International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Improving Security of Traceable White-Box CPABE with TTP Access Control

Dilu Anil

Computer Science and Engineering, ICET, Mahatma Gandhi University, Muvattupuzha, Kerala, India

Abstract: ***Various encryption schemes have gained popularity for secure transmission of data. CPABE (Ciphertext Policy Attribute Based Encryption) is one among such schemes. The decryption rights are generated based on the attributes of user. Traceability is the property by which the malicious users who intentionally try to leak the data are traced. However it is difficult to find the actual user who leaked the key since there can be many people who share the same decryption rights. In this paper a trusted third party is introduced, which will act as the public auditor. If any malicious user claims to be innocent, then the third party checks and traces all the information transferred by that user.***

Keywords: Attribute Based Encryption, Traceability, public auditor, malicious user.

1. Introduction

Attribute-based encryption (ABE) is a new encryption technique that is used for public-key cryptography. In public-key cryptography, messages that are intended for a specific receiver are being encrypted with the receiver's public-key. Identity-based encryption (IBE) is implemented by allowing the public-key of the user to be an arbitrary string, such as the email address of the receiver. ABE goes one step further and defines a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE). In ciphertext-policy attribute-based encryption (CP-ABE) the private key of the user is accompanied with a set of attributes. The ciphertext is based on an access policy defined by a universe of attributes within the system. A user will be able to decrypt a ciphertext [1], if and only if his attributes satisfy the policy of the respective ciphertext. Policies may be defined over attributes using conjunctions, disjunctions. It is necessary that atleast (k,n)-threshold gates, i.e., k out of n attributes have to be present (there may also be non-monotone access policies with additional negations and meanwhile there are also constructions for policies defined as arbitrary circuits). This methodology which is referred as Shamir's threshold scheme is also used in the implementation.

The main idea in ABE is that the role of the users is taken by the attributes. Thus, the access structure A will contain the authorized sets of attributes. For CP-ABE, if a user of the system posses an authorized set of attributes then he can decrypt the ciphertext, otherwise, he can't get any information from ciphertext if the set he possessed is unauthorized. In our construction, we restrict our attention to monotone access structure.

Users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, [2] but only specifying the policy which allows decrypting. One major issue is that if an authorized user sells his key to a malicious person, then the functionality of the system is lost. This issue can be tackled by traceability. The new systems can trace the malicious users or traitors who may leak the partial or modified decryption keys to others for profits. Traceability is the technique by which the malicious users are identified by analyzing, tracing and tracking all the information sent and received by the malicious user.

In this paper, a trusted third party is introduced for the post of public auditing. When a user found as malicious claims that he is innocent and it is the problem of the system then it is difficult to confirm whether it is right or wrong. To solve this problem, the trusted third party comes into action. By analyzing the log of this particular user TTP retrieves the decryption keys. With the help of this the confirmation can be made. Key sanity check functionality is added to check whether the sender is authorized or not. Even in the case of attacker the same check is done. The credentials of the user are stored during the registration. Based on these attributes key generation is done [4]. The keys are generated at the time of encryption, both the encryption and decryption. ABE scheme proposed in this paper can still be able to find the malicious users whose keys have been used for building the decryption device, and our scheme can achieve selective traceability in the standard model under this scenario.

2. Related Work

2.1 CPABE

Ciphertext Policy Attribute Based Encryption is an encryption method which uses policies of user to generate encryption and decryption keys. In most of the situations, when a user encrypts sensitive data, it is necessary that user should establish a specific access control policy on who can decrypt this data. For example, [6] suppose that the FBI public corruption offices in Knoxville and San Francisco are investigating an allegation of bribery involving a San

Francisco lobbyist and a Tennessee congressman. The head FBI agent may want to encrypt a sensitive memo so that only personnel that have certain credentials or attributes can access it. For instance, the head agent may specify the following access structure for accessing this information: ((“Public Corruption Office” AND (“Knoxville” OR “San Francisco”)) OR (management-level > 5) OR “Name: Charlie Eppes”). By this, the head agent could mean that the

memo should only be seen by agents who work at the public corruption offices at Knoxville or San Francisco As illustrated by this example, it can be crucial that the person in possession of the secret data be able to choose an access policy based on specific knowledge of the underlying data. Furthermore, this person may not know the exact identities of all other people who should be able to access the data, but rather she may only have a way to describe them in terms of descriptive attributes or credentials. The server is entrusted as a reference monitor that checks that a user presents proper certification before allowing him to access records or files. Traditionally, this type of expressive access control is enforced by employing a trusted server to store data locally. However, services are increasingly storing data in a distributed fashion across many servers. Replicating data across several locations has advantages in both performance and reliability. Most existing public key encryption methods allow a party to encrypt data to a particular user, but are unable to efficiently handle more expressive types of encrypted access control such as the example illustrated above.

2.2 Secret Sharing

A key distribution scheme for dynamic conferences is a method by which initially an trusted server distributes private individual pieces of information to a set of users. Later each member of any group of users of given size can compute a common secure group key. In this setting [7] any group of t users can compute a common key by each user computing using only his private initial piece of information and the identities of the other t − 1 users in the group. Keys are secure against coalition of to k users, that is, even if k users pool together their pieces they cannot compute anything about a key of any t-size conference comprised of other users. Shamir's Threshold secret sharing method is used in this paper.

In recent years the security of operations taking place over a computer network becomes very important. It is necessary to protect such actions against bad users who may try to misuse the system. Many protocols and schemes were designed to solve problem of this type. To overcome the various security vulnerabilities in the networks the design of a pre distribution algorithm using a deterministic approach is initiated. The deterministic approach is the process of determining the keys or key chain based on some criteria. In this paper, we have proposed a novel deterministic key pre distribution algorithm using the pell's equation. **Pell's equation** (also called the Pell–Fermat equation) is any Diophantine equation of the form $x^2-ny^2=1$
where n is a given positive non-square integer and integer solutions are sought for x and y. In Cartesian coordinates, the equation has the form of a hyperbola; solutions occur wherever the curve passes through a point whose x and y coordinates are both integers, such as the trivial solution with x = 1 and y = 0.Joseph Louis Lagrange proved that, as long as n is not a perfect square, Pell's equation has infinitely many distinct integer solutions. These solutions may be used to accurately approximate the square root of n by rational numbers of the form x/y.

2.3 Identity Based Encryption

In an IBE system, the public key of a user may be an arbitrary string like an e-mail address or other identifier. This eliminates certificates altogether; the sender could just encrypt the message with the identity of the recipient without having to first obtain his public key (and make sure that the obtained public key is the right one). Of course, users are not capable of generating a private key for an identity themselves. For this reason, there is a trusted party called the private key generator (PKG) [5] who does the system setup. To obtain a private key for his identity, a user would go to the PKG and prove his identity. The PKG would then generate the appropriate private key and pass it on to the user. Since the PKG is able to compute the private key corresponding to any identity, it has to be completely trusted. The PKG is free to engage in malicious activities without any risk of being confronted in a court of law. The malicious activities could include: decrypting and reading messages meant for any user, or worse still: generating and distributing private keys for any identity. This, in fact, has been cited as a reason for the slow adoption of IBE despite its nice properties in terms of usability. It has been argued that due to the inherent key escrow problem, the use of IBE is restricted to small and closed groups where a central trusted authority is available. One approach to mitigate the key escrow problem is to employ multiple PKGs [8]. This is an attractive solution and successfully avoids placing trust in a single entity by making the system distributed. However, this solution comes at the cost of introducing extra infrastructure and communication. It is burdensome for a user to go to several key authorities, prove his identity to each of them and get a private key component (which has to be done over a secure channel).

3. Methodologies

Consider a commercial application such as a pay-TV system with huge number of users for example. Each user is labeled with lots of related attributes, which are defined as TV channels that the user have ordered. As a versatile one-to-many encryption mechanism, CP-ABE system is quite suitable in this scenario. The pay-TV system provides several TV channels for users, and those who have paid for the TV channels could satisfy the access policy to decrypt the ciphertext and enjoy the ordered TV channels.

CPABE enables fine-grained access control to the encrypted data according to attributes in users' ordered lists. However, there are two problems with this approach. First, if someone (who does not have the privilege to access to those TV chat a lower cost, she/he could also get access to the TV channels. It is necessary to find out who is selling the decryption key. Second, as the TV channels of the pay-TV system expand, an increasing number of new attributes need to be added to the system to describe the new channels. If the number of the attributes exceeds the bound set during the initial deployment of the pay-TV system, then the entire system has to be re-deployed and possibly all its data will have to be re-encrypted [5], which would be a disaster to the pay-TV in the commercial applications. The problems, as described above, are the main obstacles when CP-ABE is implemented in commercial applications such as pay-TV systems and social

networks. Due to the nature of CP-ABE, if a malicious user leaks its decryption key to others for profits (such as selling the decryption key on the Internet), it is difficult to find out the original key owner from an exposed key since the decryption key is shared by multiple users who have the same attributes.

3.1 Traceable CPABE

In a Traceable CP-ABE system (T-CPABE system) it is not required that the attributes for the encryption process be fixed at the setup phase. The identities of the user are added whenever they register into the system. There are six steps in traceable CPABE.

- **Setup (pp, msk) :** The algorithm takes as inputs a security parameter encoded in unary. It outputs the public parameters pp and the master secret key msk. All these values are entered into the table. In addition, it initializes an identity table (T).
- **KeyGen (pp, msk, id, S) → $sk_{id,S}$:** In key generation phase the public parameters pp, the master secret key msk, set of attributes S and the identifier id are taken as inputs by the algorithm. The output of this algorithm is a secret key $sk_{id,S}$ corresponding to S. Then, the value of id is entered into the identity table T.
- **Encrypt (pp, m, A) → *ct* :** This is the phase where encryption takes place. The public parameters pp, message m and the Access structure corresponding to these attributes are taken as inputs so as to generate the Ciphertext (*ct*).
- **Decrypt (pp, $sk_{id,S}$, ct) :** The output message m is generated by taking public parameters pp, secret key and the Ciphertext. If the parameters or key doesn't match then ϕ is generated indicating a mismatch.
- **Key Sanity Check (pp, sk) →1 or 0 :** This is the important phase in which actual checking of the key is done. The algorithm takes as input public parameters pp and the secret key sk. It then checks the attributes and identifier to see if it was a well-formed during the decryption process. If sk passes the test, it outputs 1 otherwise 0.
- **Trace (pp, sk, T) → id or :** This algorithm is used to identify the malicious user. From the above algorithm we can conclude whether the key was well-formed or not. If it was well-formed then using the trace algorithm the identity of the malicious user is found out. Thus it outputs the id of the user. Else ∞ is generated indicating that the user need not be traced.

Apart from the above steps an additional functionality is introduced in the form of a Trusted Third Party (TTP). This admin continuously monitors the system. Whenever the system identifies a malicious user his identity is entered into the table. Even if the user claims to be innocent the admin checks all the transactions carried out by this particular user. By doing so the TTP can know if there was a malicious attempt or not. Such users can be revoked by the TTP.

3.2 Shamirs Threshold Scheme

It is well known for Shamirs (t, n) threshold scheme [3] (or Shamirs secret sharing scheme) in cryptography. The essential idea of that scheme is that t points on a t - 1 degree curve are sufficient to confirm such a curve, that is, t points are enough to determine a t - 1 degree polynomial. For a (t; n) threshold scheme, a secret can be divided into n parts (or even more), which are sent to each participant a unique part. All of them can be used to reconstruct the secret. Suppose that the secret is assumed to be an element in a finite field F_p . Choose t - 1 number of random coefficients $a_1, a_2, \ldots, a_{t-2}$ element of F_p and a_{t-1} element of F_p and set the secret in the constant term a_0. Every participant is given a point (x, y) on the above curve, that is, the input to the polynomial x and its output y = f(x). Given a subset with any t points, recover the constant term a_0 using the Lagrange interpolation. White box traceability is implemented in this paper as a web application.

A military system using the CPABE encryption was constructed. The Trusted Third Party is implemented as Admin. Attributes of each user are : Post name, Priority and the unique id generated at the time of registration. The user with higher priority will accept/reject the user just below him. Admin can accept/reject the user with highest priority. Each user has privileges to share data with persons in their own privilege level or higher levels but not to persons in their lower levels. The inbox of each user consists of different sections of messages that are received from others in the system. There are a special category of files called the red files which are of highest priority. The users who try to access these files which are not actually intended for him, then he is identified as a malicious user. His identity is entered into the table and given for traceability check.

4. Conclusion

CPABE systems which include white box traceability of the authorized malicious users have been developed. In this paper the credibility of the users in the trace list is verified. Suppose a user Bob is identified as a malicious user by the system, but claims to be innocent and framed by the system. It is a big problem to judge whether Bob is in fact innocent or not.

In this case, the suspected user does not trust the system. Thus the system needs to provide some evidence persuasive enough to prove that the suspected user is guilty. A trusted third party system is introduced which analyses the decryption keys of the detected users. The TTP also checks and tracks all the data sent as well as received b this user. A blocked from the system. If the user is legitimate but system tried to frame him/her then this can be clarified with the help of this third party.trace list is generated and the detected malicious users can even be

5. Acknowledgement

The author would like to thank Liyamol Aliyar, HOD, Department of Information Technology, Ilahia College of Engineering and Technology, Muvattupuzha for her guidance, technical and moral support

References

[1] Susan Hohenberger and Brent Waters. Attribute-based encryption with fast decryption. In Public-Key CryptographyPKC 2013, pages 162 179. Springer, 2013.
[2] Allison Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In Advances in Cryptology EUROCRYPT 2012, pages 318335. Springer, 2012.
[3] Nuttapong Attrapadung, Benot Libert, and Elie De Pana_eu. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In Public Key CryptographyPKC 2011, pages 90108. Springer, 2011.
[4] Vipul Goyal, Abhishek Jain, Omkant Pandey, and Amit Sahai. Bounded Ciphertext policy attribute based encryption. In Automata, Languages and Programming, pages 579591. Springer, 2008.
[5] Melissa Chase. Multi-authority attribute based encryption. In Theory of Cryptography, pages 515534. Springer, 2007.
[6] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In Security and Privacy, 2007. SP'07. IEEE Symposium on, pages 321–334. IEEE, 2007.
[7] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In Security and Privacy, 2007. SP'07. IEEE Symposium on, pages 321–334. IEEE, 2007.
[8] Vipul Goyal. Reducing trust in the pkg in identity based cryptosystems. In Advances in Cryptology-CRYPTO 2007, pages 430–447. Springer, 2007.
[9] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

Author Profile

Dilu Anil received the Bachelor of Technology degree in Information Technology from Mahatma Gandhi University, Kerala. She is currently doing Master of Technology degree in Computer Science and Engineering with Specialization in Information Systems from Mahatma Gandhi University, Kerala.