ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Secured Broadcast Encryption Using Key Generation

G.Deepika, N. Kavitha, M. Kiruthika, P.Visvanathan

B.E. Student, Dept. of CSE, Ganadipathy Tulsi's Jain Engineering College, Vellore, India

Assistant Professor, Dept. of CSE, Ganadipathy Tulsi's Jain Engineering College, Vellore, India

ABSTRACT: Show encryption (BE) plans permit a sender to safely telecast to any subset of individuals however require a trusted gathering to convey decoding keys. Bunch key understanding (GKA) conventions empower a gathering of individuals to arrange a typical encryption key through open systems so that lone the gathering individuals can decode the ciphertexts encoded under the common encryption key, however a sender can't prohibit a specific part from unscrambling the ciphertexts. In this paper, we connect these two ideas with a half breed primitive alluded to as contributory show encryption (ConBE). In this new primitive, a gathering of individuals arrange a typical open encryption key while every part holds a decoding key. A sender seeing the general population bunch encryption key can constrain the unscrambling to a subset of individuals from his decision. Tailing this model, we propose a ConBE plan with short ciphertexts. The plan is turned out to be completely agreement safe under the choice n-Bilinear Diffie-Hellman Exponentiation (BDHE) supposition in the standard model. Of autonomous interest, we display another BE plan that is aggregatable. The aggregatability property is appeared to be valuable to develop propelled conventions

KEYWORDS: Group key agreement (GKA), security, n-Bilinear Diffie-Hellman Exponentiation (BDHE), Scalability, confidentiality, integrity.

I. INTRODUCTION

Group key agreement (GKA) protocols enable a group of members to negotiate a common encryption key via open networks so that only the group members can decrypt the cipher texts encrypted under the shared encryption key, but a sender cannot exclude any particular member from decrypting the cipher texts. In this paper, we bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (ConBE). In this new primitive, a group of members negotiate a common public encryption key while each member holds a decryption key. A sender seeing the public group encryption key can limit the decryption to a subset of members of his choice. Following this model, we propose a ConBE scheme with short cipher texts. We present the Contributory Broadcast Encryption (ConBE) primitive, which is a hybrid of GKA and BE. Group key agreement, contributory broadcast encryption, and provable security.

II.ENCRYPTING WITH SHORT CIPHER TEXTS

The Contributory Broadcast Encryption (ConBE) primitive, which is a hybrid of GKA and BE. Using the public encryption key, anyone can encrypt any message to any subset of the group members and only the intended receivers can decrypt. In this paper, we bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (ConBE). In this new primitive, a group of members negotiate a common public encryption key while each member holds a decryption key. A sender seeing the public group encryption key can limit the decryption to a subset of members of his choice. Following this model, we propose a ConBE scheme with short cipher texts. The scheme is proven to be fully collusion-resistant under the decision n-Bilinear Diffie-Hellman Exponentiation (BDHE) assumption in the standard model.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

III.CONTRIBUTORY BROADCAST ENCRYPTION (CONBE).

The Contributory Broadcast Encryption (ConBE) primitive, which is a hybrid of GKA and BE. Using the public encryption key, anyone can encrypt any message to any subset of the group members and only the intended receivers can decrypt. In this paper, we bridge these two notions with a hybrid primitive referred to as contributory broadcast encryption (ConBE). In this new primitive, a group of members negotiate a common public encryption key while each member holds a decryption key. A sender seeing the public group encryption key can limit the decryption to a subset of members of his choice. Following this model, we propose a ConBE scheme with short cipher texts. The scheme is proven to be fully collusion-resistant under the decision n-Bilinear Diffie-Hellman Exponentiation (BDHE) assumption in the standard model. Of independent interest, we present a new BE scheme that is aggregately. The aggregatability property is shown to be useful to construct advanced protocols.

IV.CLIENT AUTHENTICATION SYSTEM

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It willsearch the query and display the query

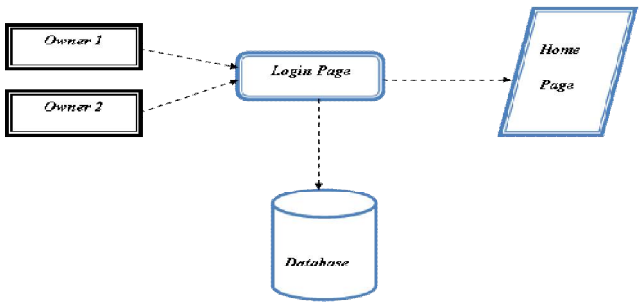

Fig.2 User Interface Design

V.GROUP CREATION

In this module focus to creating the Group. The Group Creation page to identify the records and available to users associated with a permission list when creating and viewing groups. If the person as a member of the group can send a file into the group members and also receive flies from any persons of the group.

VI.GENERATING THE FILE INTO DATABASE

In this module mainly we are focusing uploading the files. If the person as a member of the group can upload file into the group. That file can access only by an authorized group members. Uploading process is only occurred between the group members only.

VII.GENERATING THE ENCRYPTED FILE

In this module is used to help the Group member to encrypt the files and check their file is in safe also providing protection to the encrypted file. Encryption is the most effective way to achieve data security. Key Generation is the process for generating keys to our files. That key will have to be a unique for every group member while at the time of receives their file for decryption time.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

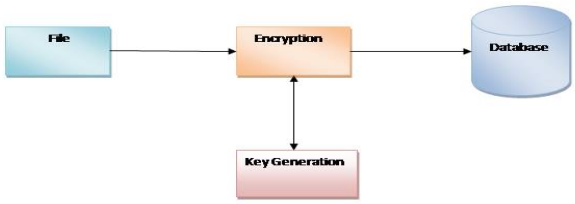

Fig.3 Encryption and Key Generation

VIII.RECOVERING THE ORIGINAL FILE THROUGH SECRET KEY

In this module is used to help the Group member to decrypt their encrypted the files. Decryption is the process of taking encoded or encrypted text or data and converting it back into plain text that Group member can read and understand.

IX. CONCLUSION

In ConBE, anyone can send secret messages to any subset of the group members, and the system does not require a trusted key server. Neither the change of the sender nor the dynamic choice of the intended receivers require extra rounds to negotiate group encryption/decryption keys. Following the ConBE model, we instantiated an efficient ConBE scheme that is secure in the standard model.

X. FUTURE WORK

Our future technique for authentication can be extended and used as the basis for an authentication scheme which is `proven' secure against any type of attack. Provided the discrete logarithm problem is intractable. Attacks to conference key and the personal private keys, are considered to demonstrate the security of the system.

REFERENCES

[1] A. Fiat and M. Naor, “Broadcast Encryption,” in Proc. Crypto 1993,1993, vol. LNCS 773, Lecture Notes in Computer Science, pp. 480-491.
[2] I. Ingemarsson, D.T. Tang and C.K. Wong, “A Conference Key DistributionSystem,” IEEE Transactions on Information Theory, vol. 28, no.5, pp. 714-720, 1982.
[3] Q. Wu, Y. Mu, W. Susilo, B. Qin and J. Domingo-Ferrer, “AsymmetricGroup Key Agreement,” in Proc. Eurocrypt 2009, 2009, vol. LNCS5479, Lecture Notes in Computer Science, pp. 153-170.
[4] http://en.wikipedia.org/wiki/PRISM %28surveillance program%29,2014.
[5] Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer and O. Farr`as, “BridgingBroadcast Encryption and Group Key Agreement,” in Proc. Asiacrypt2011, 2011, vol. LNCS 7073, Lecture Notes in Computer Science, pp.143-160.
[6] D. H. Phan, D. Pointcheval and M. Strefler, “Decentralized DynamicBroadcast Encryption,” in Proc. SCN 2012, 2011, vol. LNCS 7485,Lecture Notes in Computer Science, pp. 166-183.
[7] M. Steiner, G. Tsudik and M. Waidner, “Key Agreement in DynamicPeer Groups,” IEEE Transactions on Parallel and Distributed Systems,vol. 11, no. 8, pp. 769-780, 2000.
[8] A. Sherman and D. McGrew, “Key Establishment in Large DynamicGroups Using One-way Function Trees,” IEEE Transactions on SoftwareEngineering, vol. 29, no. 5, pp. 444-458, 2003.
[9] Y. Kim, A. Perrig and G. Tsudik, “Tree-Based Group Key Agreement,”ACM Transactions on Information System Security, vol. 7, no. 1, pp.60-96, 2004.
[10] Y. Mao, Y. Sun, M. Wu and K.J.R. Liu, “JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Management,”IEEE/ACM Transactions on Networking, vol. 14, no. 5, pp. 1128-1140,2006.
[11] C. Boyd and J.M. Gonz´alez-Nieto, “Round-Optimal Contributory ConferenceKey Agreement,” in Proc. PKC 2003, 2003, vol. LNCS 2567,Lecture Notes in Computer Science, pp. 161-174.
[12] W.-G. Tzeng and Z.-J.Tzeng, “Round Efficient Confe