International Journal of Computer Applications Technology and Research
Volume 4– Issue 5, 340 - 343, 2015, ISSN:- 2319–8656

A Novel Constant size Cipher-text Scheme for Security in Real-time Systems

M.Dhivya
Department of Computer Science and Engineering
Panimalar Institute of Technology, Chennai, India

Tina Belinda Miranda
Department of Computer Science and Engineering
Panimalar Institute of Technology, Chennai, India

S.Venkatraman
Department of Computer Science and Engineering
Panimalar Institute of Technology, Chennai, India

Abstract: In this paper, we consider 'secure attribute based system with short ciphertext' is a tool for implementing fine-grained access control over encrypted data, and is conceptually similar to traditional access control methods such as Role-Based Access Control. However, current 'secure attribute based system with short ciphertext' schemes suffer from the issue of having long decryption keys, in which the size is linear to and dependent on the number of attributes.Ciphertext-Policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. We propose a novel 'secure attribute based system with short ciphertext' scheme with constant-size decryption keys independent of the number of attributes. We found that the size can be as small as 672 bits.

Keywords – Attribute Based Encryption, Ciphertext Policy, Short Decryption Key.

1. INTRODUCTION

LIGHTWEIGHT devices (e.g. Radio Frequency Identification (RFID) tags) have been well known to have many useful applications[1]. This is useful for creating passports, ID cards and secret data storage, such as cryptographic key storage. Authorized persons generate a cryptographic key for each individual user. Then the key embedded within a user's ID card. The user can extract the key from his/her ID card for a security use.

Lightweight devices usually have limited memory capacity. This has become a major challenge to applications such as key storage. Many encryption systems can offer short decryption keys. Attribute-based encryption (ABE) is an extension of identity-based encryption which allows users to encrypt and decrypt messages based on attributes and access structures. Ciphertext-policy attribute-based encryption (CP-ABE) is a type of ABE schemes where the decryption key is associated with a user's attribute set. The encryptor encrypt the attributes for protect the data. We generate the group key for each individual user for protect the sensitive data. The encryptor defines the access structure to protect sensitive data such that only users whose attributes satisfy the access structure can decrypt the messages.[1]

Many CP-ABE schemes have been proposed for various purposes such as short ciphertext and full security proofs. However, we found no CP-ABE scheme with expressive access structures in the literature addressing the size issue of decryption keys, which seems to be a drawback due to resource consumption. All existing CP-ABE schemes suffer from the issue of long decryption keys, in which the length is dependent on the number of attributes.[2]

This issue becomes more obvious, when CP-ABE decryption keys are applied to storage-constrained devices. Because of the popularity of lightweight devices and useful applications of CP-ABE, in this work, we propose a provably secure CP-ABE scheme that offers short decryption keys, which are applicable for key storage in lightweight devices.[1],[2]

2. ARCHITECTURE

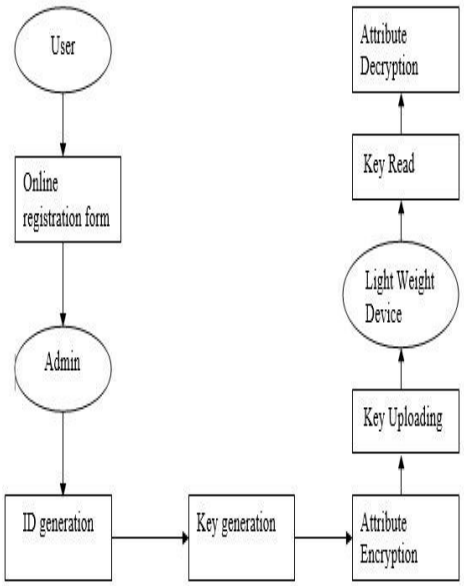

Fig.1. System Architecture

3. RELATED WORK

Attribute based Encryption consists of two variants of ABE: Key-Policy ABE and Ciphertext-Policy ABE.

KP-ABE: In a KP-ABE scheme, the ciphertext encrypting a message is associated with a set of attributes. A decryption key issued by an authority is associated with an access structure. The ciphertext can be decrypted with the decryption key if and only if the attribute set of ciphertext satisfies the access structure of decryption key.[12],[27]

CP-ABE: In a CP-ABE scheme, on the contrary, the ciphertext encrypts a message with an access structure while a decryption key is associated with a set of attributes. The decryption condition is similar: if and only if the attribute set fulfils the access structure[14].

John Bethencourt, Amit Sahai and Brent Waters presented a system for realizing complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. collusion attacks. Our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). Our system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple remote keys.In addition, we provide an implementation of our system and give performance measurement.

Serge Vaudenay provide strong definitions for security and privacy. Our model captures the notion of a powerful adversary who can monitor all communications, trace tags within a limited period of time, corrupt tags, and get side channel information on the reader output. Prove some constructions: narrow-strong and forward privacy based on a public-key cryptosystem, narrow-destructive privacy based on a random oracle, and weak privacy based on a pseudo random function.[5]

Work by Omkant Pandey and Amit Sahai Presented the first construction of a ciphertext-policy attribute based encryption scheme having a security proof based on a number theoretic assumption and supporting advanced access structures.[33]

Guojun Wang,Qin Liu and Jie Wu propose a hierarchical attribute-based encryption model by combining a HIBE system and a CP-ABE system,to provide fine-grained access control and full delegation.Based on this model to achieve high performance.we construct several traits such as high performance, fine-grained access control, scalability and full delegation.

Charan, K.Dinesh kumar and D.Arun Kumar Reddy propose verifiability guarantees that a user can effectively check if the transformation is correctly and proved it is secure. Attribute based Encryption schemes are that the access policy can be classified as key-policy and cipher-text policy.[4]

Kan Yang and Xiaohua Jia propose a revocable multi-authority CP-ABE scheme and apply it as the underlying technique to design the data access control scheme which can be applied in any remote storage systems, onlinesocial networks, etc..Attribute revocation method is efficient and also it has less Communication cost and Computation cost and is secure it can achieve both backward security and for forward security.

Venkateshprasad.kalluri and D.Haritha presents a Attribute –Based access to the media in the cloud where it uses CP-ABE technique to create an access control structure.By using this technique the encrypted data is trustworthy even on the untrusted server and also this requires flexible,cryptographic key management to support difficult access policies Yi Mu proposed a novel dynamical identity-based authenticated key management protocol to optimize key management for a user with multiple options.[8]

4. PROPOSED SYSTEM

In this proposed system scheme with constant-size decryption keys independent of the number of attributes. We found that the size can be as small as 672 bits. In comparison with other schemes in the literature, the proposed scheme is the only with expressive access structures, which is suitable for 'secure attribute based system with short ciphertext' key storage in lightweight devices. Because of the popularity of lightweight devices and useful applications of secure attribute based system with short ciphertext' , in this work, we propose a probably secure proposed system scheme that offers short decryption keys, which are applicable for key storage in lightweight devices.[17],[18],[19]

CP-ABE works under four ways Setup, Encrypt KeyGen and decrypt.

1. Setup:

The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

2. Encrypt (PK, M,A):

The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.[17]

3. Key Generation (MK, S):

The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

4. Decrypt(PK,CT, SK):

The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key or set S of attributes. If the set S of attributes satisfies the

access structure A then the algorithm will decrypt the ciphertext and return a message M.[5]

Efficiency:

The decryption key of our scheme is composed of two group elements only, and is independent of the number of attributes. Recently proposed attribute based encryption schemes in terms of policy type, access structure, security model, length of decryption key and length of ciphertext. We compare the efficiency of schemes under CPA (chosen plaintext attack) security only as previous schemes utilized different generalized security transformation from CPA to CCA.[6],[7]

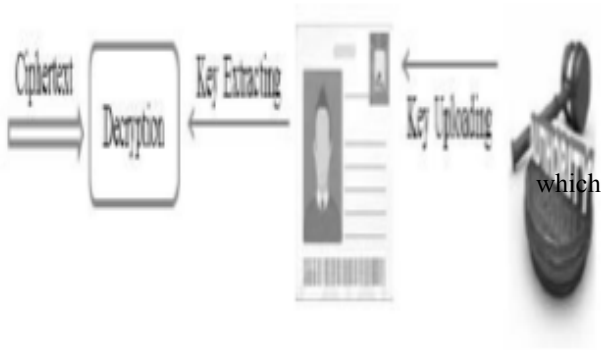

Fig.2. A Security use of decryption with decryption key stored in RFID tags embedded within ID cards.

Modules:

- Registration & ID Generation
- Key Generation & Encryption
- Uploading & Verification

Registration & ID Generation:

In this paper we develop a applying for Online Electronic Passport for this user has to register application form. User has to fill their own personal details and upload their individual photo for registration. After they submit the form authorized person will generate the ID for particular registered person. ID can be generated for every registered users.

Key Generation & Encryption:

Once Id has been generated authority will generate key for every registered person. This key contains public, private and secret key for each individual person. Based on the key only, attributes are encrypted and provide the cipher text values. Encryption is done independent on number of attributes with constant size decryption keys.

Uploading & Verification:

Authority generates a short decryption key and uploading into the device. Once encryption key has been generated it must be uploaded into the light weight devices. When user wants to see the content of his/her profile means he/she has to retrieve the key from the device. After key has been read from device they perform decryption and view full profile. Here verification is carried out, when the uploaded key and retrieved key are match means they perform some operations otherwise they didn't perform.

5. CONCLUSION

Light weight devices usually have limited memory storage, which could be too small to store decryption keys of secure attribute based system with short ciphertext schemes. We develop a project using ciphertext key for light weight devices. This CP-ABE should contain security, Performance and flexibility.[19]

Thus, the proposed scheme is very much useful in real time security systems. Future works may include schemes to reduce number of bits of key without compromising the security feature.

Thus, the proposed work can improve the real time systems.

6. REFERENCES

[1] S. Vaudenay, "On privacy models for RFID," in Proc. ASIACRYPT, 2007, vol. 4.

[2] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in Proc. ASIACRYPT, 2007, vol. 4.

[3] F. Guo, Y. Mu, and W. Susilo, "Identity-based traitor tracing with short private key and short ciphertext," in Proc. ESORICS, 2012, vol. 7.

[4] F. Guo, Y. Mu, and Z. Chen, "Identity-based encryption: How to decrypt multiple ciphertexts using a single decryption key," in Proc. Pairing, 2007, vol. 4.

[5] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-identity single-key decryption without random oracles," in Proc. Inscrypt, 2007, vol. 4.

[6] H. Guo, C. Xu, Z. Li, Y. Yao, and Y. Mu, "Efficient and dynamic key management for multiple identities in identity-based systems," Inf. Sci., vol. 2, Feb. 2013.

[7] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in Proc. CRYPTO, 2001, vol. 2.

[8] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. ACM Conf. Comput. Commun. Security, 2010.

[9] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, Jul. 2011.

[10] Z. Wan, J. Liu, and R. H. Deng, "Hasbe: A hierarchical attributebased solution for flexible and scalable access control in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 7, Apr. 2012.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006.

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, May 2007.

[13] L. Cheung and C. C. Newport, "Provably secure ciphertext policy abe," in Proc. ACM Conf. Comput. Commun. Security, 2007.

[14] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Public Key Cryptography., 2011, vol. 6.

[15] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in Proc. ISPEC, 2009, vol. 5.

[16] Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption: Extended abstract," in Proc. ACM Conf. Comput. Commun. Security, 2010.

[17] J. Herranz, F. Laguillaumie, and C. Ràfols, "Constant size ciphertexts in threshold attribute-based encryption," in Proc. Public Key Cryptography, 2010, vol. 6.

[18] 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, vol. 6.

[19] A. B. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in Proc. CRYPTO, 2012, vol. 7.

[20] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. EUROCRYPT, 2005, vol. 3.

[21] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. ACM Conf. Comput. Commun. Security, 2007.

[22] C. Chen et al., "Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures," in Proc. CT-RSA, 2013, vol. 7. GUO et al.: CP-ABE WITH CONSTANT-SIZE KEYS FOR LIGHTWEIGHT DEVICES 771

[23] N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in Proc. Public Key Cryptography., 2011, vol. 6.

[24] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," in Proc. ProvSec, 2011, vol. 6.

[25] A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang, "Threshold ciphertext policy attribute-based encryption with constant size ciphertexts," in Proc. ACISP, 2012, vol.
[26] T. Okamoto and K. Takashima, "Fully secure unbounded inner-product and attribute-based encryption," in Proc. ASIACRYPT, 2012, vol. 7.

[27] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proc. 35th ICALP, 2008, vol. 5.

[28] A. Sahai and B. Waters, "Attribute-based encryption for circuits from multilinear maps", CoRR, vol. abs/1210.5287, 2012.

[29] M. Chase, "Multi-authority attribute based encryption," in Proc. TCC, 2007, vol. 4.

[30] T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures," in Proc. ACNS, 2008, vol. 5.

[31] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Proc. Public Key Cryptography., 2013, vol.7.

[32] M. J. Hinek, S. Jiang, R. Safavi-Naini, and S. F. Shahandashti, "Attribute-based encryption without key cloning," IJACT, vol. 2, 2012.

[33]Z. Liu, Z. Cao, and D. Wong, "White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures," IEEE Trans. Inf. Forensics Security, vol. 8, Jan. 2013.