Survey of Attribute Based Encryption Schemes

Walunj Pratap[#1], Assistant Prof. Bhagwan Kurhe[*2]

[#]*PG Student, Department Of Computer Engineering & Savitribai Phule University of Pune*

[#]*Assistent Prof., Department Of Computer Engineering & Savitribai Phule University of Pune*
Pune, Maharastra, India

Abstract *— Since inception of internet security and privacy of are the critical issues faced by researchers. There have been many cryptographic solutions available to solve some of these issues, but as fine grained access control was needed existing cryptographic solutions become unsuitable for supporting such concept, thus researchers came with an idea of ABE and IBE. ABE is new field in PKC and in digital signatures. It uses access policies to control access over encrypted data. This paper covers study of various attribute based encryption schemes proposed by various researchers.*

Keywords *— Public Key Cryptography, Attribute Based Encryption and Pairing Based Cryptography.*

I. INTRODUCTION

Since the development of computer the security of data came into existence and whole new branch is devoted for research into cryptography. Securing a data is critical for any business ranging from small firm or large organizations [04][12]. Cryptography uses strong mathematics to convert data into some non-sense form called as 'ciphertext' and anyone having valid key can decrypt the 'ciphertext' [12]. There are two types of encryption algorithm symmetric and asymmetric. The encryption/decryption key in symmetric algorithm is same, while in asymmetric algorithm one key is used for encryption while other is used for decryption. The popular Diffie-Hellman [11] key exchange protocol is used for key exchange between parties involved in communication. The cryptographic algorithm is believed to be secure iff even after knowledge of algorithm used and public parameters used for encryption, it is still difficult or even impossible to recover original data without valid decryption key [07].

Sometimes it is desirable to share the data to more than one party and put a restriction on who has access to which portion of the data. This real world requirement is achieved using Attribute Based Encryption (ABE) and Role Based Access Control (RBAC). ABE effectively binds the access-policies to the data, thus only intended users can decrypt the data [08]. One can view access policy as analogous to user designation in organization. ABE can address complex access control policies required for real world applications and prior knowledge of total number of users is also not required only Knowledge of the access policy is sufficient. An important requirement that ABE schemes must guarantee is the collusion resistance.

There are two types of ABE schemes, Ciphertext Policy Attribute Based Encryption (CP-ABE) and Key Policy Attribute Based Encryption (KP-ABE) [01]. This categorization is done on the basis of whether attributes are embedded in the ciphertext (KP-ABE) or whether the access-structure is embedded in the ciphertext (KP-ABE). KP-ABE encrypts attributes along with the data and finally each user is given access structure as a part of their secret key. Whereas, CP-ABE embedded access-structure into the ciphertext and users can have their attributes saved in their secret keys. CP-ABE was introduced by Bethencourt et al [17]. Variant of ABE is Attribute Based Signature used for signing digital documents used for authentication purpose.

II. LITERATURE SURVEY

Shamir's secret sharing is a form of secret sharing where a secret (S) is divided into n parts and each part is given to one of the participants. The idea is that, only if all (or t, as in the case of threshold) participants combine their shares meaningfully will they be able to reconstruct the original secret. It is important to note here that, if fewer than n (or t, as in the case of threshold) participants co-operate they must not be able to retrieve the secret. Let us look at the case where we want to use (t; n) threshold to share the secret S. Without loss of generality we can assume S to be an element in a finite field F. We know that it takes t points to define a polynomial of degree t-1. We note here that, with fewer than t shares it is highly improbable to reconstruct the original polynomial exactly [07]. Hence, by combining the shares of less than t parties, no one gets any clue on the secret S. But when t or more parties of the n combine, then we are able to get S precisely.

Initial ciphertext-policy ABE scheme was developed by Bethencourt et al. [17]. It makes access structure public and users are kept anonymous to decryptors. The idea of tree-access structure and secret sharing was taken from [03]. Some schemes also supports threshold gates at every node of the tree thus allowing user to access data with less than or equal to access permission. Like

other schemes ABE schemes also rely on assumption that the problem does not reduce known hardness assumptions. Waters proposed efficient and secure CP-ABE scheme. The running time and size of key, ciphertext was low. Water used LSSS for access control and it was proved secure in the standard model. In the same paper, the author provides two additional constructions, which make a small compromise with respect to performance but are proved secure in the decisional bilinear Diffie-Hellman exponent assumption and the DBDH assumption. To see the improvement that their scheme offered empirically, let us denote the number of attributes in the universe as n_U, attributes possessed by the recipient user as n_r and access structure as n_s. Then, Waters' scheme gives $n_U + n_r$ secret key components and $n_U * n_S$ ciphertext components. The number of components are reduced to at least half [10].

Cheung et al proposed scheme considered only access structures with AND gates and added support for negated attributes. The construction was for access structures with AND gates on positive and negative attributes. Also, they used Cannetti-Halevi-Katz technique for protection against chosen ciphertext (CCA) secure scheme. This research given direction for threshold ABE and construction of hierarchical attributes [06].

Elgamal [02] PKE was proposed in 1984 which is still used today. The security of Elgamal is dependent on "Decisional Diffie-Hellman". The algorithms of Elgamal are defined below:

KeyGen (p) : Consider G is a multiplicative cyclic group of order p, public key is h, g, G. The private key is the exponent x E Z_p such that $h = g^x$.

Encrypt (M, s_k) : To encrypt M choose a random element x E Z_p and output the pair C = $<C_1,C_2>$ where $C_1 = g^x$ and C_2 = M.h.x.

Decrypt (C, p_k) : For decrypting compute M = C_2/C_x

RSA [12] is very early stage encryption algorithm which is based on factorization. Factorization is believed to be hard problem. It works on following sequence,

setup (k): choose two large random prime numbers p and q and k is security parameter.

Calculate n = p*q.

$\phi(n) = (p - 1)(q - 1)$.

Choose e such that 1 < e < phi(n) and e and Q(n) are coprime.

Compute d such that $e.d = 1 (\text{mod } \phi(n))$.

The public key is p_k = (n, e) and the private key is s_k = (d, p, q).

Encrypt (M, s_k): calculate $c = M^d (\text{mod } n)$.

Decrypt (sigma, p_k,M): Verifier calculates $c^e (\text{mod } n)$.

Identity based cryptography is a special form of public key cryptography. Here, the public key has been replaced with the identity of either the signer or the decryptor. There are three entities; a signer, a verifier and a key generator. The signer obtains a private key that corresponds to his identity from a key generator. He signs a message with that key. The verifier uses the identity of the signer to check validity of the signature.

There are three entities; an encryptor, decryptor, and a key generator. The decryptor sends his identity to the key generator and obtains a private key that corresponds to it. The encryptor will use that identity to encrypt the message. The ciphertext is decrypted with the private key. The general idea is to create an encryption scheme such that the receiver of a ciphertext can only decrypt if he satisfies a particular policy chosen by the sender at the time of encryption.

An attribute tree is the structure used to present the verifier's request. Attribute tree is the structure used to implement ABE scheme, it also uses bilinear maps and Lagrange interpolation to build a policy for decryption. Each inside node acts like threshold gate and leaves acts as attributes.

Baden et al. Proposed Social Network in which user is able to hide their personal information. The security to user data is provided with ABE. Wang et al. [16] evaluated the performance of CP-ABE and KP-ABE on laptop and smartphone devices and concluded ABE performance is unacceptable on smartphones and its non-feasibility on such devices would be a big obstacle to deployment of new services and to benefit from its advantages. Yang et al. [08] proposed an improved scheme in CP-ABE which extended multi-authority with attribute revocation. But, authority needed to enhance efficiency. Zu et al. [11] proposed CP-ABE scheme which utilized the access structure of linear secret sharing scheme (LSSS) to define access control in cloud storage service.

Junod et al. [16] proposed user revocation ABE scheme which utilized broadcast encryption scheme on ABE scheme. The data owner should take full charge of maintaining all the membership lists for each attribute group. However, it is not applicable to the cloud storage architecture because the data owner will no longer be directly in control of data.

III. SECURITY REQUIREMENTS OF ABE

They needed the scheme to be proved mathematically secure before being used. In 1949 Shannon came up with the first significant attempt to prove a scheme secure [11]. He came up with the term "perfectly" secure cipher. Informally, we can say an encryption scheme is perfectly secure if a ciphertext does not reveal anything about the plaintext without the key. The modern approach to proving schemes secure is referred to as "Provable Security".

IV. CONCLUSIONS

Increasing use of handheld devices and cloud system created data confidentiality and security as critical issues and ABE is the most prominent solution as per realworld requirements. ABE schemes useful in situations where list of users are unknown during

start. ABE scheme started foundation for encryption and access control. ABE gives fine grained control on decryptors. The advantage of ABE is key strength, enabling users to have a stronger encryption, than other encryption. Moreover, ABE schemes provides security against collusion attacks. Cryptanalysis has revealed that the complexity of the algorithm is of good order and cannot be made vulnerable.

REFERENCES

[1] S. Al-Riyami, J. Malone-Lee, and N. Smart. Escrow free encryption supporting cryptographic workflow. In International Journal of Information Security, volume 5, pages 217–230, September 2006.

[2] G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros. Practical group signatures without random oracles. Cryptology ePrint Archive, Report 2005/385, 2005.

[3] M. Bellare, D. Micciancio, and B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In Advances in Cryptology - EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science, pages 614–629. Springer-Verlag, 2003.

[4] M. Bellare, H. Shi, and C. Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In Topics in Cryptology CT-RSA 2005, volume 3376 of Lecture Notes in Computer Science, pages 136–153. Springer-Verlag, 2005.

[5] I. Blake, G. Seroussi, and N. Smart. Advances in Elliptic Curves in Cryptography. Cambridge University Press, 1 edition, 2004.

[6] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In Advances in Cryptology - CRYPTO 2001, volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer-Verlag, 2001.

[7] X. Boyen. Mesh Signatures: How to Leak a Secret with Unwitting and Unwilling Participants. In Advances in Cryptology - EUROCRYPT 2007, volume 4515 of Lecture Notes in Computer Science, pages 210–227. Springer-Verlag, 2007.

[8] L. Cheung and C. Newport. Provably Secure Ciphertext Policy ABE. In ACM Conference on Computer and Communications Security, pages 456–465, 2007.

[9] C. Cocks. An Identity Based Encryption Scheme Based on Quadratic Residues. In Proceedings of Cryptography and Coding, volume 2260 of Lecture Notes in Computer Science, pages 360–363. Springer-Verlag, 2001.

[10] V. Goyal, O. Pandeyy, A. Sahaiz, and B. Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In Proceedings of the 13th ACM conference on Computer and communications security, pages 89–98, 2006.

[11] D. Kahn. The Codebreakers, The Story of Secret Writing. MacMillan, 1st edition, 1967.

[12] N. Smart. Cryptography: An Introduction. Mcgraw-Hill College, 2004.

[13] B. Waters. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. Cryptology ePrint Archive, Report 2008/290, 2008. http://eprint.iacr.org/.

[14] M. Myers. Revocation: Options and Challenges. In Financial Cryptography, volume 1465 of Lecture Notes in Computer Science, pages 165–171. Springer-Verlag, 1998.

[15] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM conference on Computer and communications security, CCS '07, pages 195–203, New York, NY, USA, 2007. ACM.

[16] Ling Cheung and Calvin Newport. Provably secure ciphertext policy abe. In Proceedings of the 14th ACM conference on Computer and communications security, CCS '07, pages 456–465, New York, NY, USA, 2007. ACM.

[17] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In IEEE Symposium on Security and privacy, pages 321–334, 2007.