An Extensive Survey on Identity-Based Encryption with Added Secret Key in Cloud Computing

Kalpana Chouksey[1], Dr. Vineet Richhariya[2]

[1]M-Tech Research Scholar, [2]Research Guide & HOD, Department of Computer Science & Engineering

Lakshmi Narain College of Technology Bhopal

ABSTRACT: The study extended security notions for Identity Based Encryption (IBE) in settings where multiple Trusted Authorities (TAs) share some common parameters, as distinct from most existing research considering a single TA that issues keys to users in a system. The extension current notions of security for IBE to the multi-TA setting, and in addition, formalize the notion of TA anonymity. We study the security properties of natural multi-TA analogues of existing IBE schemes in both the Random Oracle Model (ROM) and the Standard Model with respect to these new notions. The applications of IBE schemes that not only share common parameters, but in addition share additional public parameters in such a way that a ciphertext created for an identity and a particular TA can be read by a recipient with the same identity, but with a private key issued by another TA. This gives us extensions to the basic IBE primitive which enable flexible and secure communications in coalition environments.

Keywords - Secret Key, Cloud, Identity, Encryption.

I. INTRODUCTION

Identity (ID)-based encryption, or IBE for short, is an exciting alternative to public-key encryption, which eliminates the need for a Public Key Infrastructure (PKI) that makes publicly available the mapping between identities, public keys, and validity of the latter. The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, because the identities (e.g. emails or IP addresses) together with common public parameters are sufficient for encryption. The private keys of the users are issued by a trusted third party called the private key generator (PKG).

The complexity of setting up an IBE infrastructure, for example, generating the public parameters of the TA for currently known IBE schemes that are practical to analyze, far exceeds the complexity of setting up an El-Gamal or RSA based PKE scheme. Almost all well known IBE schemes are pairing based which are not based on the mathematics of pairings) and in these schemes a number of complex issues need to be addressed { for example, appropriate elliptic curves need to be generated, the pairing map, the input and target groups and appropriate hash functions need to be defined. In addition, the representation of the various elements in the system needs to be unambiguously defined. If any kind of interoperability is desired, all these activities must be supported by appropriate standardization efforts, which lead us to the next point.

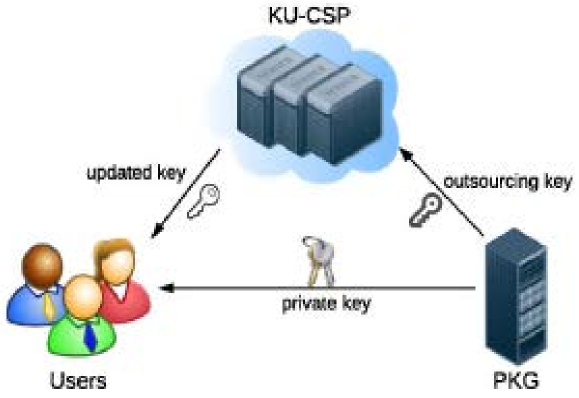

Fig. 1 System model for IBE with outsourced revocation

The complexity of setting up an IBE infrastructure, for example, generating the public parameters of the TA for currently known IBE schemes that are practical to analyze, far exceeds the complexity of setting up an El-Gamal or RSA based PKE scheme. Almost all well known IBE schemes are pairing based which are not based on the mathematics of pairings) and in these schemes a number of complex issues need to be addressed { for example, appropriate elliptic curves need to be generated, the pairing map, the input and target groups and appropriate hash functions need to be defined. In addition, the representation of the various elements in the system needs to be unambiguously defined. If any kind of interoperability is desired, all these activities must be supported by appropriate standardization efforts, which lead us to the next point.

Even when the standards are developed and perhaps even made freely available, it is not feasible to expect individual TAs to generate these parameters in a manner that is secure and inter-operable. Technology companies generate these parameters, over which they may hold exclusive rights, by virtue of holding patents over elliptic curves or other mathematical objects and algorithms on which they are based, and sell licences for their use. The cost of these licences often represents a significant investment for any corporate entity or governmental agency looking at a potential IBE deployment.

In the IBE setting, the security notion equivalent to Key Privacy is that of Recipient Anonymity: the ciphertext should not leak the identity of the (intended) recipient. The systematic study of Recipient Anonymity was initiated in, motivated both by its intrinsic interest in IBE and for its application in constructing Public Key Encryption with Keyword Search (PEKS) schemes. Since then, Recipient Anonymity has quickly become a standard security property for IBE schemes. In a hostile environment, traffic analysis can lead to the leakage of information relating to which entities are communicating and how frequently, which can often reveal important intelligence. As we will see, resistance to traffic analysis is not the only security concern in the multi-TA setting. We will also study the cryptographic implications of TA Anonymity on schemes that use IBE as a building block, later in this synopsis.

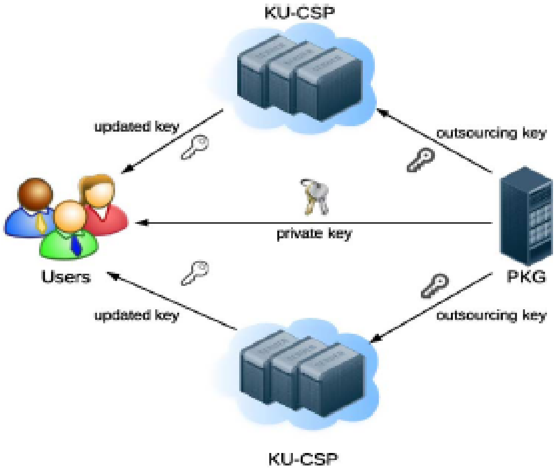

Fig. 2 System model with two KU-CSPs

II. PROBLEM IDENTIFICATION

In the existing system, the system developed on revocable IBE, there is little work presented. As mentioned before, Boneh and Franklin’s suggestion is more a viable solution but impractical. Hanaoka et al. proposed a way for users to periodically renew their private keys without interacting with PKG. However, the assumption required in their work is that each user needs to possess a tamper-resistant hardware device. Another solution is mediator-aided revocation. In this setting there is a special semi-trusted third party called a mediator who helps users to decrypt each cipher text. If an identity is revoked then the mediator is instructed to stop helping the user. Obviously, it is impractical since all users are unable to decrypt on their own and they need to communicate with mediator for each decryption. Further there is enough scope to enhance the security of the existing system by adding security levels in the existing infrastructure.

III. LITERATURE SURVEY

Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou [1], focused on the critical issue of identity revocation, we introduce outsourcing computation into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the proposed scheme is full-featured:

Wu Qiuxin, [2] Attribute-based encryption is drawing more attention with its inherent attractive properties which are potential to be widely used in the newly developing cloud computing. However, one of the main obstacles for its application is how to revoke the attributes of the users, though some ABE schemes have realized revocation, they mostly focused on the user revocation that revokes the user's whole attributes, or attribute revocation under the indirect revocation model such that all the users' private keys will be affected by the revocation. In this paper,authors define the model of CP-ABE supporting the attribute revocation under the direct revocation model, in which the revocation list is embed in the ciphertext and none of the users' private keys will be affected by the revocation process. Then authors propose a generic construction, and prove its security with the decision q-BDHE assumption.

Xin Chen; Patankar, H.; Sencun Zhu; Srivatsa, M.; Opper, J., [3] One of the key challenges in operational trust management is to continually monitor the behavior of a node and update its trust score accordingly - evidently, both speed and accuracy is of great importance here. To achieve these goals, several papers have explored the concept of mutual revocation (sometimes termed suicide) wherein the trust value of both the accuser and the accused node are temporarily set to zero without involving a quorum In addition, authors allow a trusted authority or a quorum may (periodically) review such partial mutual revocations and update the trust values of the accuser and the accused nodes accordingly (e.g., reward the accuser and punish the accused if the accusation was deemed true). Authors present a detailed design of the trust update functions for partial mutual revocation. Through the analysis, authors analyze the effectiveness of partial revocation under different attack strategies and report its performance in terms of revocation immediacy, revocation accuracy and abuse resistance.

IV. PROPOSED METHODOLOGY

Correctness: Any cloud server that faithfully follows the mechanism must produce an output that can be decrypted and verified successfully by the customer.Soundness: No cloud server can generate an incorrect output that can be decrypted and verified successfully by the customer with non-negligible probability.Input/output privacy: No sensitive information from the customer's private data can be derived by the cloud server during performing the LP computation.

Efficiency: The local computations done by customer should be substantially less than solving the original LP on his own. The computation burden on the cloud server should be within the comparable time complexity of existing practical algorithms solving LP problems.

We propose to apply problem transformation for mechanism design. The general framework is adopted from a generic approach, while our instantiation is completely different and novel. In this framework, the process on cloud server can be represented by algorithm ProofGen and the process on customer can be organized into three algorithms (KeyGen, ProbEnc, and ResultDec).

V. CONCLUSION

In this review paper we have studded The Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key Infrastructure (PKI) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in traditional PKI setting, but the cumbersome management of certificates is precisely the burden that IBE strives to alleviate.

REFERENCES

[1] Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, Senior Member, “Identity-Based Encryption with Outsourced Revocation in Cloud Computing” IEEE TRANSACTIONS ON COMPUTERS, VOL. 64, NO. 2, FEBRUARY 2015.

[2] Wu Qiuxin, "A generic construction of ciphertext-policy attribute-based encryption supporting attribute revocation," in Communications, China , vol.11, no.13, pp.93-100, Supplement 2014

[3] Xin Chen; Patankar, H.; Sencun Zhu; Srivatsa, M.; Opper, J., "Zigzag: Partial mutual revocation based trust management in tactical ad hoc networks," in Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on , vol., no., pp.131-139, 24-27 June 2013

[4] M. Abdalla, P. Fouque, and D. Pointcheval. Password-based authenticated key exchange in the three-party setting. In S. Vaudenay, editor, Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography - PKC 2005, pages 65{84. Springer-Verlag LNCS 3386, 2005.

[5] M. Abdalla and D. Pointcheval. Simple password-based encrypted key exchange protocols. In A. Menezes, editor, Proceedings of the RSA Conference: Topics in Cryptology - the Cryptographers' Track (CT-RSA 2005), pages 191/208. Springer-Verlag LNCS 3376, 2005.

[6] M. Abe and T. Okamoto. A signature scheme with message recovery as secure as discrete logarithm. In K. Lam, E. Okamoto, and C. Xing, editors, Advances in Cryptology - Proceedings of ASIACRYPT 1999, pages 378{389. Springer- Verlag LNCS 1716, 1999.

[7] S.S. Al-Riyami and K.G. Paterson. Certi¯cateless public key cryptography. In C.S. Laih, editor, Advances in Cryptology - Proceedings of ASIACRYPT 2003, pages 452{473. Springer-Verlag LNCS 2894, 2003.

[8] S.S. Al-Riyami and K.G. Paterson. Tripartite authenticated key agreement protocols from pairings. In K.G. Paterson, editor, Proceedings of the 9th IMA International Conference on Cryptography and Coding, pages 332{359. Springer-Verlag LNCS 2898, 2003.