Collusion resistant broadcast encryption with short cipher texts and private keys

M.Surendar[1], S.Revanth raj[2], k.Blessing Christiana[3]

[1]*Student, Information Technology, New Prince Shri Bhavani College Of Engineering and Technology, Tamilnadu , India*

[2]*Student, Information Technology, New Prince Shri Bhavani College Of Engineering and Technology, Tamilnadu , India*

[1]*Assistant professor, Information Technology, New Prince Shri Bhavani College Of Engineering and Technology, Tamilnadu , India*

ABSTRACT

In this paper, we present an adaptively secure identity-based broadcast encryption system featuring constant sized ciphertext in the standard model. Size of the public key and the private keys of our system are both linear in the maximum number of receivers. Our system is fully collusion-resistant and has stateless receivers. Our scheme is well optimized for the broadcast encryption. The computational complexity of decryption of our scheme depends only on the number of receivers, not the maximum number of receivers of the system. Technically, we employ dual system encryption technique and our proposal offers adaptive security under the general subgroup decisional assumption. Our scheme demonstrates that the adaptive security of the schemes utilizing a composite order group can be proven under the general subgroup decisional assumption, while many existing systems working in a composite order group are secure under multiple subgroup decision assumptions.

Keyword: *Cryptography, public key, broadcast encryption, identity-based broadcast encryption, Subgroup decisional assumption.*

---

1. INTRODUCTION

BROADCAST encryption (BE) is a cryptographic primitive that enables a sender to share the encrypted data to multiple receivers over a broadcast channel efficiently. In a broadcast encryption system, a broadcaster adaptively chooses the set S of target users and sends the encryption of messages to them. The encrypted data can only be decrypted by recipients included in the set and any other cannot. The system is said to be full collusion resistant if even all users outside of S collude and pool their secret keys, they cannot obtain any non-trivial information about the contents of the broadcast. Furthermore, if anyone can play the role of broadcaster and encrypt with the public parameters, such system is called public key broadcast encryption.

2. EXISTING SYSTEM

It deals with providing cipher text values to the tag representation of files that have been shared between network nodes.

2.1 EXISTING ALGORITHM

- Tag Encryption Algorithm

2.2 ALGORITHM DEFINITION

The process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data.

2.3 DRAWBACKS

- Adaptive Security is very Low
- not suitable for data protection

3. PROPOSED SYSTEM

A new public key broadcast encryption (BE) for achieving adaptive security against arbitrary number of colluders.the private key size and public key size are all poly-logarithmic in the total number of users.

3.1 PROPOSED ALGORITHM

- Broadcast Encryption Systems

3.2 ALGORITNM DEFINITION

A broadcast encryption scheme consists of four randomized algorithms: Setup, KeyGen, Enc, Dec.

3.3 ADVATAGES

- Adaptive Security is high
- It is suitable for Data Protection
- we have proposed a fully collusion resistant broadcast encryption featuring constant ciphertexts

4. OVERALL ARCHITECTURE:

Fig

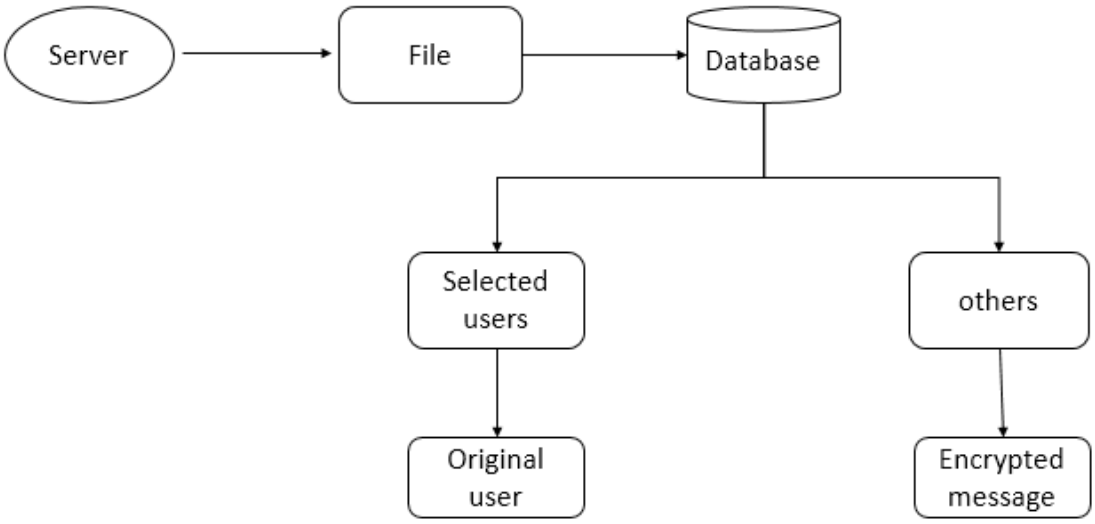

Figure: 4

5. FUTURE ENHANCEMENT

Identity-based broadcast encryption (IBBE) is a combination of broadcast encryption and identity-based encryption (IBE) that support exponentially many users as potential receivers.

5.1 FUTURE TECHNIQUE

- Identity-based broadcast encryption (IBBE)

5.2 TECHNIQUE DEFINITION

As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user

5.3 EXTRAVAGANCE

- More Security
- It is potential for many receivers

6. LITERATURE SURVEY:

We build the first public-key broadcast encryption systems that simultaneously achieve adaptive security against arbitrary number of colluders, have small system parameters, and have security proofs that do not rely on knowledge assumptions or complexity leveraging. Our schemes are built from either composite order multilinear maps or obfuscation and enjoy a ciphertext overhead, private key size, and public key size that are all poly-logarithmic in the total number of users. Previous broadcast schemes with similar parameters are either proven secure in a weaker static model, or rely on non-falsifiable knowledge assumptions.

7. CONCLUSION

We have analyzed the edge weights of this network are unpredictable and change rapidly rather than being static or time varying. To address the fastest-path problem in an eventdependent network, we proposed ONSC approaches to dynamically and promptly respond to queries for the nearest shelter with the fastest paths. Our designed NFG not only stored the fastest paths of the static network but also effectively sped up the calculation of the fastest path when the network changed frequently. ONSC with DRVF and DRVF-II algorithms was developed to address various system restrictions such as computing power and memory space. The hybrid method can be applied under special cases of EDG, particularly when the location of the impassable edge and the mobile clients are close to the root.

8. REFERENCE

- [[1] Sahana, an Open Source Disaster Management System. [Online]. Available: http://www.sahanafoundation.org/
- [2] Ushahidi, an Open Source Project for Crowd Sourcing Crisis Management. [Online]. Available: http://www.ushahidi.com/ and Mission4636, [Online]. Available: http://www.mission4636.org/
- [3] Google Crisis Response, an Open Disaster Management System. [Online]. Available: http://www.google.org/crisisresponse/

.

- [[4] I. C. Chang, H.-T. Tai, F.-H. Yeh, D.-L. Hsieh, and S.-H. Chang, "A VANET-based route planning algorithm for travelling time-and energyefficient GPS navigation App," *Int. J. Distrib. Sensor Netw.*, vol. 2013, 2013, Art. ID. 794521.
- [5] B. Yang, C. Guo, C. S. Jensen, M. Kaul, and S. Shang, "Stochastic skyline route planning under time-varying uncertainty," in *Proc. IEEE 30th ICDE*, 2014, pp. 1301–1314.
- [6] C. Lin, K.-L Choy, G. Pang, and M. T. W. Ng, "A data mining and optimization-based real-time mobile intelligent routing system for city logistics," in *Proc. IEEE 8th Int. Conf. Ind. Inf. Syst.*, 2013, pp. 156–161.
- [7] S. Xu, K. Deng, S. E. Li, S. Li, and B. Cheng, "Legendre pseudospectral computation of optimal speed profiles for vehicle eco-driving system," in *Proc. IEEE Intell. Veh. Symp.*, 2014, pp. 1103–1108.
- [8] Y. J. Zheng and H. F. Ling, "Emergency transportation planning in disaster relief supply chain management: A cooperative fuzzy optimization approach," *Soft Comput.*, vol. 17, no. 7, pp. 1301–1314, Jul. 2013.
- [9] K. Seongmoon, M. E. Lewis, and C. C. White, III, "Optimal vehicle routing with real-time traffic information," *IEEE Trans. Intell. Transp. Syst.*, vol. 6, no. 2, pp. 178–188, Jun. 2005.
- [10] H. Jeung, M. L. Yiu, X. Zhou, and C. S. Jensen, "Path prediction and predictive range querying in road network databases," *Int. J. Very Large Data Bases*, vol. 19, no. 4, pp. 585–602, Aug. 2010.