Scientific Journal Impact Factor (SJIF): 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745   ISSN (PRINT) : 2393 - 8161

An efficiently outsourcing Attribute Based Encryption using SPs

Nithya S[1], Nice Mathew[2]
[1]PG Student, Department of CSE, IIET, Nellikuzhi
[2]Asst.Professor, Department of CSE, IIET, Nellikuzhi

Abstract— Attribute-Based Encryption (ABE) is a cryptographic elementary which extremely enhances the flexibility of access control mechanisms. Due to the high expressiveness of ABE policies, the computational complexities of ABE key-issuing and decryption are getting remarkably high. An efficiently Outsourced ABE system, which supports both secure outsourced key-issuing and decryption. This method offloads all access policy and attributes related operations in the data storing process or decryption to a Decryption Service Provider (DSP) and authorization to Key Generation Service Provider (KGSP) or Attribute Authority (AA), respectively. This leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. In addition, outsourced ABE construction which provides checkability results in an efficient way.

Keywords— Attribute-based encryption, access control, outsourcing computation

I. INTRODUCTION

Attribute-Based Encryption (ABE) is a cryptographic elementary which extremely enhances the flexibility of access control mechanisms. In ABE system, users' private keys and cipher texts are associated with sets of attributes and access policies respectively, and a specific key can decrypt a specific ciphertext only if associated attributes and policy are paired. There are two kinds of ABE: key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). In KP-ABE, the access policy is assigned in private key, whereas, in CP-ABE, it is specified in ciphertext. Due to the high expressiveness of attribute based encryption policies, the computational complexities of ABE key-issuing and decryption are gaining unusually high. The attribute authority is responsible to deal with a lot of heavy computation in a modular system. When a large number of users call for their private keys, it may overburden the attribute authority. The revocation of any single private key requires key-update at attribute authority for the resting unrevoked keys. All of these heavy tasks consolidated at authority side would make it an efficiency bottleneck in the access control system. Nevertheless, one of the main efficiency drawbacks of ABE is that the computational cost during decryption phase increases with the complexity of the access formula. Thus, there is an increasing need to enhance the efficiency of ABE.

An alternative approach is to improve the ABE scheme by providing two additional service providers to reduce the load of attribute authority. A key generation service provider and decryption service provider are used to perform authentication and decryption operation. This paper also proposed a method to provide additional security to encrypted file stored in Storage service provider.

II. RELATED WORK

In the construction [1], introduced a trivial policy controlled by a default attribute and use an AND gate connecting the trivial policy and user's policy. Fuzzy identity-based encryption in [2], was firstly dealt with by Goyal et al. [11]. Two different and complementary concepts of ABE were explained in [11]: KP-ABE and CP-ABE. A creation of KP-ABE was given in the same paper [11], while the first CP-ABE construction supporting tree-based structure in generic group model is presented by Bethencourt et al. [4]. Accordingly, some constructions supporting for any modes of access structures were given [6]. Concerning revocation of ABE, a delegatable revocation is suggested in [13] to gain scalable and fine-grained access control. To reduce the load at local, it always wishes to deliver expensive computational tasks outside. Actually, the problem that how to securely outsource various modes of expensive computations has drawn huge consideration from theoretical computer science community. Atallah et al. [14] presented a scheme for secure outsourcing of scientific computations such as matrix multiplication and quadrature. Though, the solution used the disguise technique and thus leaded to outpour of private information. Atallah and Li [15] researched the problem of computing the edit distance between two sequences and proposed an efficient protocol to securely outsource sequence comparison with two servers.

Nevertheless, the suggested protocols required the pricey operations of homomorphic encryption. Atallah and Frikken [16] further studied the problem and gave an enhanced protocols based on this, so-called weak secret hiding assumption. Recently, Wang et al. [17] proposed efficient mechanisms for secure outsourcing of linear programming computation. Though several methods have been introduced to securely outsource kinds of expensive computations, they are not suitable for recalling ABE computational overhead of exponentiation at user side. To achieve this goal, the traditional approach is to apply server-aided techniques [8]. However, existing works are conformed to accelerate the speed of exponentiation using mistrustful servers. Directly utilizing these techniques in ABE will not work efficiently. Another approach might be to leverage recent general outsourcing technique or delegating computation [18] based on fully homomorphic encryption or interactive proof system. Yet, Gentry [19] has demonstrated that even for weak security parameters on ‘‘bootstrapping’’ operation of the homomorphic encryption, it would take at least 30 seconds on a high performance machine. Therefore, even if the privacy of the input and output can be kept by utilizing these general techniques, the computational overburden is still huge and impractical. Another several related works are [7], [5]. In [3], a novel model for outsourcing the decryption of ABE is given. Recently proposed a concrete construction for ABE with verifiable decryption, which achieves both security and verifiability without random oracles. Their work appends a redundancy with ciphertext and uses this redundancy for correctness checking. We emphasize that compared with our scheme their construction does not consider to offload the overhead computation at authority by outsourcing key-issuing.

III. PRELIMINARY

This section defines the notations used in this paper.

3.1. Notations

The notations used in this paper are:

Table 1. Notations Used

Acronym	***Description***
AA	Attribute Authority
KGSP	Key Generation Service Provider
DSP	Decryption Service Provider
SSP	Storage Service Provider
ABE	Attribute Based Encryption

IV. SYSTEM MODEL AND SECURITY DEFINITION

4.1. System Model

The System Model for the outsourced attribute based encryption scheme is shown in Figure.1.The main difference between the system model of typical ABE and outsourced ABE scheme is a KGSP and DSP are additionally provided.

- KGSP is responsible to perform the authentication of the user during the data retrieval time. The presence of KGSP reduces the overload of attribute authority at the data retrieval time.
- DSP performs the decryption operation during the authentication phase.
- SSPs are responsible to keep the encrypted documents securely. In order to provide more security to the stored data, using two storage service providers instead of one.

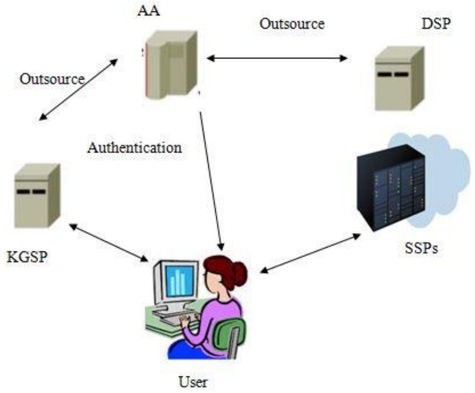

Figure.1. System Model

4.2. Security Definition

In this work, assumes that all the entities except AA are ‘‘honest-but-curious’’. More precisely, they will follow this proposed protocol but they try to find out as much private information as possible based on their possessions. Based on this consideration, two types of adversaries are categorized.

- Type-I adversary defined as a group of curious users colluding with SSP, is able to potentially access all the ciphertext stored at SSP, and aims to decrypt ciphertext intended for users not in the group.
- Type-II adversary defined at SSP, is able to potentially access all the ciphertexts stored at SSP, and aims to decrypt any ciphertext.

V. PROPOSED SYSTEM

To eliminate the most overhead computation at both the attribute authority and the user sides, use an outsourced Attribute Based Encryption scheme which supports both outsourced decryption and enabling delegating key generation. In this scheme, also introduces a secure way to store data on mistrustful storage server and user. During data retrieval, the attribute authority can outsource computation through delegating the task of authentication to a key generation service provider (KGSP) to reduce local overhead. Moreover, the decryption service provider (DSP) is responsible to perform outsourced decryption. Following this technique, constant efficiency is achieved at both attribute authority and user sides.

For outsourced ABE scheme, Attribute authority outsources the task of authentication to KGSP and decryption operation to DSP. In this scheme, attributes for the authentication process is chosen by the authority based on user provided data not by the user. Instead of a single attribute, a combination of attributes is used. An outsourced ABE scheme provides a secure way to store data on mistrustful storage server and mistrustful user. So user authentication is performed during both storing and retrieving time. It ensures security of data stored in a storage provider by splitting and encrypting the uploaded data. During the retrieval time, decryption and merging operation is performed locally.

5.1. Key Generation

User has to register to the system by filling up all their own personal details. Based on these details, user attributes are chosen for the authentication purpose. Once user registered completely, details will be stored for further processing. The Attribute Authority (AA) and Key Generation service provider is responsible to provide authentication based on user's attribute. Key generation is performed using any homomorphic encryption algorithm. Homomorphic encryption that allows computations to be executed on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. During key generation, it randomly selects two prime numbers. Based on these numbers, generate Master key and Secret key which will be generated for each data upload. These are used for user authentication function. A key is generated using AES algorithm at the time of registration for each user which is used for the file encryption and decryption process.

5.2. User Authentication

In an efficiently outsourcing ABE scheme, user authentication plays a crucial role. Because this scheme used in a condition where both storage service providers and users are mistrustful. User authentication is performed by attribute authority at the time of file upload and KGSP at the time of the file download. During file upload, a random key is generated for each file. Then a blind transformation is performed on the attribute set values and the random generated value at the user side. Similarly at the authority side, a blind transformation is performed on the random key and attribute set which is in encrypted form. If the result of blind transformation on plaintext and result obtained by decrypting the blind transformation on encrypted values are same, then only file upload is allowed. The same authentication operation is performed by key generation service provider at the time of downloading.

5.3. Data Storage and Retrieval

The system only allows a valid user to upload a particular file into the SSPs. In SSPs, files are in splitted and encrypted form. So the storage service provider is unable to get the file because it is in encrypted format. AES encryption algorithm is used to encrypt the splits. Beyond that the file is splitted before encryption. The splitting up of file is done based on the type of the file. After splitting and encryption, operation, the split files are converted into another format. Then only splits are saved into two servers. So the storage service providers are unable to get the original file because it is in encrypted format. Beyond that the file is splitted before encryption and converted into another file format. If both servers are compromised, then only the attacker gets the data. In order to obtain the original data, he needs to know the extension of the file because it is in another file format. The user gets the file only after performing decryption, file conversion and merging of splits. Hence it is highly secure in the case of mistrustful storage service providers.

During file retrieval operation, process is same as file upload except here Key Generation Service Provider (KGSP) is responsible to perform the authentication operation. KGSP allows only a valid user to retrieve a particular file from SSP. In SSP, files are in splitted and encrypted form. Also, it is converted into another file format before storing into servers. So the storage service provider is unable to get the file because it is in encrypted format and the server is unaware about the type of the file. The user gets the file only after performing decryption and merging of splits. The merging of splitted files is the reverse process of splitting a file into multiple files. The merging of file is also done based on the type of the file.

Hence file is secure in the case of both untrusted storage service provider and user. Then the system allows only valid user to download his data. An attacker gets the data from the server if and only if both servers are compromised. Because the data is splitted into two servers. AA lists only the names of the files of particular valid user and AA is responsible to perform the file conversion. So, only the valid user gets the file after performing decryption, file conversion and merging of splits.

VI. ALGORITHM USED IN THE PROPOSED SYSTEM

In this paper, mainly uses two algorithms one is homomorphic encryption algorithm for authentication process and another is AES algorithm for encryption and decryption of files.

6.1. **Algorithm 1**: Homomorphic Encryption Algorithm

6.1.1. Key Generation

Input: Bit Length value and certainty
Output: Master Key and Secret Key

- Constructs two randomly generated prime numbers p and q.
- Compute n=p*q and lambda=LCM (p-1, q-1).
- Select random integer g.
- Publishes MK: (n , g)
  SK :(g, n, lambda)

6.1.2. Encryption

Input: Plain Text and Master Key
Output: Ciphertext

- Let m be the message to be encrypted where mЄZ_n^{*}
- Select a random r where r ЄZ_n^{*}.
- Compute ciphertext as: $c=g^{m} \bullet r^{n} \bmod n^{2}$

6.1.3. Decryption

Input: Ciphertext and Secret Key
Output: Master Key and Secret Key

- Let c be the ciphertext to decrypt where cЄ$Z^{*}_{n^{2}}$
- Compute plaintext message as:
  $m= L (c^{lambda} \bmod n^{2}) * u \bmod n,$
  where $u = (L(g^{lambda} \bmod n^{2}))^{(-1)} \bmod n.$

6.2. **Algorithm 2**: Data Encryption/Decryption Algorithm

6.2.1. Data Encryption

Input: Split File
Output: Encrypted File

- Generate AES symmetric key using a random value for each user.
- Convert the file into byte array.
- Encrypt the content of byte array using AES key.
- Write the encrypted data into file.

- Store the encrypted files into the servers.

6.2.2. Data Decryption

Input: Encrypted File and Key
Output: Decrypted File

- Convert the file into byte array.
- Decrypt the content of byte array using AES key.
- Write the decrypted data into file.
  Finally merges the decrypted files.

VII. APPLICATION

Different applications of Attribute Based Encryption scheme are as follows:

- Mistrustful Storage Service Provider and User: Data Owner needs to store his private data on untrusted storage server instead of trusted server with specified group of users.
- Constellation of role-based characteristics rather than identity.
- To significantly advance the field of trustworthy computing by basing access on a person's job description.

VIII. SIMULATION

The proposed tactic is implemented using Java programming. First step is user has to register to the system by providing his details. After validating the data, the authority accepts the registration and chooses the attributes of the user for further authentication process. User authentication is performed by attribute authority at the time of file upload and KGSP at the time of the file download. During file upload, a blind transformation is performed on the attribute set values and the random generated value at the user side. Similarly at the authority side, a blind transformation is performed on the random value and attribute set which are in encrypted form. If the result of blind transformation on plaintext and result obtained by decrypting the blind transformation on encrypted values are same, then only file upload is allowed. The same authentication operation is performed by key generation service provider at the time of downloading. The uploaded files are stored in different servers in which it is in splitted and encrypted format. Similarly valid user gets the exact file after performing decryption and merging of splits.

IX. EXPERIMENTAL RESULTS

The proposed method is an experiment through Java. Compared with the original scheme, it involves two level encryption and decryption. In our construction instead of single attribute, a set of user’s attributes is chosen. Attribute Authority is responsible for attribute selection. User is unaware about the attribute set. In general ABE scheme, user’s attribute is used to generate the key and based on this key both encryption and decryption operations are performed. But in our construction, attributes are used to perform user authentication. Our construction also requires an additional operation using blind transformation on attribute set. This leading to its slowness. Similarly, our data storing and retrieval operations are also relatively longer than that of the original scheme. This is because AA generates Master Key and Secret Key for each file and performs authentication during storing of files and also during retrieval. Beyond that the data is stored into different servers after performing splitting and encryption operations and retrieved from servers after performing decryption and merging operation. Fortunately, owing to outsourced computation, the computation cost at AA side is reduced to constant due to the presence of KGSP and DSP. KGSP reduces the load of AA by performing user authentication at the time of retrieval and DSP is responsible to perform decryption operation. To sum up, our outsourced construction achieves efficiency at both AA and user sides without introducing significant overhead compared to the original approach. In decryption, all the operations are delivered to DSP and the computational cost of decryption for user is constant, only one exponentiation operation. Whereas the original ABE scheme [2] requires 2d pairing as well as 2d exponentiation operations for a single decryption, where d is the threshold value.

Our outsourced construction takes more time than the original ABE scheme. This is because the outsourcing computation cannot be realized in the simple manner of ‘‘one plus one equals two’’, and some additional cost should be paid for preserving privacy at the same time achieving efficiency.

X. COMPARISON OF EXISTING & PROPOSED SYSTEM

In the existing system, Master key and Secret key which is generated from user provided attribute is only used to ensure the authentication of a user. Also encrypted data is stored in a single storage service provider. But in the proposed system, user authentication is done using attribute set which is selected by authority from user profile. Also encrypted data stored in different storage service providers. So this system ensures more security compared to existing systems in the case of mistrustful Storage Service Provider and User.

XI. CONCLUSION

Attribute-Based Encryption (ABE) is a cryptographic elementary which extremely enhances the flexibility of access control mechanisms. In ABE system, users’ private keys and ciphertexts are associated with sets of attributes and access policies respectively, and a specific key can decrypt a specific ciphertext only if associated attributes and policy are paired. An efficiently Outsourced ABE system, which supports both secure outsourced user authentication and decryption operations. This method offloads all access policy and attributes related operations in the data storing process or decryption to a Decryption Service Provider (DSP) and authorization to Key Generation Service Provider (KGSP) at the time of data retrieval and to Attribute Authority (AA) at the time of data storing. This leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. It is mainly used in situation where both users and storage service providers are untrusted. The main advantages of this scheme are highly secure compared to existing ABE shemes and also reduces the overload of attribute authority.

REFERENCES

[1] Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang, ‘‘Securely Outsourcing Attribute-Based Encryption with Checkability’’, *Parallel and Distributed Systems,IEEE Transactions on,* On page(s): 2201 - 2210 Volume: 25, Issue: 8, August 2014

[2] A. Sahai and B. Waters, ‘‘Fuzzy Identity-Based Encryption,’’ in Proc. Adv. Cryptol.-EUROCRYPT, LNCS 3494, R. Cramer, Ed.,Berlin, Germany, 2005, pp. 457-473, Springer-Verlag.

[3] D.Boneh and M. Franklin. “Identity-Based Encryption from the Weil Pairing.” Proc. of CRYPTO’01, Santa Barbara, California, USA, 2001.

[4] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption,’’ in Proc. IEEE Symp. Security Privacy, May 2007, pp. 321-334.

[5] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, ‘‘Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption,’’ in Proc. 18th ESORICS, 2013, pp. 592-609.

[6] L. Cheung and C. Newport, ‘‘Provably Secure Ciphertext Policy ABE,’’ in Proc. 14th ACM Conf. CCS, 2007, pp. 456-465.

[7] M. Green, S. Hohenberger, and B. Waters, ‘‘Outsourcing the Decryption of ABE Ciphertexts,’’ in Proc. 20th USENIX Conf. SEC, 2011, p. 34.

[8] S. Hohenberger and A. Lysyanskaya, ‘‘How to Securely Outsource Cryptographic Computations,’’ in Proc. Theory Cryptogr., LNCS 3378, J. Kilian, Ed., Berlin, Germany, pp. 264-282, Springer- Verlag.
[9] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’10), 2010.
[10] V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, “Multiauthority attribute-based encryption with honest- but-curious central authority" International Journal of Computer Mathematics, vol. 89,pp. 3,2012.
[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ‘‘Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,’’ in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89-98.
[12] J.Lai, R. Deng, C. Guan, and J. Weng, ‘‘Attribute based Encryption with Verifiable Outsource d Decryption,’’ IEEE Trans.Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354, Aug. 2013.
[13] S.Yu,C. Wang,K.Ren, and W. Lou, ‘‘Achieving Secure, Scalable, Fine Grained Data Access Control in Cloud Computing,’’ in Proc. IEEE 29th INFOCOM, 2010, pp.534-542.
[14] M.J. Atallah, K. Pantazopoulos, J.R.Ricea,E.E. Spafford, ‘‘Secure Outsourcing of ScientificComputations,’’ in Trends in Software Engineering, vol.54, M.V.Zelkowitz,Ed.Amsterdam, The Netherlands: Elsevier, 2002, pp. 215-272.
[15] M.J.Atallah and J.Li,‘‘Secure Outsourcing of Sequence Comparisons,’’Int’l J.Inf.Security,vol. 4, no. 4, pp.277-287, Oct. 2005.
[16] M.J. Atallah and K.B. Frikken, ‘‘Securely Outsourcing Linear Algebra Computations,’’ in Proc. 5th ACM Symp. ASIACCS, 2010, pp. 48-59.
[17] C. Wang, K. Ren, and J. Wang, ‘‘Secure and Practical Outsourcing of Linear Programming in Cloud Computing,’’ in Proc. IEEE INFOCOM, 2011, pp. 820- 828.
[18] C. Gentry, ‘‘Fully Homomorphic Encryption Using Ideal Lattices,’’ in Proc. 41st Annu. ACM
[19] STOC, 2009, pp.169-178.
[20] C.Gentry and S.Halevi,‘‘ImplementingGentry’s Fully- Homomorphic Encryption Scheme,’’ in Proc. Adv.Cryptol.-EUROCRYPT, LNCS 6632, K. Paterson, Ed.,Berlin, Germany, 2011, pp.
[21] 129-148, Springer-Verlag.
[22] J. Li, C. Jia, J. Li, and X. Chen, ‘‘Outsourcing Encryption of Attribute-Based Encryption with Mapreduce,’’ in Proc.Int’l Conf. Inf. Commun. Security, 2012, pp. 191-201