ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Improving a New Approach For Providing Privacy Preserving With Attribute Based Encryption

T.Yamini Koteswari
M.Tech Student,
Department of CSE
Vignan's Nirula Institute of Technology And Science For Women,
Pedapalakaluru, Guntur-522 005.

Dr. B.Bhanu Prakash
Associate Professor
Department of CSE
Vignan's Nirula Institute of Technology And Science For Women,
Pedapalakaluru, Guntur-522 005.

ABSTRACT:

Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the versatility of access control mechanisms. Due to the high expressiveness of ABE policies, the computational complexities of ABE key-issuing and decryption are getting prohibitively high. Despite that the existing Outsourced ABE solutions are able to offload some intensive computing tasks to a third party, the verifiability of results returned from the third party has yet to be addressed. Aiming at tackling the challenge above, we propose a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption. Our new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. In addition, for the first time, we propose an outsourced ABE construction which provides checkability of the outsourced computation results in an efficient way. Extensive security and performance analysis show that the proposed schemes are proven secure and practical

Index Terms— Attribute-based encryption, access control, outsourcing computation, key issuing, checkability

INTRODUCTION:

A novel public key primitive, attribute-based encryption (ABE)Until now, there are two kinds of ABE having been proposekey-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. Recently, as the development of cloud computing [2], users' concerns about data security are the main obstaclesthat impedes cloud computing from wide adoption. These concerns are originated from the fact that sensitive dataresides in public cloud, which is maintained and operated by untrusted cloud service provider (CSP). ABE provides asecure way that allows data owner to share outsourced data on untrusted storage server instead of trusted serverwith specified group of users. This advantage makes the methodology appealing in cloud storage that requires secureaccess control for a large number of users belonging to different organizations. Nevertheless, one of the main efficiency drawbacks of ABE is that the computational cost during decryption phasegrows with the complexity of the access formula.

Thus, before widely deployed, there is an increasing need to improve the efficiency of ABE. To address this problem, outsourced ABE, which provides a way to outsource intensive computing task during decryption to CSP withoutrevealing data or private keys,was introduced [3], [4]. It has a wide range of applications. For example, in the mobile cloud computing consisting of mobile devices or sensors as information collection nodes, user terminal (e.g., mobile device) has limited computation ability to independently complete basic

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

encryption or decryption to protect sensitive data residing in public cloud. Outsourced ABE allows user to perform heavy decryption through ‘‘borrowing’’ the computation resources from CSP. Therefore, in this paradigm, the computation/storage intensive tasks can be performed even by resource-constrained users.

That the attribute authority has to deal with a lot of heavy computation in a scalable system. More precisely, the attribute authority has to issue private keys to all users, but yet generation of private key typically requires large modular exponentiation computation, which grows linearly with the complexity of the predicate formula.

Existing system

In order to facilitate the development, delivery and reuse of environmental software models, service orientation has been recently pushed forward by several important initiatives1;2;3 and international standardization bodies4 in the environmental domain. In the light of those efforts, both geospatial data and geo-processing units are exposed as Web services, which can be used as building blocks for the composition of environmental models in the form of BPEL processesseveral challenges arise upon this paradigm shift. Efficient execution and monitoring of long-running environmental processes that consume and produce large volumes of data, in the presence of multiple concurrent process instances are among the prominent issues that one should effectively deal with Aiming at eliminating the most overhead computation at both the attribute authority and the user sides, we propose an outsourced ABE scheme not only supporting outsourced decryption but also enabling delegating key generation.

Following our technique, constant efficiency is achieved at both attribute authority and user sides. In addition, we observe that when experiencing commercial cloud computing services, the CSPs may be selfish in order to save its computation or bandwidth, which may cause results returned incorrectly. In order to deal with this problem, we consider to realize checkability on results returned from both KGSP and DSP, and provide a security and functionality enhanced construction, which is provable secure under the recent formulized refereed delegation of computation (RDoC) model.

Proposed System

In an effort to address situations such as the one described previously, we introduce a framework comprising a scalable Peer-to-Peer (P2P) architecture and a set of distributed algorithms to support construction of KP-ABE was provided in the same paper [6],while the first CP-APE construction supporting tree-based structure in generic group model is presented by . [7]. Accordingly, several constructions supporting for any kinds of access structures were provided [8],[9] for practical applications [10], [11]. Concerning revocation of ABE, a delegatable revocation is proposed in [12] to achieve scalable and fine-grained access control. To reduce the load at local, it always desires to deliver expensive computational tasks outside. Actually, the problem that how to securely outsource different kinds of expensive computations has drew considerable attention from theoretical computer science community.

Atallah et al. presented a framework for secure outsourcing scientific computations such as matrix multiplication and Another several related work similar to us are for outsourcing the enabling checkability on returned results from CSPs. Recently Lai et al. [28] 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.

MODULES:

- Key Management.
- Security Requirements.
- CP-ABE SCHEME

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- User
- Data Owner

KEY MANAGEMENT:

Key management describes the data sharing architecture and defines the security model. This consists of Key generation center, Data-storing center, Data owner, and User.

Key generation center: It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. It is assumed to be honest-but-curious Data-storing center: is an entity provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services.

SECURITY REQUIREMENT:

Data confidentiality:

Unauthorized users who do not have enough attribute satisfying the access policy should be prevented from accessing the plaintext of the data. Additionally, the KGC is no longer fully trusted in the data sharing system. Thus, unauthorized access from the KGC as well as the data-storing center to the plaintext of the encrypted data should be prevented. Collusion resistance is one of the most important security property required in ABE systems .If multiple users collude, they may be able to decrypt a cipher-text by combining their attributes even if each of the users cannot decrypt the cipher-text alone.

Since we assume the KGC and data-storing center are honest, we do not consider any active attacks from them by colluding with revoked users as in. Backward and forward secrecy. In the context of attribute-based encryption, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data distributed before he holds the attribute.

CP-ABE SCHEME:

In this section, we develop a variation of the CP-ABE algorithm partially based on (but not limited to) Bethen court et al.'s construction in order to enhance the expressiveness of the access control policy instead of building a new CP-ABE scheme from scratch. Its key generation procedure is modified for our purpose of removing escrow. The proposed scheme is then built on this new CP-ABE ariation by further integrating it into the proxy re-encryption protocol for the user evocation. To handle the fine-grained user revocation, the data storing center must obtain the user access (or revocation) list for each attribute group, since otherwise revocation cannot take effect after all. This setting where the data-storing center knows the revocation list does not violate the security requirements, because it is only allowed to re-encrypt the ciphertexts and can by no means obtain any information about the attribute keys of users.

USER:

It is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the cipher-text and obtain the data.

DATA OWNER:

Administrator can enter in to the website with his credentials. He allows to upload it into the external data-storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute-based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it.

ORGANIZATION

This paper is organized as follows. In Section 2 we describe some preliminaries. In Section 3, we present the system model and security definition. The proposed construction and its security analysis are presented in, we consider a both security and functionality enhanced construction under RDoC model.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

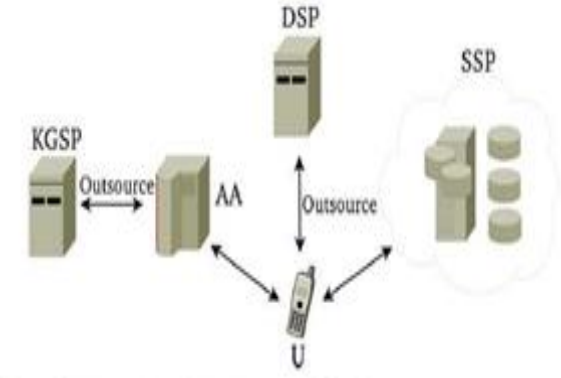

Fig. 1. System model for outsourced ABE scheme.

Cryptographic Background

In this paper, we use the bilinear pairings on elliptic curves. We now give a brief review on the property of pairing and the candidate hard problem that will be used.

Definition 1 (Bilinear Map). Let G;GT be cyclic groups of prime order q, writing the group action multiplicatively. g is a generator of G. Let e : G _G ! GT be a map with the following properties:

Definition 2 (DBDH Problem). The decision Bilinear Diffie- Hellman (DBDH) problem is that, given we say that the ðt; _Þ-DBDH assumption holds in G if no t-time algorithm has probability at least 2 þ _ in solving the DBDH problem for non-negligible

System Model

We present the system model for outsourced ABE scheme in Fig. 1. Compared with the model for typical ABE, a KGSP and a DSP are additionally involved. KGSP is to perform aided key-issuing computation to relieve AA load in a scale system when a large number of users make requests on private key generation and key-update.DSP is to complete delegated expensive operations to overcome the disadvantage that the decryption phase in typical ABE requires a large number of overload operations at U.

Following the custom in [3], we denote ðIenc; IkeyÞ as the input to encryption and key generation. In CP-ABE scheme, ðIenc; IkeyÞ ¼ ðA; !Þ while that is ð!;AÞ in KPABE, where ! and A are attribute set and access structure, respectively. Then, based on the proposed system model, we provide algorithm definitions as follows. Setupð_Þ: The setup algorithm takes as inputVa security parameter. It outputs a public key PK and a master key MK.

KeyGeninitðIkey;MKÞ :

For each user's private key request, the initialization algorithm for delegated key generation takes as inputVan access policy (or attribute set) Ikey and the master key MK. It outputs the key pair ðOKKGSP; OKAAÞ. KeyGenoutðIkey; OKKGSPÞ : The delegated key generation algorithm takes as inputVthe access structure (or attribute set) Ikey and the key OKKGSP for KGSP. It outputs a partial transformation key TKKGSP.KeyGeninðIkey; OKAAÞ : The inside key generation algorithm takes as inputVthe access structure (or attribute set) Ikey and the key OKAA for attribute authority. It outputs another partial transformation key TKAA.

KeyBlindðTKÞ : The transformation key blinding algorithm takes as inputVthe transformation key TK ¼ ðTKKGSP; TKAAÞ. It outputs a private key SK and a blinded transformation key f TK.

EncryptðM; IencÞ: The encryption algorithm takes as inputVa message M and an attribute set (or access structure) Ienc to be encrypted with. It outputs the ciphertext CT.

DecryptoutðCT; f TKÞ : The delegated decryption algorithm takes as inputVa ciphertext CT which was assumed to be encrypted under the attribute set (or access structure) Ienc and the blinded transformation key f TK for access structure (or attribute set) Ikey. I outputs the partially decrypted ciphertext CTpart if _ðIkey; IencÞ ¼ 1, otherwise outputs ?, where _ð_; _Þ is a predicate predefined.

DecryptðCTpart; SKÞ: The decryption algorithm takes as inputVthe partially decrypted ciphertext CTpart and the private key SK. It outputs the origina message M.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Security Definition

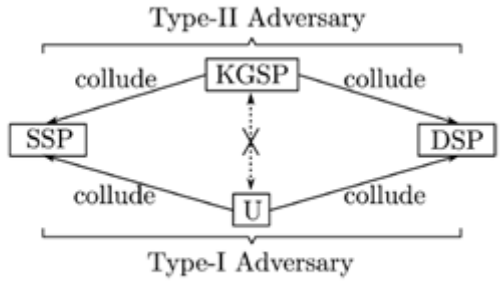

Fig. 2. Adversary model for outsourced ABE scheme.

In this work, we assume that all the entities except AA are‘‘honest-but-curious’’. More precisely, they will follow proposed protocol but try to find out as much private ciphertext intended for users not in the group. Type-II adversary defined as KGSP colluding withSSP and DSP, is able to potentially access all the keys for KGSP, all the ciphertexts stored at SSP, all theblinded transformation keys stored at DSP, etc, andaims to decrypt any ciphertext.Having this intuition, we follow the RCCA (replayablechosen ciphertext attack) security in [29], [3] to defineRCCA security. For saving space, we just show the definitionof RCCA security here, and the detailed game can berefered to Appendix A, which is (RCCA Security). An outsourced CP-ABE orKP-ABE scheme with delegated key generation and decryption is secure against replayable chosen-ciphertext attack ifall polynomial time adversaries have at most a negligible advantage in the RCCA security game for both type-I and type-II adversaries.

PROPOSED CONSTRUCTION

In this paper, the role of the party is taken by the attributes. Thus, the access structure A will contain the authorized sets of attributes. Specifically, our construction supports for access structure described dg where U is the attribute universe, ! and !_ areattribute sets and d is a predefined threshold value. For simplicity, we will take user’s attribute set to input to key generation instead of his access structure which is different from our definition in Section We note that such substitution is trivial since user is easy to compute his access structure with the individual attribute set. Furthermore, we deliver the decision for access control redefines such predicate as follows:

Intuition for Proposed Construction

The challenge for constructing outsourced ABE scheme is the realization of delegated key generation and decryption. proposed construction, where ^ is an AND gate connecting two sub-policies PolicyKGSP an PolicyAA. PolicyKGSP is for the request attribute set which will be performed at KGSP while PolicyAA is a trivial policy controlled by AA. The reason that we say it is trivial is that a single default attribute _ is appended with each request attribute set, which has no effect on the global access control policy. Using this trick, we are allowed to randomly generate an outsourcing key (which is OKKGSP in our construction) to delegate partial key generation operation to KGSP without master or private key leakage.

To outsource decryption, we make use of the idea in by choosing a random ‘‘blinding factor’’ (which is t in our construction) to produce blinded transformation key which is able to be sent to DSP to perform decryption partially instead of private key itself. This skill allows us to delegate partial decryption operation to DSP without private key or original message leakage.

CONSTRUCTION

Before providing our construction, we define the Lagrange.Our scheme is based on ABE in [1] which shares the same access formula. The message space for our construction is GT . Actually, using the hybrid encryption technique, we can easily extend it to support for message space consisting of The construction in detail is shown as follows.

Setupð_Þ: First, define the attributes in universe U as elements in Zq. For simplicity, let n ¼ jUj and we can

SECURITY ANALYSIS

Theorem 1. The outsourced ABE scheme is indistinguishable secure against chosen-plaintext

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

attack in selective model under DBDH assumption. Proof Intuition for Proposed Construction For simplicity, we only consider and provide the second construction with two KGSPs. The key challenge for our second construction exists in two folds.One is how to prevent from the collusion between the user and the malicious KGSP. Our solution is to intelligently extend the hybrid policy trick in the first construction. Specifically, in addition to building an AND gate between PAA and PKGSP, we introduce a (2, 2)-secret sharing on PKGSP and make each KGSP only know its own share OKKGSP½i_ for i ¼ 1, 2. In this sense, even if user collude with a KGSP and obtain fOKKGSP½i_g for i ¼ 1 or 2, he cannot recover the secret (which is actually x1 in our construction) to serve the devil.

PERFORMANCE ANALYSIS

In this Section, we provide the performance analysis from both theoretical calculation and empirical evaluation of our main construction in Section 4.3 Efficiency Analysis We compare our scheme with the original ABE [1] and the state-of-the-art [3], [4] in Table 2. We use EXP to denote a nmulti-based exponentiation operation in G and P the pairing operation. We assume one multi-based exponentiation multiplies up to 2 single-based exponentiations and takes roughly the same time as single-based exponentiations.

CONCLUSION

We provide a new outsourced ABE scheme simultaneously supporting outsourced key-issuing and decryption. With the aid of KGSP and DSP, our scheme achieves constant efficiency at both authority and user sides. In addition, we provide a trust-reduced construction with two KGSPs which is secure under recently formulized RDoC model. Unlike the state-of-the-art outsourced ABE, checkability is supported by this construction. The security of proposed schemes have been analyzed and given in this paper. Experimental results demonstrate that our constructions are efficient and practical.

FUTURE ENHANCEMENT:

In future we can implement mobile number service (i.e providing one time password to mobile numbers as well as users).

REFERENCES:

[1] 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.

[2] D. Zeng, S. Guo, and J. Hu, ‘‘Reliable Bulk-Data Dissemination in Delay Tolerant Networks,’’ IEEE Trans. Parallel Distrib. Syst. http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.221

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

[4] Z. Zhou and D. Huang, ‘‘Efficient and Secure Data Storage Operations for Mobile Cloud Computing,’’ in Cryptology ePrint Archive, Report 2011/185, 2011.

[5] P. Golle and I. Mironov, ‘‘Uncheatable Distributed Computations,’’ in Proc. Conf. Topics Cryptol., CT-RSA, 2001, pp. 425-440.

[6] 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.

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

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

[9] T. Nishide, K. Yoneyama, andK. Ohta, ‘‘Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures,’’ in Proc. Appl. Cryptogr.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Netw. Security, LNCS 5037, S. Bellovin, R. Gennaro, A. Keromytis, and M. Yung, Eds., Berlin, Germany, 2008, pp. 111-129, Springer-Verlag.

[10] F. Han, J. Qin, H. Zhao, and J. Hu, ''A General Transformation from KP-ABE to Searchable Encryption,'' Future Gen. Comput. Syst., vol. 30, pp. 107-115, Jan. 2014.

[11] H. Zhao, J. Qin, and J. Hu, ''Energy Efficient Key Management Scheme for Body Sensor Networks,'' IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2202-2210, Nov. 2013.

[12] S.Yu,C. Wang,K.Ren, andW. Lou, ''Achieving Secure, Scalable, Fine-Grained Data Access Control in Cloud Computing,'' in Proc. IEEE 29th INFOCOM, 2010, pp. 534-542

[13] M.J. Atallah, K. Pantazopoulos, J.R. Rice, and E.E. Spafford, ''Secure Outsourcing of Scientific Computations,'' in Trends in Software Engineering, vol. 54, M.V. Zelkowitz, Ed. Amsterdam, The Netherlands: Elsevier, 2002, pp. 215-272.

[14] 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.

[15] D. Benjamin and M.J. Atallah, ''Private and Cheating-Free Outsourcing of Algebraic Computations,'' in Proc. 6th Annu. Conf. PST, 2008, pp. 240-245.

[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] K. Bicakci and N. Baykal, ''Server Assisted Signatures Revisited,'' in Proc. Topics Cryptol.-CT-RSA, LNCS 2964, T. Okamoto, Ed., Berlin, Germany, 2004, pp. 1991-1992. Springer-Verlag.

[19] M. Jakobsson and S. Wetzel, ''Secure Server-Aided Signature Generation,'' in Proc. Public Key Cryptogr., 2001, pp. 383-401.

[20] S. Hohenberger and A. Lysyanskaya, LNCS 3378, J. Kilian, Ed., Berlin, Germany, pp. 264-282, Springer-Verlag.

Author Details

T.Yamini pursuing M.Tech in Vignan's Nirula Institute of Tecnology For Women, Pedapalakaluru, Guntur and completed B.Tech in Malineni Lakshmaiah Women's Engineering College, Guntur.

Dr.B.Bhanu Prakash received his Ph.D from Acharya Nagarjuna University in the domain of Data Mining. He is having 10 years of experience in this field.