International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 3 –SEPTEMBER 2014.

Study of Public Key Based Encryption and Decryption Techniques

N. Parameshwar[*1], and D.K.Shareef[#2]

[*]*Student, Dept of CSE, Ananthalakshmi Institute of Technology & sciences , Affiliated to JNTUA University, ALITS- Anantapur*

[#] *Asst Professor, Dept of CSE, Ananthalakshmi Institute of Technology & sciences , Affiliated to JNTUA University, ALITS- Anantapur*

***Abstract*—In a distributed cloud environment, the user is provided with an untrusted service provider with a transformation key that allows the cloud to translate any ABE ciphertext satisfied by the user's attributes. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message. Anyways, this system does not guarantee the correctness of the transformation done by the cloud. Verifiability ensures whether the transformation has happened correctly or not. In this paper, we propose an improvised version of ABE with verifiability. A concrete scheme for ABE with verifiable outsourced decryption is proposed which is both secure and verifiable without relying upon random oracles.**

Keywords: ABE, CP-ABE, Verifiable C-ABE, Concrete ABE.

I. INTRODUCTION

In a distributed environment with untrusted servers such as cloud, complex-access control mechanisms are needed to access the encrypted data. Attribute Based Encryption (ABE) is a new public key based one-to-many encryption enabling control over encrypted data using access policies and ascribed attributes. ABE is a special case of functional encryption. In a public key encryption system, data is encrypted to be read by a particular individual who has already established a public key. In a functional encryption system, the functionality f(x:y) determines what a user with secret key y can learn from a cipher text encrypted under x. The enhanced functionality and flexibility provided by such systems is very appealing for many practical applications. Given many of the potential uses of ABE systems, constructing efficient systems ensuring strong security is an important concern.

The existing ABE schemes are selectively secure for which the security is proved for weaker model where a part of the cipher text must be revealed before the attacker receives the public parameters.

In this work, we propose improvements to the original ABE scheme to ensure verifiability and propose a Concrete-ABE (C-ABE) scheme with verifiable outsourced decryption. The proposed scheme substantially reduced the computation time required for resource-limited devices to recover plaintexts.

II. EXISTING SYSTEM

In an identity based encryption system, an authority distributes keys to users with associated identities, and messages are encrypted directly to identities. These schemes were proven secure in the random oracle model. Selectively secure schemes are constructed that confined to the partitioning strategy of the keys but incurs cost for large and complex models. Hierarchical Identity Based Encryption (HIBE)[2] expands the functionality of identity based encryption to include a hierarchical structure on identities, where identities can delegate secret keys to their subordinate identities. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher texts. There are two kinds of ABE schemes:

Key-policy ABE (KP-ABE) and Cipher text-policy ABE (CP-ABE). [1]

In a CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a cipher text only if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text. In a KP-ABE scheme, the roles of an attribute set and an access policy are swapped. The previous constructions for ABE schemes provide 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. 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. For ABE systems, private keys and cipher texts have much more structure in such a way that different keys with sharable attributes can be related and this severely restricts allowable partitions.

One of the efficiency drawbacks of the most existing ABE schemes is that decryption is expensive for resource-limited devices due to pairing operations. The complexity of the ABE model grows as the number of pairing keys to decrypt the cipher text grows.

To overcome the problems involved in the ABE schemes, we introduce an enhanced notion of ABE with outsourced decryption, eliminating the decryption overhead for the users.

III. PROPOSED SYSTEM

A C-ABE scheme is a ciphertext-policy attribute-based encryption system consists of four algorithms: Setup, Encrypt, KeyGen, and Decrypt.

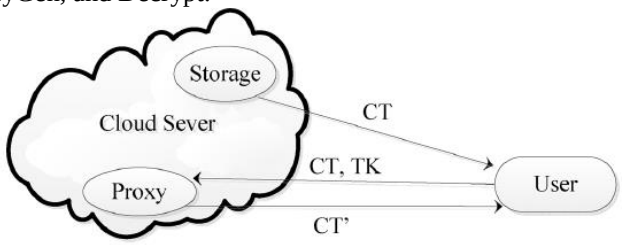

Fig 1: Concrete ABE scheme with outsourced decryption

Setup(λ,U) → (PK, MSK) :The setup algorithm takes in the security parameter λ and the attribute universe description U. It outputs the public parameters PK and a master secret key MSK.

Encrypt(PK,M, A) →CT :The encryption algorithm takes in the public parameters PK, the message M, and an access structure A over the universe of attributes. The result will be a ciphertext CT such that only users whose private keys satisfy the access structure A should be able to extract M.

KeyGen(MSK, PK, S) →SK: The key generation algorithm takes in the master secret key MSK, the public parameters PK, and a set of attributes S. It outputs a private key SK.

Decrypt(PK,CT, SK) →M :The decryption algorithm takes in the public parameters PK, a cipher text CT, and a private key SK. If the set of attributes of the private key satisfies the access structure of the cipher text, it outputs the message M.

For correctness, we require the following to hold:
1) If the set of attributes satisfies the access structure A, then M ←Decrypt(Pk, Sk_S, CT).
2) Otherwise, Decrypt(Pk, Sk_S, CT) outputs the error symbol ⊥ .
The security definition for C-ABE systems are as given below:

Setup: The challenger runs the Setup algorithm and gives the public parameters PK to the attacker.

Phase 1 The attacker queries the challenger for private keys corresponding to sets of attributes S1... Sq1.

Challenge The attacker declares two equal length messages M0 and M1 and an access structure A^*. This access structure cannot be satisfied by any of the queried attribute sets S1,....., Sq_1 . The challenger flips a random coin βϵ{0, 1}, and encrypts Mb under A^*, producing CT^*. It gives CT^* to the attacker.

Phase 2 The attacker queries the challenger for private keys corresponding to sets of attributes Sq_{1+1},.....,Sq, with the added restriction that none of these satisfy A^*.

Guess The attacker outputs a guess β' for β.

The advantage of an attacker is this game is de_ned to be Pr[β = β']-1/2 .
2 . We note that the model can easily be extended to handle chosen-ciphertext attacks by allowing for decryption queries in Phase 1 and Phase 2.

Definition 3 A cipher text-policy attribute-based encryption system is fully secure if all polynomial time attackers have at most a negligible advantage in this security game.

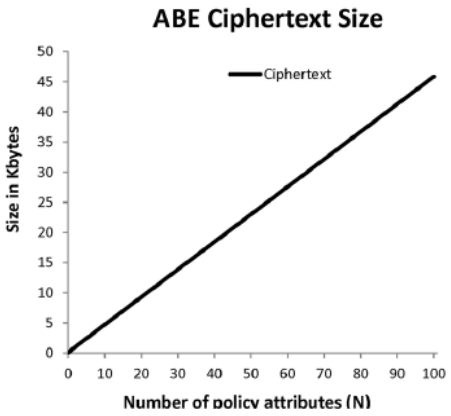

Fig 2: Performance of C-ABE for ciphertext size

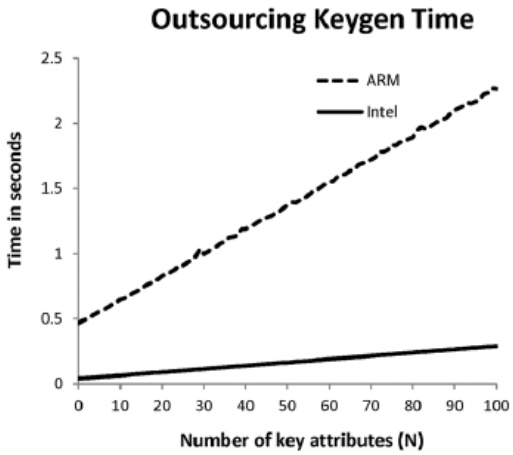

Fig 3: Performance of C-ABE for Outsourced Key generation

IV. CONCLUSION

The proposed ABE scheme with verified outsourcability does not rely upon the random oracles. The ABE ciphertext size and decryption/transformation time increase linearly as the cipher text policy's complexity grows. The proposed outsourcing substantially reduces the computation time required for devices with limited computing resource to recover the plaintext. The checksum value is taken as a commitment for the plain text which can checked if the transformation has happened correctly or not.

REFERENCES

[1] Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng , "Attribute-Based Encryption With Verifiable Outsourced Decryption" , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 8, AUGUST 2013 1343.

[2] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Proc. EUROCRYPT, 2010, pp. 62–91.

[3] M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.

[4] C. Dwork, "Differential Privacy: A Survey of Results," Proc. Fifth Int'l Conf. Theory and Applications of Models of Computation (TAMC),pp. 1-19, 2008.

[5] M. Green, A. Akinyele, and M. Rushanan, Libfenc: The Functional Encryption Library

[6] M. Bellare, A. Boldyreva, and A. Palacio, "An uninstantiable randomoracle- model scheme for a hybrid-encryption problem," in Proc. EUROCRYPT, 2004, pp. 171–188.