Attribute Based Data Encryption and Outsourced Decryption with Verifiability

Publication History
Received: 23 January 2015
Accepted: 3 March 2015
Published: 18 April 2015

Citation
Saravanan K, Manikannan K. Attribute Based Data Encryption and Outsourced Decryption with Verifiability. Discovery, 2015, 30(133), 327-332
Attribute Based Data Encryption and Outsourced Decryption with Verifiability

K. Saravanan¹, Mr. K. Manikannan²
II ME CSE¹, Assistant Professor²
Adhiparasakthi Engineering College
Melmuruvathur – 603319.
skarwan234@gmail.com¹, kmanikannan@adhiparasakthi.in²

Abstract - Attribute-based encoding (ABE) is a public-key supported one-to-many encoding that permits users to code and decode knowledge primarily based on user attributes. A promising application of ABE is versatile access management of encrypted knowledge held on within the cloud, exploitation access policies and ascribed attributes related to personal keys and cipher texts. As more sensitive data is shared and stored by third-party sites on the Internet, encryption is needed for data stored at these sites. Main drawback of existing encrypt technique, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). This system develop a new concept for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption. We presented the cipher text-policy attribute-based encryption systems that are efficient, expressive, and provably secure under concrete assumptions. Also this system prove the security of our system from three static assumptions. By using an Encryption/Decryption standard our distributed secure computation system show that our approach seamlessly integrates security enforcement at the user intensity with a certain trust level. Hence a system is proposed so as to define as strategy to check the unique attribute based encryption using proxies and outsourced decryption. we have a tendency to show an implementation of our theme and results of performance measurements, that indicates a major reduction on computing resources obligatory on users. Within the projected system the analysis and accuracy of the attributes area unit copied so as to produce higher encryption/decryption strategy whereas transferring knowledge from supply to destination.

Key words: Attribute-based encoding, Key-Policy ABE, Encryption, Decryption.

I INTRODUCTION

There is a trend for sensitive user data to be stored by third parties on the Internet. For example, personal email, data, and personal preferences are stored on web portal sites such as Google and Yahoo. The attack correlation center, dshield.org, presents aggregated views of attacks on the Internet, but stores intrusion reports individually submitted by users. Given the variety, amount, and importance of information stored at these sites, there is cause for concern that personal data will be compromised. This worry is escalated by the surge in recent attacks and legal pressure faced by such services. One method for alleviating some of these problems is to store data in encrypted form. Thus, if the storage is compromised the amount of information loss will be limited. One disadvantage of encrypting data is that it severely limits the ability of users to selectively share their encrypted data at a fine-grained level. Suppose a particular user wants to grant decryption access to a party to all of its Internet traffic logs for all entries on a particular range of dates that had a source IP address from a particular subnet. To solving this lack of security problem by introducing the concept of Attributed-Based Encryption (ABE). In an ABE system, a user's keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key.

II OVERVIEW

The system the analysis and accuracy of the attributes square measure derived so as to produce higher encryption/decryption strategy whereas transferring information from supply to destination. The generation of the general public and personal key victimization the attributes and key with proxies and access structure attributes square measure same because the existing system. The combination of the general public and personal key generates the message. The verification of the outsourced decipherment also are created victimization the mix of personal key and parameter attribute that generates the rework and retrieve key equally because the existing system. Additionally the construct of proxy verification square measure created since the proxies’ square measure intermediate between the supply and also the destination. The validation square measure created victimization the non-public key talk to the proxies and also the supply. The attribute used square measure checked for its individuality thus on avoid constant attribute for the common constant quantity information. The coding of knowledge square measure valid victimization the general public. Therefore this technique overcomes the disadvantage of the prevailing system.

Objective

The main aim of this paper is to outline a scientific paradigm for confirming attribute and master secret key based mostly
encoding and cryptography. Issues associated with sharing data during a distributed system is one of one among one during all one amongst one in every of the foremost sensible issue consisting of autonomous entities that has to be firmly transferred in a heterogeneous multi divided systems. Hence the ideas of encoding and cryptography square measure developed to transfer the information from supply to destination firmly. By mistreatment associate encryption/Decryption customary our distributed secure computation system shows that our approach seamlessly integrates security social control at the user intensity with an exact trust level.

III DATA PROCESSING OF THE SYSTEM

The evaluation and accuracy of the attributes are traced in order to provide better encryption/decryption strategy while transferring data from source to destination. Figure 1 shows generation of the public and private key using the attributes and master key with proxies and access structure attributes are same as the existing system. The combination of the public and private key generates the message. The verification of the outsourced decryption are also made using the combination of private key and parameter attribute that generates the transform and retrieve key similarly as the existing system. Additionally the concepts of proxy verification are made since the proxies are intermediate between the source and the destination.

The generation of the public and private key using the attributes and master key with proxies and access structure attributes are same as the existing system. The combination of the public and private key generates the message. The verification of the outsourced decryption are also made using the combination of private key and parameter attribute that generates the transform and retrieve key.

Figure 1 System Architecture Diagram

V ATTRIBUTE BASED ENCRYPTION

We are particularly interested in attribute-based encryption as a special case of functional encryption because it provides a functionality that can be very useful in practice. For example, a police force could use an ABE system to encrypt documents under policies like “Internal Affairs OR (Undercover AND Central)" and give out secret keys to undercover officers in the central division corresponding to the attributes “Undercover” and “Central”. Given the many potential uses of ABE systems, constructing efficient systems with strong security guarantees is an important problem.

Previous Constructions and Selective Security.

All previous constructions of ABE systems have only been proven to be selectively secure. This is a limited model of security where the attacker is required to announce the target he intends to attack before seeing the public parameters of the system. This is an unnatural and undesirable restriction on the attacker, but it unfortunately appears to be necessary for the proof techniques used in prior works. To see why this is the case, it is instructive to look into the way that previous security proofs have worked. In these security proofs, the simulator uses the attacker's announced target to embed the challenge in the public parameters in such a way that the simulator can produce any keys the attacker can request but can also leverage the attacker's output to break the underlying challenge. This is a partitioning strategy reminiscent of the strategies first used to prove security for IBE systems. The formation of the public parameters partitions the keys into two classes: those that the simulator can make, and those that are useful to the simulator in solving its challenge.

While this partitioning strategy was successfully employed by Boneh and Boyen [4], and Waters [10] to prove
full security for an IBE system, any partitioning approach seems doomed to failure when one tries to achieve full security for ABE systems. Without selectivity, the simulator cannot anticipate which keys the attacker may ask for, so the attacker must make some type of a guess about what the partition should be. One natural direction is to partition the identity space in some random way and hope that the attacker’s queries respect the partition (which was the main idea behind the works in the IBE setting). For ABE systems, however, private keys and cipher texts have much more structure; different keys can be related (they may share attributes), and this severely restricts allowable partitions. Thus, the power and expressiveness of ABE systems work directly against us when attempting to create partitioning proofs.

V CIPHERTEXT ATTRIBUTE BASED ENCRYPTION

The lack of satisfaction with generic group model proofs has motivated the problem of finding an expressive CP-ABE system under a more solid model. There have been multiple approaches in this direction. First, we can view the Sahai-Waters[1] construction most “naturally” as Key-Policy ABE for a threshold gate. In their work, Sahai and Waters describe how to realize Ciphertext-Policy ABE for threshold gates by “grafting” so called “dummy attributes” over their basic system. Essentially, they transformed a KP-ABE system into a CP-ABE one with the expressiveness of a single threshold gate. Cheung and Newport[2] provide a direct construction for constructing a policy with a single AND gate under the Bilinear Di_e-Hellman assumption. Their approach has the drawbacks that it only allows a fixed number of system attributes and is limited to an AND gate (does not enable thresholds). In retrospect these two limitations actually make it less expressive than the SW transformation, although this wasn’t necessarily immediately apparent.

Most recently, Goyal, Jain, Pandey, and Sahai[3] generalized the transformational approach to show how to transform a KP-ABE system into a CP-ABE one using what they call a “universal access tree”. In particular, they provided a mapping onto a “universal” (or complete) access tree of up to depth d formulas consisting of threshold gates of input size m, where m and d are chosen by the setup algorithm. They applied a similar "dummy attribute" approach. In order to accommodate a general access formula of size n, their scheme first translates this into a balanced formula. Under standard techniques a formula of size n can be “balanced” such that any formula (tree) of size n can be covered by a complete tree of size approximately $O(n^{42})$. Their work was the first feasibility result for expressive CP-ABE under a non-interactive assumption. Unfortunately, the parameters of ciphertext and private key sizes add encryption and decryption complexity blow up (in the worst case) by an $n^{42}$ factor limiting its usefulness in practice. For instance, in a system with U attributes defined and n nodes the ciphertext overhead will be approximately a factor of $U \cdot n^{42}$ greater than that of the BSW system. To give a concrete example, for the modest parameters of universe size U = 100 attributes and a formula of 20 nodes the blowup factor relative to BSW is approximately 140,000.

VI ABE WITH FAST DECRYPTION EFFICIENCY AND TRADEOFFS

The main feature of the above scheme is that decryption only requires two pairings. While decryption also requires two exponentiations per row used, if the LSSS is derived from an AND/OR tree then the exponents wi will be 1. (That is, they will be either 0 or 1, but the wi = 0 rows should not be used.) Thus, decryption can be very fast.

There are two tradeoffs:
1. The private key size and generation time blows up by roughly a factor of |Γ| compared to GPSW, where Γ is the set of distinct attributes used in making the key.
2. Decryption reduces the number of pairings, but requires modular multiplications of roughly a factor of |Γ| compared to GPSW, where Γ is the set of distinct attributes used in decryption.

Thus, while there is a blow-up, this increase is tied only to the number of distinct attributes “touched” by the corresponding operation, and not by a global bound. Depending on the application, one should take into consideration whether the blow up in key size is worth it. Moreover, the decryption time could actually increase over GPSW [16] once becomes sufficiently large. However, it would have to be so large that 2 pairings plus |Γ| pairings and |Γ| multiplications dominates |Γ| pairings and |Γ| multiplications. As one benchmark, it required 8.22ms to compute a pairing for a BN256 curve with the RELIC library on a modern PC while roughly 0.0034ms to compute a modular multiplication. Thus, in a setting where |Γ| = |Γ| (the number of rows of the access matrix touched during decryption is the same as the number of distinct attributes touched), the decryption algorithm would need to touch over 2416 distinct attributes before GPSW would be faster. Should this occur, however, it is worth noting that the above private keys actually contain a GPSW key; thus, if this threshold was ever reached, one could revert back to doing GPSW decryption.

VII SECURITY PROPERTIES OF PROXY SIGNATURE

Desirable security properties of proxy signatures have been evolved from the introduction of proxy signature. A widely accepted list of required security properties is given below:
• **Strong unforgeability**: A designated proxy signer can create a valid proxy signature on behalf of the original signer. But the original signer and other third parties cannot create a valid proxy signature.

• **Strong identifiability**: Anyone can determine the identity of corresponding proxy signer from the proxy signature.

• **Strong undeniability**: Once a proxy signer creates a valid proxy signature on behalf of the original signer, he cannot deny the signature creation.

• **Verifiability**: The verifier can be convinced of the signers’ agreement from the proxy signature.

• **Distinguishability**: Proxy signatures are distinguishable from the normal signatures by everyone.

• **Secrecy**: The original signer’s private key cannot be derived from any information, such as the shares of the proxy key, proxy signatures, etc.

• **Prevention of misuse**: The proxy signer cannot use the proxy key for other purposes than it is made for. That is, he cannot sign message with the proxy key that have not been defined in the warrant. If he does so, he will be identified explicitly from the warrant.

### A. Classification of Proxy Signature

According to the nature of delegation capability, proxy signature can be classified as proxy-unprotected, proxy-protected and threshold notions. This differentiation is important in practical applications, since it enables proxy signature schemes to avoid potential disputes between the original signer and the proxy signer.

1. **Proxy-Unprotected Notion**

   The scenario exists when an original signer gives her signing rights (full delegation with warrant) to a proxy signer. The original signer sends a signed warrant to the proxy signer, who then uses this information to generate proxy signatures by executing a standard signature scheme.

   When a proxy signature is sent, the recipient checks its validity according to the corresponding standard signature verification process. As the proxy signer does not append his private key on top of the received delegation, a dishonest original signer can sign the message and later claim that the signature was created by the proxy signer. This type of proxy signature primarily lacks strong unforgetability property.

2. **Threshold Notion**

   In a threshold proxy signature, the proxy key is shared by a group of n proxy signers. In order to produce a valid proxy signature on a given message m, individual proxy signer produces his partial signature on that message, and then combines them into a full proxy signature on message m.

   In a (t, n) threshold proxy signature scheme, the original signer delegates her signing capability to a proxy group of n members. Any t or more proxy signers of the group can cooperatively issue a proxy signature on behalf of the original signer, but (t – 1) or less proxy signers cannot forge a signature.

### VII CONCLUSION

In this paper, we proposed the concept of future enhancement over the Distributed Attribute-Based Encryption (DABE) as an extension of Cipher text-Policy Attribute-Based Encryption (CP-ABE) that supports an arbitrary number of attribute authorities and allows to dynamically add new users and authorities at any time, which will provide an efficient construction of DABE that uses only two pairing operations in the decryption algorithm and no pairing operation in any other algorithm. A limitation of the construction is that access policies need to be in DNF form. We leave it as an open question to design a more expressive DABE scheme, while preferably maintaining the O(1) number of pairings that our construction offers. In this work we proposed CP-ASBE a form of CP-ABE that organizes user attributes into a recursive family of sets and allows users to impose dynamic constraints on how attributes may be combined. We demonstrated how CP-ASBE can naturally support compound attributes, and numerical attributes with multiple value assignments. We showed that it achieves this versatility with very little overhead through efficiency analysis and performance evaluation of a prototype implementation. An interesting direction for future research is to study the potential of CP-ASBE schemes and ABE schemes in general in supporting constructs similar to “OR roles” and constraints like “dynamic mutually exclusive roles” that are common in traditional mediated RBAC settings. Other directions for future work are the design of efficient CP-ASBE schemes that are secure in the standard model and extending CP-ASBE to a multi-authority setting.

### REFERENCES