ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Secured and Verifiable Approach for Attribute Based Encryption in Cloud Computing

Miss. Snehal Sunil Sancheti, Prof. Mrs. A. S. Patil
E & TC Department, PVPIT, University of Pune, India, E & TC Department, PVPIT, University of Pune, India
snehalsancheti@gmail.com

Abstract

Cloud Computing has changed the phenomena of IT industry completely. It allows access to highly scalable, inexpensive, on demand computing resources that can execute the code and store data that are provided. But adoption and approach to cloud computing applies only if the security is ensured. Cloud computing is lacking in security, confidentiality and visibility. Secure the cloud means to secure the storage. Security is achieved by the encryption. There are various encryption standards to ensure the cloud security. Attribute-based encryption (ABE) is public key encryption technique 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 cloud outsourced decryption technique is used. By providing a transformation key to the cloud ABE cipher text is converted into simple cipher text and it only incurs a small computational overhead for the user to recover the plaintext from the transformed ciphertext.. To ensure that transformation performed by cloud server is correct and the data is not modified by the untrusted servers proposed system is introduced. This provides secured and Verifiable Outsourced decryption.

Keywords: Attribute Based Encryption, Ciphertext Policy Attribute Based Encryption, Cloud Computing, Key Policy Attribute Based Encryption.

Introductions

In Recent years cloud computing technology prototypes have exceedingly become a new way to provide shared services and data over the internet. Especially this prototype encourages an effective way of data sharing among the users of cloud , since the users are able to export the data to a public cloud storage which can provide access to data as a service .Considering this new model questions are raised as far the security if the services are concerned.

To reduce costs and improve productivity and efficiency organizations across the globe look at technology as an essential part. The new advancements in cloud computing technology help organizations in reducing the computing costs while boosting work productivity. with ever increasing interest in cloud services and technology and the rise of Software As a Service(Saas) based applications the requirements for cloud based technologies is accelerating Apart from this with growing influence of web 2.0 technologies, non-enterprise users are also massively using cloud computing technologies. In the upcoming age cloud services will become the cornerstone of the modern commercial world.

In spite of cloud technology's tremendous capacity, there are still many technical hurdles that continue to hamper the wide spread adaption the technology. [1] Recent Privacy threats experienced by users of services offered by Apple, Google, Amazon [1] are clear indications that cloud is internally insecure from the users perspective.

Because users don't have access to cloud service providers internal operations preserving privacy of user in cloud computing environment is a challenge for researchers.

Yanbin Lu and Gene Tsudik [2] list following challenges in preserving privacy in cloud.

- Challenge 1: How to protect user private data from abuse by the cloud server?
- Challenge 2: While using SaaS applications on cloud computing technology organizations outsource their data to cloud server? How to protect such outsourced data?
- Challenge 3: How to query the cloud server without exposing query details?
- Challenge 4: How to query contents from untrusted entities?
- Challenge 5: How to design and implement content level fine-grained access control for users?

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Up till now lot of work has been done to conserve the privacy in cloud server databases. Siani Pearson, Yun Shen and Miranda Mowbray [3] proposed a privacy manager for cloud computing. Jianwang [4] proposed anonymity based method for preserving cloud privacy. Miao Zhou [5] proposed a method for improved key management for maintaining privacy. Qin Liu [6] proposed bilinear graph based privacy preserving keyword searching method for accessing files. HaiboHu [7] proposed comprehensive privacy preserving scheme for indexed data. Marten van Dijk and Ari Juels [8] argued that alone cryptography is insufficient to maintain the privacy in cloud computing. Yanbin Lu and Gene Tsudik [9] proposed most comprehensive scheme that preserves the privacy and gives substantial improvements in encrypted database search, attribute-based encryption and predicate encryption. ShuchengYu [10] proposed Fine-grained Data Access Control in Cloud Computing using attribute based encryption. Although many schemes have been suggested to protect the privacy in cloud computing, most of them have not been able to resolve all the above listed challenges.

Schemes proposed in [3] and [4] fail to not provide solution for challenges 5, 3, 4. And also fail to consider comprehensive approach while solving the privacy preserving problem.

AdiShamir [11] in his achievement work first time proposed a novel type of cryptographic scheme called 'Identity-Based Cryptosystems and Signature Schemes' which allows number of pair of users to communicate with each other securely and to verify each other's signatures without exchange of private or public keys, with- out keeping key directories, and without using the services of a third party. It allows for a sender of message to encrypt a message to an identity without access to a public key certificate.

AmitSahai and Brent Waters [12] proposed fuzzy identity based encryption scheme which they termed as 'Attribute-Based Encryption' (ABE). This scheme based on AdiShamir [11] makes easy to find error tolerance between identity of private key and the public key which is used to encrypt a cipher text. In this scheme user's keys and ciphertexts are labeled with set of attributes and user who is having secret key will be allowed to decrypt ciphertext encrypted with public key if and only if they are within a certain distance of each other when measured by some metric.

Based on [12], VipulGoyal et Al. [13] discovered a new cryptosystem which they called 'Key -Policy Attribute-Based Encryption (KP-ABE)'. This system first time implemented fine gained access control on sensitive data that is shared and stored by third-party sites on the Internet. In this system ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

Bethencourt et al. [14] proposed a new cryptosystem called as 'Ciphertext-Policy Attribute-Based Encryption' (CP-ABE) which allowed user to store encrypted data to be kept confidential even if server on which data is stored is non-trusted.

Lu and Tsudik [2] proposed a new cryptosystem for preserving privacy in cloud database querying. Based on [11], [12], [13], [14] Lu and Tsudik brilliantly solved all the previously mentioned challenges in the privacy preservation of the cloud. Moreover other attempts [6], [7] did try to solve the problem of privacy preservation in Cloud environment but they were directed at file and indexed data. Lu and Tsudik [2] have solution for relational databases which are widely used by Saas based applications in the cloud.

Although Lu and Tsudik [2] have proposed a new method, which has the following limitations.

- It hides the attribute values in conditional expression but access structure is revealed to the adversary.
- Join operations between two tables are not supported
- If set of attribute values in access structure is small, then adversary can always encrypt something under all possible values and can collude with cloud service provider to check match for these encrypted values. This might reveal attribute values in token.
- Enterprise server is need to be online continuously so that user can extract decryption keys and search tokens.

Existing system

In cipher text policy attribute-based encryption (CP-ABE), every secret key is associated with a set of attributes, and every cipher text is associated with an access structure on attributes. Decryption is enabled if and only if the user's attribute set satisfies the cipher text access structure. Using (CP-ABE) any encryptor to specify access control in terms of any access formula over the attributes in the system. In the existing system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The Concept of verifiable is not described in detail in the existing system. The introduced cipher text policy attribute based encryption is the new way for the encryption. The encryption is fully based on the user attributes.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Most of the existing systems are proposed the attribute based encryption with various limitations and low performance to produce the cipher text. Whenever we use the attribute based encryption the length of the cipher text is greater to the proportion of the plain text size.

Demerits:

- No error recovery algorithms are implemented in existing system.
- No methods to verify the transformation.
- The untrusted server can perform the transformation in the sensitive data wrong transformations may lead to problems.
- Decryption time is high.

Proposed system

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.

Merits:

- The proposed system let the user to verify the cloud server transformation.
- The proposed system is verifiable but not with compromised with security.
- It is a new approach for outsourcing encryption that let the user to verify.
- It guarantees that the adversary cannot be able to learn anything about the encrypted cipher text.

System outline

Attribute Based Encryption is today's best solution available for preserving privacy in cloud environment. But its biggest drawback is time taken for encryption. This makes these schemes unattractive for real life application. In our dissertation we implement a scheme where this entire cryptographic operation will be carried out on cloud side with substantial computing power. This will make use of these scheme suitable for real life applications.

Data outsourcing to the cloud is beneficial for reasons of reduced cost, improve manageability, sharing of number of resources, less maintenance and scalability, but some technical challenges remain. Sensitive data stored in the cloud must be protected from being read by a cloud provider.

A.System block diagram:

Figure 1 shows the block diagram of System Architecture.

Figure:

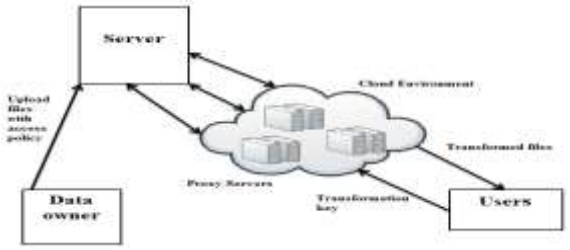


Fig. 1. System Architecture.

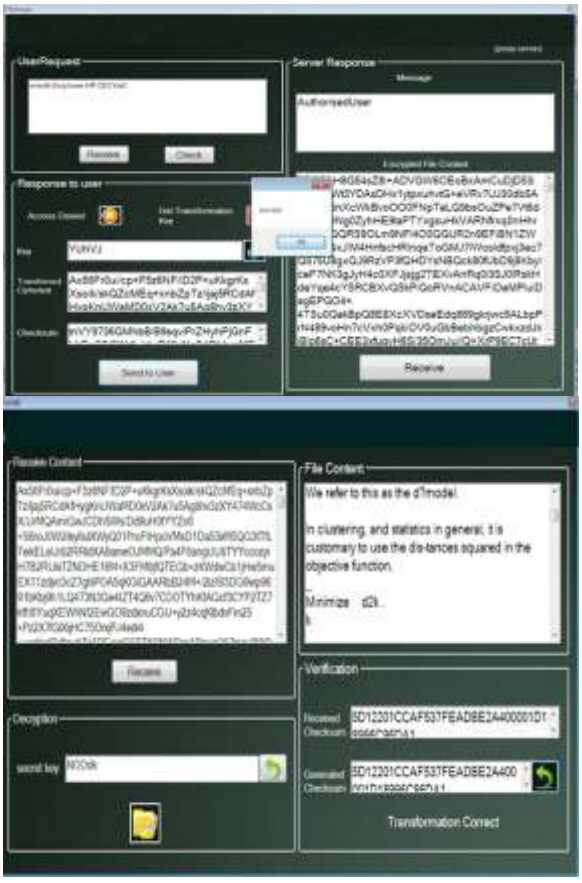
B. Description of the diagram:

The data owner uploads the files with access policy on the cloud server. The server maintains all details about the user and the corresponding attributes. The files placed on the server side are in the encrypted format and when a request arises from the user the server outsources the encrypted data content. At first the user sends his attributes and the required file name to the proxy server. The proxy server sends the user details to the server for authentication. The server checks whether the user attributes solves the access structure for the required file. If the user attributes does not satisfy the access structure then the user is not an authorized user to access the required file. If the user attribute solves the access policy then the user is an authorized user for the required file. Then the server outsources the file to the proxy server. Then the proxy requires a transformation key for the decryption. So it asks the transformation key to the user. Then the user sends transformation key to the proxy server. The proxy performs the decryption on the file received from the server and sends the file to user. Whenever there is an outsource of a file held in the proxy and the main sever they also outsources the encrypted checksum for the corresponding file. Then the user performs the decryption using his private key. It also decrypts the checksum using the same private key. The user then verifies the checksum produced with the checksum received from the proxy server. If both the checksums are same then the transformation performed by the proxy server is correct.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Experimental result

Experimental results show that the implementation of Attribute Based Encryption with verification works well and gives satisfactory results.



Refrences

1. *Kui Ren, Cong Wang, and Qian Wang, "Security Challenges for the Public Cloud", Internet Computing, IEEE, Vol. 16, Issue 1, Jan.-Feb. 2012.*
2. *Y. Lu and G. Tsudik, "Privacy-Preserving Cloud Database Querying", Journal of Internet Services and Information Security (JISIS), Vol. 1, No. 4, November 2011.*
3. *Siani Pearson, Yun Shen, Miranda Mowbray, "A Privacy Manager for Cloud Computing", First International Conference, CloudCom 2009, Beijing, China, December 1-4, 2009. Proceedings*
4. *Jian Wang, Yan Zhao, Shuo Jiang, Jiajin Le, "Providing privacy preserving in cloud computing", Test and Measurement, vol. 2, ICTM '09, International Conference, 2009.*
5. *Miao Zhou , Yi Mu , Willy Susilo , Jun Yan , Liju Dong, "Privacy enhanced data outsourcing in the cloud, Journal of Network and Computer Applications", vol. 35, issue 4, pp. 1367–1373, 2012.*
6. *Qin Liu, Guojun Wang, Jie Wu, "Secure and privacy preserving keyword searching for cloud storage services", Journal of Network and Computer Applications, vol. 35, pp. 927–933, 2012.*
7. *Haibo Hu, Jianliang Xu , Chushi Ren , Byron Choi, "Processing private queries over untrusted data cloud through privacy homomorphism" , Data Engineering (ICDE), 2011.*
8. *Marten Van Dijk, Ari Juels, "On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing", IACR Cryptology eprint Archive, 2010.*
9. *Dr. Alexander Benlian, Prof. Dr. Thomas Hess, Prof. Dr. Peter Buxmann, "Drivers of SaaS-Adoption – An Empirical Study of Different Application Type", Business & Information Systems Engineering, Vol. 1, Issue 5, pp 357-369, October 2009.*
10. *Shucheng Yu Cong Wang, Kui Ren , Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", INFOCOM, 2010 Proceedings IEEE.*
11. *Adi Shamir, " Identity-Based Cryptosystems and Signature Schemes", Proceedings of CRYPTO 84*
12. *Amit Sahai, Brent Waters, "Fuzzy Identity-Based Encryption", 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005 Proceedings.*
13. *Vipul Goyal,Omkant Pandey, Amit Sahai, Brent Waters , "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Proceeding CCS '06 Proceedings of the 13th ACM conference on Computer and communications security Pages 89 - 98 ,ACM New York, NY*
14. *John Bethencourt, Amit Sahai, Brent Waters, "Ciphertext-Policy Attribute-Based Encryption, Security and Privacy", 2007.*
15. *M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryptionof ABE ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.*
16. *Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng, "Attribute-Based Encryption With Verifiable Outsourced Decryption", IEEE Transaction on Information Forensics and Security, vol. 8, no. 8, August 2013.*