INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A NOVEL APPROACH FOR CONSTRUCTION OF EFFICIENT ATTRIBUTE BASED ENCRYPTION WITH VERIFIABLE OUTSOURCED DECRYPTION

MR. M. D. GHODESWAR, DR. S. S. SHEREKAR, DR. V. M. THAKARE

SGBAU Amravati, India.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* Cloud computing is the technique which supports flexible, on-demand and low cost usage of computing resources but the various privacy concerns emerge from it. Attribute Based Encryption scheme with outsourced decryption enables sharing of encrypted data, but also overcomes efficiency drawback in terms of decryption cost of standard ABE scheme. In this paper a novel approach for construction of efficient Multi-authority ABE with verifiable outsourced decryption is proposed, which helps to reduce the computation time required for the decryption.

Keywords: Attribute-Based Encryption, Outsourced Decryption, Multi-Authority, Verifiability

Corresponding Author: MR. M. D. GHODESWAR

Access Online On:

www.ijpret.com

How to Cite This Article:

M. D. Ghodeswar, IJPRET, 2016; Volume 4(9): 1704-1712

PAPER-QR CODE

INTRODUCTION

Attribute based encryption provides flexible access control and data confidentiality functionalities; it has become a promising technique for building secure access in practical distributed systems. The drawback of existing ABE scheme is decryption which involves expensive pairing operations and the number of such operation leads to the complexity of the access policy. Various techniques are proposed to protect the data contents privacy via access control.

This paper discusses the few techniques to improve the efficiency of decryption in anonymous ABE. These techniques reduce the computation time required for the decryption operation. But these methods also have some problem so to overcome such problems improved version of ABE scheme is proposed**.**

I) Background

To protect the data contents privacy via access control various techniques have been proposed. Identity-based encryption (IBE) was introduced first, in which the sender of a message can specify an identity such that only a receiver with matching identity can decrypt it. Few years later, Fuzzy Identity-Based Encryption is introduced, which is also known as Attribute-Based Encryption (ABE). In such encryption scheme, an identity is viewed as a set of descriptive attributes and decryption is possible if a decryptor's identity has some overlaps with the one specified in the ciphertext. Soon after, more general tree-based ABE schemes, Key-Policy Attribute-Based Encryption (KP-ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE), are presented to express more general condition than simple 'overlap'. They are counterparts to each other in the sense that the decision of encryption policy is made by different parties.

In the KP-ABE, a ciphertext is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user's identity. A user can decrypt the ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext. However, the encryption policy is described in the keys, so the encryptor does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation. On the other hand, those problems and overhead are all solved in the CP-ABE. In the CP-ABE, ciphertexts are created with an access structure, which specifies the encryption policy, and private keys are generated according to users' attributes. A user can decrypt the ciphertext if and only if his

attributes in the private key satisfy the access tree specified in the ciphertext. By doing so, the encryptor holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system reboots.

This paper introduces some techniques which provide efficient and verifiable outsourced decryption these are organized as follows. **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected. **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

II) Previous Work Done

In research literature, to improve the efficiency of decryption in anonymous ABE different techniques are studied. Junzuo Lai et al. (2013) [1] has proposed original model of ABE with outsourced decryption to allow for the verifiability of the transformations. After describing the formal definition of verifiability, author has proposed a new ABE model and construct a new model called concrete ABE with verifiable outsourced decryption. This scheme does not rely on random oracles. Yingui Zhang et al. (2013) [2] has proposed a new technique match-then-decrypt in to the decryption of anonymous ABE, in which match-then-decrypt phase is added. Taeho Jung et al. (2015) [3] has proposed AnonyControl and AnonyControl-F to allow cloud servers to control users access privileges without knowing their identity information. The proposed schemes are able to protect user's privacy against each single authority. Partial information is disclosed in AnonyControl and no information is disclosed in AnonyControl-F. Baodong Qin et al. (2015) [4] have proposed an efficient method to verify the correctness of the transformed ciphertext in an ABE system with outsourced decryption. This scheme works in the key encapsulated mechanism (KEM). Suqing Lin et al. (2015) [5] has proposed a novel technique to build an ABE with verifiable outsourced decryption based on a AB-KEM, a symmetric key encryption scheme and a commitment scheme. This scheme provides VO-ABE which can be considered in both key-policy and ciphertext-policy setting.

III) Existing Methodologies

Many ABE schemes with verifiable outsourced decryption are implemented. These techniques are implemented to achieve verifiability, security, low cost of decryption etc. A CP-ABE scheme consists of four algorithms: Setup, Key Gen, Encrypt and Decrypt.

In the first scheme CP-ABE scheme with outsourced decryption consists of seven algorithms: Setup, Key Gen, Encrypt, Decrypt, and Gen TK $_{out}$, Transform $_{out}$, Decrypt $_{out.}$ In this model Decrypt $_{out}$ includes the original ciphertext and the transformed ciphertext. User needs to know only the small part of the original ciphertext to verify the correctness of the transformation done by the cloud in the algorithm Decrypt $_{out}$. Following fig shows the ABE system with outsourced decryption. In this scheme, re-encryption is done with the help of proxy. But there is no way to verify the proxy's transform. Since the proxy is untrusted and hence verifiable outsourced decryption is needed.

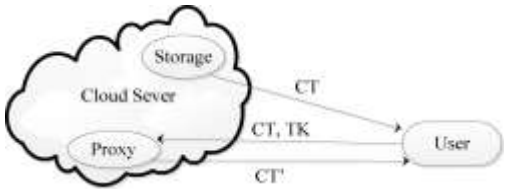

Fig 1: ABE system with Outsourced Decryption

In second scheme anonymous CP-ABE consists of four algorithms: Setup, Key Gen, Encrypt and Decrypt where Decrypt algorithm involves two phases i.e. attribute matching detection and decryption phase.

In the third scheme analysis on security and performance is given to show feasibility of the scheme AnonyControl and AnonyControl-F. In this scheme multi-authority based encryption AnonyControl and AnonyControl-F is implemented.

In the fourth scheme, underlying outsourced ABE system work in the KEM setting i.e. it encrypts a random key rather than real message. Instead of using the random key to symmetrically encrypt data intermediate verification key is computed and then extractor is used to derive a symmetric key. Finally, symmetric encryption scheme is used to hide the real message and verification key is computed. The later implicitly guarantees the correctness of the recovered random key. Following fig shows the system model for the proposed method. In this scheme a separate cloud storage server and the ciphertext transformation server is used.

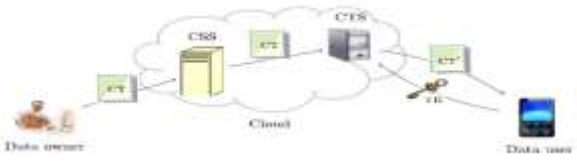

Fig 2: System Model for ABE with outsourced Decryption

In the fifth scheme, the model of CP-ABE with outsourced decryption consists of seven algorithms (Setup, Key Gen, Encrypt, Decrypt, Gen TK $_{out}$, Transform $_{out}$, Decrypt $_{out}$). A trusted party generates the public parameters and a master secret key by running the algorithm Setup, and a user obtains a private key generated by the trusted party running Key Gen. After taking the ciphertext, the user decides whether to outsource decryption of the ciphertext. If the user wants to outsource decryption, he can execute the algorithm Gen TK out and use his private key to generate the transform key by himself. Taking as input the transform key and a ciphertext, the proxy is able to change the ciphertext into a constant-size ciphertext by the algorithm transform out if the set of attributes associated with the private key satisfies the access structure associated with the ciphertext.

IV) Analysis and Discussion

The ABE ciphertext size and decryption/transformation time increase linearly as the ciphertext policy's complexity grows. Outsourcing substantially reduces the computation time required for devices with limited computing resource to recover the plaintext. The bulk of the decryption operation is now handled by the proxy. The transformed ciphertext is not only much efficient to decrypt but also much smaller in size.

Match then decrypt presents the security comparison with respect to the complexity assumption, the security model and anonymity. This scheme achieves the goal of protecting users' privacy and they have the same access policy.

Semi anonymous privilege control scheme AnonyControl to address not only the data privacy, but also the user identity privacy in existing access control schemes. AnonyControl decentralizes the central authority to limit the identity leakage and thus achieves semi anonymity. AnonyControl-F fully prevents the identity leakage and achieves the full anonymity.

For the three schemes, almost all the ciphertext processing is outsourced to a cloud server and that the outsourced ciphertext size and decryption time increase linearly with the number of policy attributes, while the local ciphertext size and decryption time are kept small and constant. The new scheme is verifiable and has nearly the same efficiency as the underlying non-verifiable scheme. Though the schemes are both verifiable, the former is much more efficiency in both ciphertext size and decryption time than the latter.

The computation cost for the third-party service to transform a standard ABE ciphertext in our scheme is half of that in Therefore; ABE with verifiable outsourced decryption is more efficient than the existing scheme.

ABE scheme	Advantages	Disadvantages
VO-ABE	It reduces the computation time do the devices with limited computing resources to recover the plaintext.	This scheme does not rely on random oracles.
Match-then-decrypt	This method improves the efficiency of decryption in anonymous ABE.	Complexity of the construction is quite high.
Multi-Authority Anonymous ABE	AnonyControl is secure and efficient for cloud storage system.	Extra communication overhead is required during 1-out-of-n oblivious transfer in AnonyControlF.
Efficient VO-ABE scheme	This scheme is more efficient and decryption time is faster.	The drawback of this scheme is it introduces minimal overhead in exchange for verifiability.
Revisiting VO-ABE	This scheme reduces the computation time required for encryption time, transform time and the time of decrypting a transformed text.	The drawback of this scheme is, it is Selectively secure

TABLE 1: Comparison between various ABE Schemes

V) Proposed Methodology

Multi-Authority VO-ABE algorithms

In the proposed methodology, an efficient technique to verify the ciphertext in anonymous ABE system with outsourced decryption with multiple authorities is discussed. The algorithms used are setup, key gen, encrypt, decrypt, gen tk, transform out, verify and decrypt'. Each algorithm works independently and finally provides efficient outsourced decryption with less computation cost and also provides security and verifiability. Following diagram shows the system model of the proposed method.

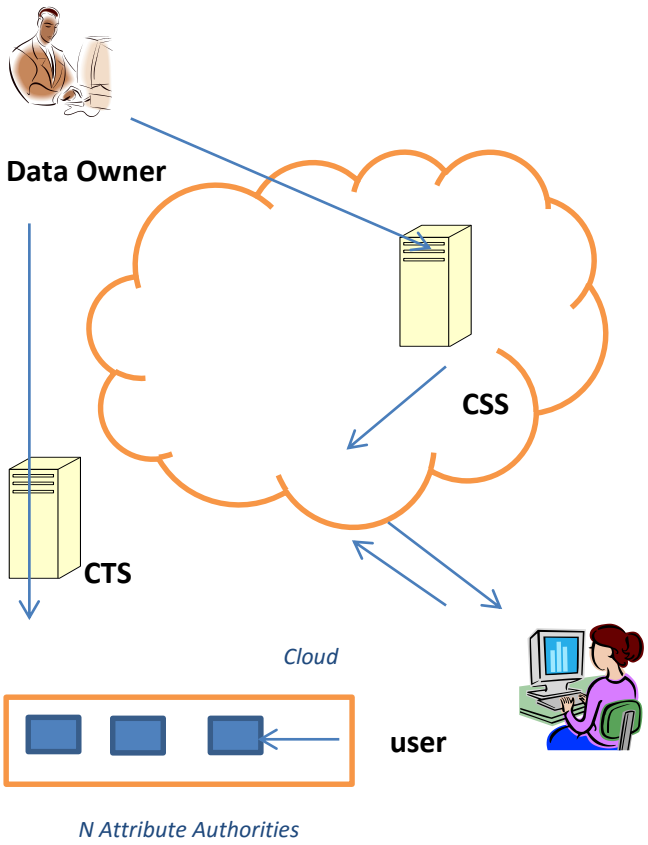

Fig3: System Model of Multi-Authority ABE

Abbreviation used in Fig 3

CSS – Cloud Storage Server

CTS: Ciphertext Transformation Server

1. Setup

This algorithm takes nothing as input. Attribute authorities execute this algorithm and compute public key as well as authority wise public parameter for individually computing a master key.

2. Key Gen

This algorithm enables user to interact with every attribute authority and obtain a private key.

3. Encrypt

This algorithm takes public key and message as input and outputs ciphertext

4. Decrypt

This decryption algorithm takes public key, private key, ciphertext and returns a message.

5. Gen TK

The transform key generation algorithm takes as input public key, ciphertext and private key then outputs a transformed key

6. Transform out

The transform algorithm takes as input public key, ciphertext, transform key the outputs a transformed ciphertext

7. Verify

The verification algorithm takes input as public key, a transformed ciphertext and secret value and then outputs a bit and status value.

8. Decrypt

The decryption algorithm takes as input public key, ciphertext and secret value then run verify algorithm. To obtain bit ans status value

If b= 1

Outputs message

Else return error symbol

VI) Outcome Possible Result

The proposed method, multiauthority based VO-ABE will successfully improves the efficiency of decryption test. Also it achieves verifiability and security.

VII) Conclusion

This paper is focused on various techniques of efficient construction of attribute-based encryption with verifiable outsourced decryption, so the proposed scheme will improve the performance of decryption operation performed.

IX) FUTURE SCOPE:

The efficient user revocation mechanism must be introduced as the future work

REFERENCES:

1. Junzuo Lai, Robert H Deng, Chaowen Guan, Jian Weng, "Attribute-Based Encryption with Verifiable Outsourced Decryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol . 8, No. 8, PP. 1343-1354, AUGUST 2013.
2. Yinghui Zhang, Xiaofeng Chen, Jin Li, Duncan Wong, Hui Li, "Anonymous Attribute-Based Encryption Supporting Efficient Decryption Test", In Proc of ASIA CCS'13, Hangzhou, China, PP. 511-516 ACM Press. 2013.
3. Taeho Jung, Xiiang-Yang Li, Zhiguo Wan, Meng Wan, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol. 10, No. 1, January 2015.
4. Baodong Qin, Robert H. Deng, Shengli Liu, and Siqi Ma, "Attribute-Based Encryption With Efficient Verifiable Outsourced Decryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 7, JULY 2015.
5. Suqing Lin, Rui Zhang, Hui Ma, and Mingsheng Wang, "Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO.10,OCTOBER2015