic saving. But for protecting data privacy, sensitive data has to be encrypted before outsourcing to commercial public cloud. Encrypted cloud data search system remains a very challenging task because of inherent security and privacy obstacles. There are so many security issues over the hybrid cloud during migration of data from one site to public cloud and also we cannot handle group of receivers in case of SKE. For secure communication and also handle dynamic attributes with continuous values, we need a new technique called as Amalgam attribute based encryption techniques. It is amalgam, as it combines the cipher text –policy attribute-based encryption (CP-ABE) with location-based encryption (LBE) on the level of symmetric keys in the hybrid cloud.

Keywords: *SKE, MRSE, CP-ABE, LBE, Hybrid cloud.*

1. Introduction

The word "cloud" was originate from the computer network Schemas which use it to hide the complexity of communication involved [1]. Cloud computing relies on sharing of resources to achieve coherence and economic of sales, similar to usefulness over a network. Cloud users can distantly store their data into the cloud so as to enjoy the features including resource group, rapid suppleness measured service, on-demand self service and broad network access. Cloud computing customers use cloud templates to move application between clouds through a self-service gateway. The predefined blueprints define all that an application requires to run in different environments. For greater flexibility and economic saving the cloud consumers use cloud templates to move application between clouds templates to move application between clouds through a self-service portal. The predefine blueprints define all that application required to run in different environments. For great flexibility and economic saving the cloud consumers are encouraging to outsource their local complex data management system into cloud, especially when the data produced by them that need to be stored and utilized is rapidly increased. The improved use of cloud computing services has pressed the issue of privacy concerns of cloud computing services to the utmost important. Cloud computing has developed from being a hopeful business concept to one of the fastest growing sections of the many industry. Now, slump-hit companies increasingly understand that simply by tapping into the cloud they can achieve fast access to business applications or infrastructure resources, all at insignificant cost. But as lot and lot of information on persons and companies are placed in the cloud, concerns are foundation to grow about just how safe an environment it is.

Cloud providers have a strong motivation to maintain conviction and as such utilize a higher level of security. Still, in the cloud, your data will be scattered over these individual computers regardless of where your base warehouse of data is finally stored. Industrious hackers can attack almost any server, and there are the statistics that show contravene result from stolen or lost computer and other devices and from workers accidentally revealing data on the Internet, due to insider theft. When come to privacy, cloud computing make use of the virtual computing technology, users private data may be distributed in various virtual data center quite than stay in the same physical location, even across the various country, at the moment, data privacy protection will face the argument of different legal systems. Conversely, users may seep out hidden information when they accessing cloud computing services. Invaders can analyze the serious task depend on the computing task presented by the users. To protect data secrecy and unwanted accesses in cloud on sensitive data might have be encrypted by the data owners before outsourcing to the public cloud. Decrypting huge amount of the data leads it increase in bandwidth cost in cloud scale system. Reducing local storage management the data can be stored in the cloud in less they can be searched and utilized easily. For this reason the privacy-preserving and security over encrypted data in most impotent. Security as

a major impediment to broad scale realization for cloud, regardless of the cloud services and in response is strengthening their security controls. Encryption is one of the important techniques to provide security over cloud. When compare to public cloud there are more security issues over the hybrid cloud.

Encryption effortlessly and simply provides the protection and advanced security intellect data to protect sensitive data-at-reset within public, private or hybrid cloud surroundings. While using symmetric and asymmetric encryption, the main problem is that a symmetric key has to be scattered between any related combination of senders and receivers and in public key approach, it does not consider many to one situation. In addition, functions of asymmetric encryption are more resource difficult then symmetric ones. Hence, both concepts do not well for dynamic and mobile situations. Our early work has been focus on security issues over the encrypted data on the cloud, during encryption the data can be encrypted using symmetric encryption but it has a problem, it does not provide secure communication with a dynamic groups or an unknown receivers.

2. Related Work

In this section, we are analyzing existing schemes that can prospectively be used to implement a various encryption techniques for messaging functions, safe communication and searching over the data.

2.1 Symmetric Encryption

In an extensive or distributed situation, usual cryptographic structures suffer from key distribution problems (SE) or problems related to the competence of encryption function (ASE). Figure1 illustrate the essential approach how symmetric encryption (SE) can be applied to attain secure communication. The main problem is that a symmetric key has to distribute between any pertinent combination of dispatchers and receivers. In case the group of receivers is not known when a message is sent out, this method is not applicable.

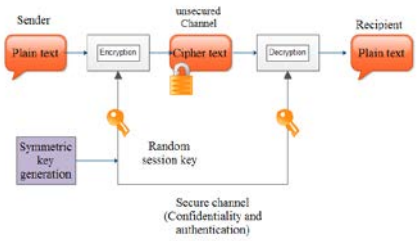

Fig. 1 Symmetric Encryption

2.2 Asymmetric Encryption

Public key encryption (figure 2) can resolve they key distribution difficulty of symmetric encryption. Now, instead of using a single symmetric key for both encryption and decryption, a couple of key is used. It consists of public key and private key, by issuing the public key of all possible receivers, a sender can send encrypted messages. Yet, this method does not consider one-to-many settings. Also, functional of asymmetric encryption are additional resource challenging than symmetric ones. For that reason, both ideas alone do not fit well in dynamic and mobile situations.

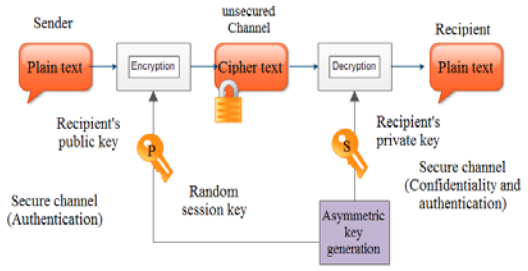

Fig. 2 Asymmetric Encryption.

Standard asymmetric encryption method are not realistic for securing communication with dynamic groups or unknown receivers , since new entities cannot be addressed and also documentation verification is an enormous problems. Dealing with these problems, more recent asymmetric encryption technique planned to simplify the role of the receivers' individuality and thus can allow a more exible requirement of receivers and content. As a result in the method, the key-related concepts refer to attributes which can signify properties of receivers and/or messages.

2.3 Identity-Based Encryption

It is documentation less option to public key encryption, let's encrypting messages under textual strings, in its place of public keys [8]. Such a string at first refers to the individuality of receivers. It requires the ease of use of a complete list of all future receivers. So far, it allows understanding encryption that is partially suitable for one-to many settings, by describing a cluster by a single textual string. Dissimilarly, we search for devise an encryption scheme that is able to control more expressive policies.

2.4 Searchable Encryption on cloud data

The encryption documents along with the index are placed in the data server [6]. The index is hidden to the server since it is highly confidential. The third party cannot able to access the document since they don't have the trapdoor. The trapdoor is provided only to the authorized user. If the unauthorized user will reveal the trapdoor then it leads to problem.

3. Existing Work

3.1 System Model

In the cloud, the data owners are outsource their data into cloud servers. Collection of data will be stored in the cloud server by means of encryption form. For effective searching capability the index I can be build with an encryption data and then exude both the index I and the encrypted document collection to the cloud server. When the user requested document will be placed in the server by means of encrypted form with the help of data owner [13]. The ranking method is performed for the requested documents of the data user for better improvement of the results.

3.2 Security Model

Symmetric encryption is the encryption method, which is used to encrypt the data into cipher text by suing the private key. In an extensive or distributed situation, usual cryptographic structures suffer from key distribution problems (SE) or problems related to the competence of encryption function (ASE). Plain text is the most portable format because it is supported by nearly every application on every machine and it does not contain any formatting commands. The cipher text is the result of encryption performed on plaintext using an algorithm, called a cipher. Cipher text is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption is the process of turning cipher text into readable plaintext, cipher text in not to be confused with code text because the latter is a result of a code, not a cipher. The main problem is that a symmetric key has to distribute between any relevant combination of dispatchers and receivers. In case the group of revivers is not known when a message is sent out, this method is not applicable.

4. Proposed System

The main disadvantages of existing schemes while using symmetric key, and asymmetric keys are,

a) It does not provide secure communication with a dynamic group or unknown receivers.
b) Due to security issues in hybrid cloud.

4.1 System Model

In cloud computing the search service including three entities as (figure 3) data owner, data user, and hybrid cloud server. When the user requests the data to the cloud server by using multi keyword search, Collection of data will be stored in the cloud server based upon the user request the document is encrypted before outsourcing by means of amalgam attribute based encryption (AABA), which is combination of CP-ABE and LBE in the level of symmetric key. For effective searching capability the index I is build for encrypted data and then exude both the index I and the encrypted document collection are outsource to the hybrid cloud server. Due to security issues in hybrid cloud we prefer an AABA. The ranking method was performed for the requested documents of the data user for better improvement of the results.

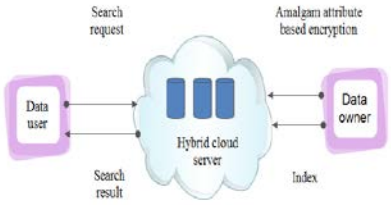

Fig. 3 Architecture of the search over amalgam attribute based encryption over the hybrid cloud

4.2 Security Model

In security model, CP-ABE encryption algorithm takes as input a message and an attribute policy. The algorithm encrypts a message constructs a cipher text. Such that only a receiver acquires a group of attributes that satisfies the attribute policy is adept to decrypt that message. In order to evade the computation of parings and thus allow more practical applications, CP-ABE can be used in hybrid approach. A message itself is encrypted with a random symmetric secret key. Only this session key is the CP-ABE encrypted under a policy. In location based encryption (LBE), the targeted receiver geographical locality L is

shared with the session key, in order to generate a location-locked key. This key is then sent along with session key, in order to generate a location-locked key. This key is then sent along with the encrypted message. As a consequence, the cipher text can only be decrypted if the session key, in order to generate a location-locked key. This key is then sent along with the encrypted message. As a consequence, the cipher text can only be decrypted if the session key can be mended from the location-locked key. LBE needs that this decryption is only potential if the receiver's device is physically accessible at location L, or correspondingly inside a geographic area related with L. This process is called location verification. It pivots on a tamper-resistant GPS handset inside the recipient's mobile device. In LBE, the sender has to broadcast limits which identify the area where decryption is allowable and may specify further dynamic restraints like time periods or even speed that have to be confirmed upon decryption.

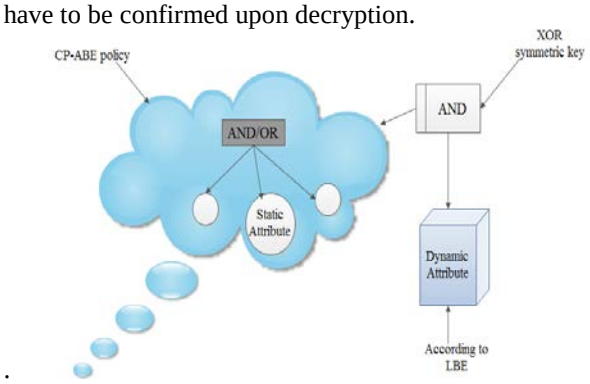

Fig. 4 CP-ABE and LBE construction principle

CP-ABE is used to control static attribute within an encryption policy, while the principle of location-based encryption is engaged to derive a symmetric key from a dynamic attribute. In order to store the computation of pairings, we influences CP-ABE in a hybrid approach this means, we divide the encryption of the load from the encryption of the session key. The session key is then as well bound to the location-based encryption. Therefore, in order to decrypt, both the CP-ABE policy and the LBE constraint have to be satisfied. Figure 4 shows this CP-ABE and LBE construction principle in overview.

Security Issues in Hybrid Cloud

Hybrid cloud as the name implies, a hybrid cloud is the combination of two or more clouds. Its main feature is that is uses existing resource on premises and combines is with cloud functionality**.** Benefits of hybrid cloud computing are Flexible business operations, Optimized costs, Enhanced security, Improved performance. Hybrid cloud technologies are still developing at a rapid pace. One of the biggest challenges posed by a hybrid cloud is the dependency on IT infrastructure. With complex networking solutions running in an environment, you need to efficiently manage both private and public clouds. Choosing the right provider for your cloud computing solutions can prevent outages and improve redundancy issues, while offering the highest performance. The main benefit of this model is that it allows enterprise to still have control over their data while enjoying some of the benefits of the cloud. Many large enterprises these days use hybrid clouds, in the sense that they place their application on site and partly in cloud. Due to the importance of data in many enterprises, the ability to monitor, protect, and enforce access permissions. The security is unacceptable and many complex systems and solutions are devised in order to protect the integrity of their data security.

a) Security of data that has effect of cost and agility provided by hybrid clouds, may enterprises refuse to commit to it because they trust existing internal security measures over the cloud service providers. That the confidentiality of the data will be violated as the data present in the cloud can be leaked.

b) Adjustment and reprogramming are lot of migrating components from one-sit to public cloud many applications used by enterprises interactions and inter-dependencies, and moving them to the cloud without any preparation could result broken the data or process.

c) Integrity of applications of cloud service providers is standardization of APIs that can easily accommodate many different subscribers with different needs to upgrades. This standardization could introduce security risks that a security of enterprise is vulnerabilities for many situations. Where their data could get compromised through no fault.

From the above issues only we are choosing the Amalgam attributed based encryption.

ISSN 2348 - 7968

Conclusion and Future Work

In this paper, we defined and solved the problem of encryption on cloud data. The most common use of encryption is to provide confidentiality by hiding all useful information about the plaintext. Among various encryption techniques we choose the amalgam attribute based encryption for secure communication on dynamic attributes. It can proficiently deal with dynamic locality, even in resource constrained situations. As our future work, we will concentrate on furthermore efficiency on the retrievals of data on the hybrid cloud.

References

[1] L.M. vaquror, L.RoderoMerino, J. Caceres and M.Linder, "A breaking the cloud:towards a cloud definition" ACMSIGOM comput comm.. Rev.Vol.39;no.1.pp.50-55, 2009.
[2] S.Kamar and K.Lauter " Crypotographic cloud storage,in RLCPS jancuary 2010,LNCS.springer,Heidelberg.
[3] D.song, D.Wangner, and A.Perrig "Practical technique for search on encryption data," in proc.of s&p,2000.
[4] E.J Goh "Secure indexes "Crytology eprint archive,2003
[5] Y-C chang and M. Mitzemacher , " Privacy preserving keyword searches on remote encrypted data" in proc of ACNS,2005.
[6] R, Cutmola, J.A. Grarcy. S.Kamara and R.ostroustrogy " Searchable symmetric encryption: Improved definition and efficient construction" in proc.of ACMCCS,2006
[7] Stefan G. Weber "*Designing a Hybrid Attribute-Based Encryption Scheme Supporting Dynamic Attributes*".
[8] Boneh, D., Franklin, M.K.: Identity-Based Encryption from the Weil Pairing. SIAM Journal on Computing 32(3), 586-615 (2003).
[9] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: IEEE Symposium on Security and Privacy (SP '07). pp. 321-334. IEEE CS (2007).
[10] A. Beimel. *Secure Schemes for Secret Sharing and Key Distribution*. PhD thesis, Israel.
[11] E. Shen, E. Shi, and B. Waters, "Predicate privacy in encryption systems," in *Proc. of TCC*, 2009.
[12] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proc. of ICDCS'10*, 2010.
[13] S. Zerr, E. Demidova, D. Olmedilla, W. Nejdl, M. Winslett, and S. Mitra,"Zerber: r-confidential indexing for distributed documents," in *Proc. Of EDBT*, 2008, pp. 287–298.
[14] S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski, "Zerber+r: Top-k retrieval from a confidential index," in *Proc. of EDBT*, 2009.
[15] Shamir, A.: How to Share a Secret. Communications of the ACM 22(11), 612-613 (1979).

Raj Priyadarshini received the B.E. degree under Department of Computer Science and Engineering from Mailam Engineering College in 2011 affiliated to Anna University and received the M.TECH degree under Department of Computer Science and Engineering in the specialization of Distributed Computing Systems in 2013 affiliated to Pondicherry University. She is currently working as a Assistant Professor in the Department of Computer Science and Engineering from Alpha College of Engineering and Technology, Pondicherry. She is a member of IAENG.

Kanchanadevi She is currently pursuing the B.Tech degree in the Department of Computer Science and Engineering from Alpha College of Engineering and Technology affiliated to Pondicherry University.