INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue1)
Available online at: www.ijariit.com

Cipher Text Policy Attribute-Based Encryption Supporting Flexible Attributes

Mr. M. D. Ghodeswar
SGBAU Amravati, India
mdghodeswar@gmail.com

Dr. Mrs. S. S. Sherekar
SGBAU Amravati, India
ss_sherekar@rediffmail.com

Dr. V. M. Thakare
SGBAU Amravati, India
vilthakare@yahoo.com

Abstract*— Ciphertext Policy Attribute-Based Encryption (CP-ABE) has been a very active research area in recent years. Because of two properties traceability and large universe, CP-ABE is enriching the commercial applications. But to achieve this it requires more computation overhead. In this paper a novel approach for construction of efficient ciphertext policy ABE supporting flexible attributes is proposed, which helps to reduce the computation overhead and improves security by providing privacy preserving data access policies.

Keywords*— Attribute-Based Encryption, Ciphertext Policy, Privacy, Traceability.

I. INTRODUCTION

In CP-ABE each user possesses a set of attributes and can decrypt the ciphertext if his/her attributes satisfy the ciphertext's access policy. This results in an obvious consequence that the encryptor or system does not know who leaks the decryption key to others intentionally. Due to the fact that the attributes are shared by multiple users and different users may have the same subset of attributes, the encryptor or system has no feasible method to trace the suspicious receiver if the decryption key is leaked.

The two new large universe CP-ABE systems are proposed, the Traceable Large Universe CP-ABE system (the T-LU-CPABE system) and the enhanced Traceable Large Universe CP-ABE system (the eT-LU-CPABE system), which are white-box1 traceable on prime order bilinear groups. To the best of our knowledge, both the T-LU-CPABE system and the eT-LU-CPABE system are the first practical CP-ABE systems that simultaneously support the following two properties: white-box traceability and large universe.

Moreover, the eT-LU-CPABE system achieves another remarkable property: constant storage for traitor tracing. Compared with other constructions based on Composite order groups, constructions on the efficient prime order bilinear groups are built. The new system is proved to be selectively secure in the standard model.

II. BACKGROUND

In Attribute based encryption scheme with fuzzy version of IBE each users private key is associated with a set of attributes and each ciphertext is encrypted by an access policy. To decrypt the message, the attributes in the user private key need to satisfy the access policy. The key difference between identity and attribute is that identities are many-to-one mapped to users while attributes are many-to-many mapped to users. Thus, to simulate a constant size conjunctive header, one need to encrypt the message using each receiver's identity and the size of ciphertext is linearly increasing.

Then after CP-ABE scheme with constant size conjuctive headers and constant number of pairing operations is proposed. Then a more general construction of CP-ABE with constant ciphertext is proposed. This scheme achieves constant ciphertext with any monotonic threshold data access policy. After that a novel approach is proposed to the hidden policy to preserve privacy efficiently. The main difference between PP-CP-ABE and existing hidden policy attribute based encryption schemes is PP-CP-ABE significantly reduced the size of ciphertext to a constant size that is linearly increasing on the number of attributes in the hidden policy.

This paper introduces some techniques which traceability using CP-ABE scheme for error tracing 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.

III. PREVIOUS WORK DONE

In research literature, to reduce the ciphertext size from linear to constant and supports expressive access policies various techniques are studied. Zhibin Zhou et al. (2015) [1] has proposed novel PP-CP-ABE construction, named Privacy Preserving Constant-size Ciphertext Policy Attribute Based Encryption (PP-CP-ABE), which enforces hidden access policies with wildcards and incurs constant-size conjunctive headers, regardless of the number of attributes. Each conjunctive ciphertext header only requires 2 bilinear group elements, which are bounded by 100 bytes in total. Junzuo Lai et al. (2012) [2] has proposed In many applications, specific attribute values carry much more sensitive information than the generic attribute names. This observation motivated to consider a new model of CP-ABE with partially hidden access structures. In this model, each attribute includes two parts: attribute name and its value; if the set of attributes associated with a user's private key does not satisfy the access structure associated with a ciphertext, attribute values in the access structure are hidden, while other information, such as attribute names, about the access structure is public. Zhen Liu et al. (2015) [3] has proposed the scheme is also selectively traceable against policy-specific decryption blackbox. More importantly, a general statement that if a CP-ABE scheme is (selectively) traceable against policy-specific decryption blackbox, it is also (selectively) traceable against key-like decryption blackbox, which implies that there is a need to focus on building CP-ABE schemes which are traceable against policy-specific decryption blackbox. Zhen Liu et al. (2013) [4] have proposed a new CP-ABE which is fully secure (i.e. provably secure against adaptive adversaries in the standard model), highly expressive (i.e. supporting any monotonic access structures), and blackbox traceable. Furthermore, this new CP-ABE achieves fully collusion-resistant blackbox traceability, that is, the tracing algorithm can find out at least one of the malicious users even if there are an arbitrary number of malicious users colluding by pulling all of their decryption keys together when building a key-like decryption blackbox. Note that collusion-resistant traceability is orthogonal to collusion-resistant security, which is the primary requirement of CP-ABE., Traceability is regarded as an additional feature besides the traditional CPABE full security, high expressivity and efficiency. Jinguang Han et al. (2015) [5] has proposed a privacy-preserving DCP-ABE (PPDCP-ABE) scheme where the central authority is not required and each authority can work independently without any cooperation. As a notable feature, each authority can dynamically join or leave the system, namely other authorities do not need to change their secret keys and reinitialize the system when an authority joins or leaves the system. Each authority monitors a set of attributes and issues secret keys to users accordingly.

IV. EXISTING METHODOLOGIES

Many CP-ABE schemes for preserving privacy and security 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.

PP-CP-ABE: construct an efficient Privacy Preserving Constant Ciphertext Policy Attribute Based Encryption (PP-CP-ABE) scheme that enforces hidden conjunctive access policies with wildcards in constant ciphertext size. To the best of our knowledge, this is the first construction that achieves these properties [1].

PP-AB-BE: Based on PP-CP-ABE, a Privacy Preserving Attribute Based Broadcast Encryption (PPAB-BE) scheme is presented. Compared with existing BE schemes, PP-AB-BE is flexible as it uses both descriptive and non-descriptive attributes, which enables a user to specify the decryptors based on different abstraction levels, with or without exact information of intended receivers. Moreover, PP-AB-BE demands less storage overhead compared to existing BE schemes. Construction of this scheme requires minimal storage to support all the possible user group formations for BE applications [2].

In this model, each attribute includes two parts: attribute name and its value; if the set of attributes associated with a user's private key does not satisfy the access structure associated with a ciphertext, attribute values in the access structure are hidden, while other information, such as attribute names, about the access structure is public [3].

The CP-ABE scheme proposed in the preliminary version is selectively traceable against policy-specific decryption blackbox. Combining the results in preliminary version and a fully secure and highly expressive CP-ABE scheme which is adaptively traceable against key-like decryption blackbox and selectively traceable against policy-specific decryption blackbox is found to be fully efficient and secure [4].

CP-ABE that simultaneously supports public and fully collusion-resistant blackbox traceability, full security, high expressivity, and without the one-use restriction, and for a system with fully collusion-resistant blackbox traceability, sub-linear overhead is the most efficient one to date are fully secure and highly expressive. a privacy-preserving DCP-ABE (PPDCP-ABE) scheme where the central authority is not required and each authority can work independently without any cooperation. As a notable feature, each authority can dynamically join or leave the system, namely other authorities do not need to change their secret keys and reinitialize the system when an authority joins or leaves the system. Each authority monitors a set of attributes and issues secret keys to users accordingly. To resist the collusion attacks, a user's secret keys are tied to his GID. Especially, a user can obtain secret keys for his attributes from multiple authorities without them knowing any information about his GID and attributes. Therefore, the proposed PPDCP-ABE scheme can provide stronger privacy protection compared to the previous PPMA-ABE schemes where only the GID is protected [5].

V. ANALYSIS AND DISCUSSION

Constant Ciphertext Policy Attribute Based Encryption (PP-CP-ABE) was proposed. Compared with existing CP-ABE constructions, PP-CP-ABE significantly reduces the ciphertext size from linear to constant and supports expressive access policies.

Efficient CP-ABE can handle any access structure that can be expressed as an LSSS. Previous CP-ABE schemes with partially hidden access structures only support restricted access Structures.

The Blackbox traceable CP-ABE scheme is proved secure against adaptive adversaries in the standard model. For the traceability against key-like decryption blackbox, the scheme is proved traceable against adaptive adversaries in the standard model, and for the traceability against policy-specific decryption blackbox, the scheme can be proved traceable against selective adversaries in the standard model.

In PPDCP-ABE scheme both the privacy of the GID and the attributes are concerned. In this scheme, a central authority is not required and multiple authorities can work independently without any cooperation.

TABLE I
Comparison Between various CP-ABE schemes

ABE scheme	**Advantages**	**Disadvantages**
PP-CP-ABE	Significantly reduces the ciphertext size from linear to constant and supports expressive access policies minimal storage overhead	only supports conjunctive access policy
CP-ABE with Partially Hidden Access Structures	Can handle any access structure.	Expressive CP-ABE constructions with partially hidden access structures from simple assumptions
Traceable CP-ABE	selectively traceable against policy-specific decryption blackbox	prime order group CP-ABE scheme
Blackbox Traceable CP-ABE	high expressivity and full security fully collusion resistant (and public) blackbox traceability	The drawback of this scheme is it introduces minimal overhead
Decentralized CP-ABE	Protect users' privacy and reduce the trust on the central authority	Selectively secure.

VI. PROPOSED METHODOLOGY

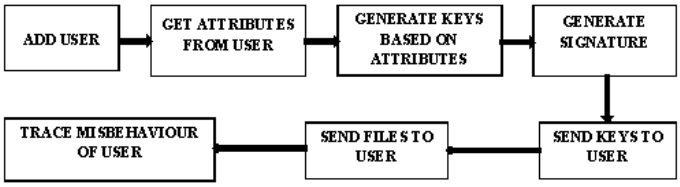

Fig 1: CP-ABE SFA

VII. OUTCOME POSSIBLE RESULT

The proposed method, ciphertext policy attribute based encryption supporting flexible attribute will successfully improves the traceability of the decryption keys used.

CONCLUSIONS

The property of white-box traceability in CP-ABE is achieved, which could trace the malicious users leaking the partial or modified decryption keys to others for profits. Also the property of large universe in whitebox traceable CP-ABE is obtained where the attributes' size is unbounded and the public parameters' size does not grow linearly with the number of attributes. In addition, the system is optimized in tracing the malicious users to cut down the storage cost for traceability and to make the system efficient in the revocation of the users.

ACKNOWLEDGMENT

. This work is supported by the Office of Research, Sant Gadge Baba Amravati University.

REFERENCES

[1] Zhibin Zhou, Dijiang Huang, Zhije Wang, "Efficient Privacy Preserving Ciphertext-Policy Attribute Based-Encryption and Broadcast Encryption", IEEE TRANSACTIONS ON COMPUTERS, Vol . 64, No. 1, PP. 126-138, JANUARY 2015.

[2] Junzuo Lai, Robert Deng, Yingjiu Li, "Expressive CP-ABE with partially Hidden Access Structures", In Proc of ASIA CCS'12, Seoul, Korea, ACM Press. 2012.

[3] Zhen Liu, Zhenfu Cao, Duncan Wong, "Traceable CP-ABE: How to Trace Decryption Devices Found in the Wild", IEEE TRANSACTIONS ON INFORMATION FORENSICS, Vol. 10, No. 1, January 2015.

[4] Zhen Liu, Zhenfu Cao, Duncan Wong, "Blackbox Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Devices on eBay", IEEE TRANSACTIONS ON COMPUTER SECURITY, VOL. 10, NO. 7, JULY 2015.

[5] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, Man Ho Allen Au, "Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO.3, MARCH 2015

