A Verifiable Approach for Attribute Based Encryption in Cloud Computing

Inian Lourde Alex A[1], Ramalingam A[2], Mohan Kumar S[3]
PG Scholars Sri Manakula Vinayagar Engineering College (*Puducherry*) [1,3]
Associate Professor Sri Manakula Vinayagar Engineering College (*Puducherry*) [2]

ABSTRACT

Cloud Computing is used for enabling convenient, on-demand network to access shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, and services) which are rapidly provisioned and released with management effort or service provider interaction. Cloud technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth. The security is the major issue in the cloud computing. The issue is overcome by the encryption. The various encryption standards ensure the cloud security. Attribute-based encryption (ABE) is a vision of public key encryption that allows users to encrypt and decrypt messages based on user attributes. In a typical implementation, the size of the cipher text is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption To reduce the decryption time in outsourced encryption method the user provides a transformation key to the cloud to translate any ABE cipher text into simple cipher text and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher text. We cannot guarantee that the cloud server will perform the transformation correctly. The proposed system introduces the Verifiable Outsourced Encryption so that the user can check the correctness of the transformation performed by the cloud server and the user let to know the data is not modified by the untrusted servers.

1. INTRODUCTION

The definition of Cloud computing varies from individual to individual. Basic working of cloud computing is to provide a cheap and efficient services in order to reduces the cost of data management and infrastructure. Cloud computing provides different services rather than a unit of product. These services put forwarded 3 models: Software as a Service (SAAS), Platform as a Service (PAAS), and Infrastructure as a Service (IAAS).The major problem faced in cloud computing is recent days is the data integrity problem. Most of the enterprise application are deployed in cloud. Cloud are of three types, public cloud which is mostly maintained by third parties, private cloud which is used for specific application and hybrid cloud which is a combination of both the above mentioned clouds. Besides the benefits associated with the cloud computing, there are different security issues in cloud in order to differentiate one cloud user's data from the other in order to retain the data, privacy, reliability, confidentiality and integrity.

In this paper, we have focused on the ABE (Attribute Based Encryption) technique a new public key based one-to-many encryption that enables access control over encrypted data using access policies and ascribed attributes associated with private keys and cipher texts. There are two kinds of ABE schemes: key-policy ABE (KP-ABE) and cipher text-policy In a CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a cipher text only if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text. In a KP-ABE scheme, the roles of an attribute set and an access policy are swapped from what we described for CP-ABE: attributes sets are used to annotate the cipher texts and access polices over these attributes are associated with users' private keys. In the following, we will use the terms access policy, access structure and access formula inter changeably.

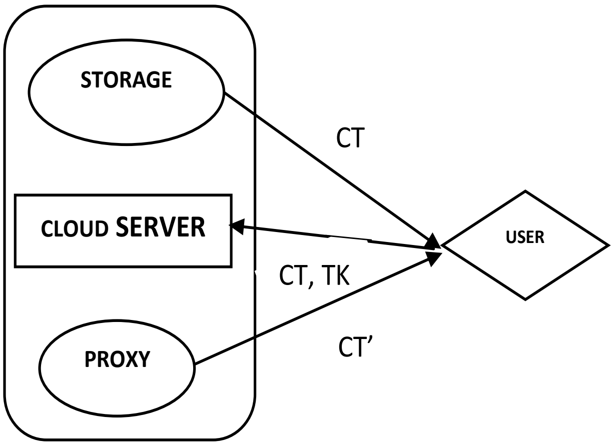

Figure 1.ABE system for outsourced decryption

One of the main efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource-limited devices due to the number of pairing operations required to decrypt a cipher text with complex accessing policy. The cost of security can be proven only in a weak model (i.e., selective security), there exist several expressive ABE schemes where the decryption algorithm only requires a constant number of pairing computations. Recently, Green et al proposed a remedy to this problem by introducing the notion of ABE with outsourced decryption, which largely eliminates the decryption overhead for users.

Based on the existing ABE schemes, Green et al. also presented concrete ABE schemes with outsourced decryption. In these schemes a user provides an untrusted server, say a proxy operated by a cloud service provider, with a transformation key TK that allows the latter to translate any ABE cipher text CT satisfied by that user's attributes or access policy into a simple cipher text CT', and it only incurs a small overhead for the user to recover the plaintext from the transformed cipher text CT'. The security property of the ABE scheme with outsourced decryption guarantees that an adversary (including the malicious cloud server) be not able to learn anything about the encrypted message; however, the scheme provides no guarantee on the correctness of the transformation done by the cloud server.

In the cloud computing setting, cloud service providers may have strong financial incentives to return incorrect answers that are easily detected by users. Consider a cloud based electronic medical record system in which patients' medical records are protected using ABE schemes with outsourced decryption and are stored in the cloud. In order to access patients' medical records effectively on the mobile phone, a doctor generates and delegates a transformation key to a proxy in the cloud for outsourced decryption; given a transformed cipher text from the proxy, the doctor can read a patient's medical record by just performing a simple step of computation. If no verification of the correctness of the transformation is guaranteed, however, the system might run into the following two problems: 1) for the purpose of saving computation cost, the intermediate could return a medical record transformed previously for the same doctor; 2) due to system malfunction or malicious attack, the proxy could send the medical record of another patient or a file of the correct form but carrying wrong information.

The consequence of treating the patient based on incorrect information could be very serious or even catastrophic. The above observation motivates us to study ABE with verifiable outsourced decryption in this paper. We emphasize that an ABE scheme with secure outsourced decryption does not necessarily guarantee verifiability (i.e., correctness of the transformation done by the cloud server). For example, the secure ABE schemes with outsourced decryption proposed by Green et al are not verifiable.

2. RELATED WORK

There are many research efforts that address the security problem in cloud computing, but they have not satisfied the exact requirements. In this section we have highlighted some better known proposal for the access control based security problems that occurs in the cloud.

Vipul Gopal [1] addressed that more sensitive and important data is shared and stored by third-party sites (untrusted) on the Internet, there will be a necessity to encrypt data stored at these sites. One disadvantage of encrypting data is that it can be comparatively shared only at a coarse-grained level. Method adopted here is Key-Policy Attribute-Based Encryption (KP-ABE). In this system cipher texts are named with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. Here cipher texts are associated with sets of attributes, whereas user secret keys are associated with policies.

Allison Lewko [2] proposed that previous constructions of ABE were only proven to be selectively secured not fully secure. This proposed system provides the fully secured encryption which overcomes the problem in the existing system. Methods Used here is Dual system encryption. In a dual encryption system, keys and cipher texts can take on one of two forms normal and semi-functional. Both normal and semi functional cipher texts can be decrypted by a normal key. A semi-functional key can only decrypt normal cipher texts.

Ling Cheung [3] developed a new scheme which allows an encryptor to use any AND gate on positive and negative attributes as an access policy on the cipher text. Methods Used here is cipher text policy attribute-based encryption. Proposed method to present variant with substantially smaller cipher texts and faster encryption/decryption operations and to Obtain CCA security. In cipher text policy attribute-based encryption (CP-ABE), every secret key is associated with a set of attributes, and every cipher text is combined with an access structure on attributes. Decryption is enabled if the user’s attribute set satisfies the cipher text access structure. It provides fine-grained access control on sharing of data in numerous practical settings, including secure databases and multicast.

Allison Lewko [4] stated that the past constructions of HIBE in the standard model, a maximum hierarchy depth had to be used at setup. In all the past constructions of Attribute Based Encryption in the standard model, either a small totality size or a bound on the size of attribute sets had to be fixed at beginning (setup). A two-level HIBE (2-HIBE) scheme consists of a root private key generator (PKG), domain PKGs and users, all of which are associated with primitive IDs (PIDs) that are arbitrary strings. The public key of the users consists of their PID and their domain’s PID (in whole called an address). In a regular IBE (which corresponds to a 1-HIBE) scheme, there is only single PKG that distributes private keys to each user (whose public keys are their PID).In a 2-HIBE, users recover their private key from their domain PKG. Domain PKGs can calculate the private key of any user in their domain, provided they have formerly requested their domain secret key from the root PKG (who possesses a master secret).

Amit Sahai [5] proposed that existing work in applying biometrics to cryptography has focused on the derivation of a secret from a biometric in a secret way. Biometric is used as an identity then the verification process for an identity is very clear. Biometric identity is an inherent trait and will always with a person. Using biometrics in Identity-Based Encryption will mean that the person will always have their public key handy. In most of the situations a user will want to present an encryption key to someone when they are physically present.

Unlike the existing techniques, our works aims at addressing a novel approach for CP-ABE system which allows user to verify the transformation performed by the untrusted servers in a distributed based cloud environment. In addition to this we reduce the decryption time for the user by indulging a proxy server. Our work compliments the existing by reducing the workload for the user considerably to enhance cloud security in a multiuser environment.

3. Security Issues in Cloud Computing

There are many security issues for cloud as it encompasses many technologies including databases, networks, operating systems, virtualization, resource scheduling, load balancing, and memory management. So, the security issues for many of these systems and technologies are adopted to cloud computing. For instance, the network that interconnects the systems in a cloud has to be secure and safe. And also, virtualization paradigm in cloud computing results in several security criteria. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security provides encrypting the data and ensuring that necessary policies are enforced for data sharing. In extent, resource allocation and memory management algorithms have to be secure and safe. Finally, data mining techniques may be useful for malware detection in clouds. Security issues of cloud computing are discussed below:

3.1 XML Signature Element Wrapping

XML signature Element Wrapping is the renowned attack for web service. It is used to defend a component name, attribute name and value from unauthorized party but unable to protect the position in the documents. Attacker targets the component by operating the Simple Object Access Protocol messages and putting anything that attackers like. Remedy measures for this attack is using the digital certificate. Example is X.509 authorized by third party such as certificate authorities and also uses the combination of WS-security with XML signature to a particular component. XML should have the list of components and it can reject the messages which have forged files and also reject the unexpected messages from the client.

3.2 Browser Security

The second issue is the Browser Security. The client sends the request to the server by web browser, and the web browser will make use of SSL to encrypt the credentials to authenticate the user. SSL support point to point communication means, if there is third party, intermediate host can decrypt the data. If cracker installs sniffing packages on intermediary host, the attackers may get the credentials of the user and login as a valid user. Remedy measure for this attack is Vendor should use WS-security concept on web browsers because WS-security works in message level that use XML encryption for continuous encryption of Simple Object Access Protocol messages which does not have to be decrypted at mediator hosts.

3.3 Cloud Malware Injection Attack

The next issue is Cloud Malware Injection Attack, which tries to damage a malicious application or virtual machine. An intruder is obligatory to generate his personal malicious application, service or virtual machine request and put it on the cloud. Once the malicious software is entered into the cloud structure, the attacker care for the malicious software as legitimate request. If satisfied user ask for the spiteful service then malicious is implemented. Attacker upload malicious program in to the cloud structure. Once cloud structure care for as a legitimate service the virus is implemented which damages the cloud structure. In this case hardware is damaged and attacker aim is to harm the user. Once user asks for the malicious program request the cloud gives the virus to the client over the internet. The client machine is affected by virus. Remedy measure for this attack is authentication check for received messages. Store the original image information of the request by using hash function and compare it with the hash value of all upcoming service requests. In this way attacker makes a legitimate hash value to deal with cloud system or to enter into the cloud system.

3.4 Flooding Attacks

Flooding attacks is the next issue. Attacker strikes the cloud system openly. The most outstanding feature of cloud system is to make available of hard scalable recourses. Cloud system continuously increase its size when there is more requests from clients, cloud system provide new service request in order to obtain client requirements. Flooding attack is generally distributing a large amount of non-sense requests to a limited service. Once the attacker throw a number of requests, by providing large recourses cloud system will try to work against the requests, ultimately system uses all recourses and not capable to provide service to normal requests from user. Then attacker harms the service server. DOS attacks cost additional fees to the consumer for usage of recourses. In an unforeseen situation the owner of the service has to tally additional money. Remedy measure for this attack is it's difficult to stop Dos Attacks. To stop from damaging the server, Intrusion detection system will filter the spiteful requests, installing firewall. Occasionally intrusion detection system provides fake alerts and could mislead administrator.

3.5 Data Protection

Data protection in cloud computing is a main factor, it could be difficult for the cloud customer to efficiently check the activities of the cloud supplier and as a result he is sure that data is handled in a appropriate way, but it does not like that this problem is intensify in case of various transformation of data**.** Remedy measure for this attack is that a consumer of cloud should check data handle either it is handled lawfully or not.

3.6 Incomplete Data Deletion

Incomplete data deletion is mostly risky in cloud systems, it does not remove completed data because duplication of data is placed in other servers. For example when a client request to detach a cloud resource, then with most OS this will not detach accurately. Accurate data deletion is impossible because copies of data are stored in the nearest copy but are not available. Remedy measure is that VPN should use for securing the data and used the query that will detach all the data from the main servers along with its copies.

3.7 Locks in

Another problem is locks in; at this time there is a little tender in the manner of tools, standard data format or procedures, services edge that could handle data, application and service portability. This will disable the customer to move from one cloud provider to another or shift the services back to home IT location.

4. PROPOSED WORK

In this section, we have addressed on the data protection issue in cloud computing environment. The Problem in the Existing system is the user cannot trust the transformation performed by an untrusted server. To overcome that problem the proposed system contains a checksum to verify the correctness of the transformation. The system proposed method is a verifiable approach. The goal of the proposed system is to reduce the decryption time on the user side. According to that the proposed system allows to perform a transformation over the cipher text. The transformation process reduces the size of the cipher text. Even the transformation is performed the file reminds as in the cipher text form and not in a fully decrypted form. Then the user can decrypt the file with his secret key.

The problem of the verification overcame here. We provide a checksum value for the each file. Whenever the user receives a file also receives the corresponding checksum. The user then produces the checksum for the received file and checks whether the both are same or not. If both are same then the transformation is correct otherwise wrong.

The major advantages of the proposed system is that, 1) allow the user to verify the cloud server transformation 2) a new approach for outsourcing encryption that let the user to verify 3) guarantees that the hackers cannot be able to identify anything from the encrypted cipher text.

5. CONCLUSION

The Attribute based Encryption increases the cipher text size according to the number of attributes. To overcome that problem the outsourced decryption is introduced. The outsourced decryption reduces the cipher text size by decrypting the cipher text during the file outsourcing. But in the outsourced decryption the decryption is performed by the untrusted server. So we cannot say that the decryption performed by the server is correct or wrong. So the problem is solved by the proposed system. The proposed system allows the user to check whether the decryption performed by the server correct or wrong. This method is achieved by producing a checksum for the cipher text. The decryption is correct if the user can produce the same checksum which the data owner produced.

REFERENCES

[1] V.Goyal, O. Pandey,A. Sahai, and B.Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Computer and Communications Security, 2006, pp. 89–98.

[2] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in Proc. EUROCRYPT, 2010, pp. 62–91.

[3] L. Cheung and C. C. Newport, “Provably secure ciphertext policy ABE,” in Proc. ACM Conf. Computer and Communications Security, 2007, pp. 456–465.

[4] A. B. Lewko and B. Waters, “Unbounded HIBE and attribute-based encryption,” in Proc. EUROCRYPT, 2011, pp. 547–567.

[5] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. EUROCRYPT, 2005, pp. 457–473.

[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attributebased encryption,” in

Proc. IEEE Symp. Security and Privacy, 2007, pp. 321–334.

[7] L. Cheung and C. C. Newport, “Provably secure ciphertext policy ABE,” in Proc. ACM Conf. Computer and Communications Security, 2007, pp. 456–465.

[8] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. EUROCRYPT, 2005, pp. 457–473.

[9] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proc. ACM Conf. Computer and Communications Security, 2007, pp. 195–203.

[10] T. Okamoto and K. Takashima, “Fully secure functional encryption with general relations from the decisional linear assumption,” in Proc. CRYPTO, 2010, pp. 191–208.

[11] R. Canetti, H. Krawczyk, and J. B. Nielsen, “Relaxing chosen-ciphertext security,” in Proc. CRYPTO, 2003, pp. 565–582.

[12] T. Okamoto and K. Takashima, “Fully secure unbounded inner-product and attribute-based encryption,” in Proc. ASIACRYPT, 2012, pp.349–366.

[13] B. Chevallier-Mames, J.-S. Coron, N. McCullagh D.Naccache,and M. Scott, “Secure delegation of elliptic-curve pairing,” in Proc.CARDIS, 2010, pp. 24–35.

[14] K.-M. Chung, Y. T. Kalai, and S. P. Vadhan, “Improved delegation of computation using fully homomorphic encryption,” in Proc. CRYPTO, 2010, pp. 483–501.