Volume 6, Issue 10, October 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Secure Symmetric Key Broadcast Encryption (Skbe) for Sharingdata Over Dynamic Group Members

[1]Mahammad Salmasultana, [2]Ramachandran Vedantham
[1] (M.Tech) –CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Namburu, Guntur, Andhra Pradesh, India
[2] Associate Professor, Dept of IT, Vasireddy Venkatadri Institute of Technology (VVIT), Namburu, Guntur, Andhra Pradesh, India

Abstract:*Nowadays privacy is a primitivechallengefor any outsourced dataovergroup members or any networks in this connectionEncryption is used in a communication system to secure information in the transmitted messages from anyone other than the well-intended receiver. In order to perform the encryption and decryption,both i.e (encryption and decryption)keys should be matched at both end i.e. receiver and sender. As our presented systems stated that broadcast encryption (BE) is obligatory for secure data outsourcing over a group and Group key agreement (GKA) protocol let'screate a confidential channel among group members but due to lack of keymanagement and group member revocation is a still challenging issues. To overcome the challenges over prented system we proposed a Symmetric key broadcast encryption (SKBE) which leads the above issues effectively than our presented system.*

Keywords:*Broadcast encryption; Group key agreement; Symmetric key broadcast encryption (SKBE).*

I. INTRODUCTION

Nowadays privacy is a primitivechallenge for any outsourced data overgroup members or any networks there is an increasing demand of versatile cryptographic primitives to protect group communications and computation platforms lets take some of the platforms like instant-messaging tools, collaborative computing, mobile ad hoc networks and social networks for above platforms of applications cryptographic primitives consenting a sender to firmly encrypt to any subgroup of the users of the services without trusting on providers. Broadcast Encryption (BE) is a well-studied simple intentional for secure group concerned infrastructures. It lets sender to firmly broadcast to any subgroup members though, a BE system profoundly be contingent on a effusively reliable key server who yields secret decryption keys for the group members and can read all the communications to any members. As a result of the augmented fame with group concerned infrastructures and protocols, group communication occurs in many different settings from network layer multicasting to application layer. Regardless of the security services, underlying environment are necessary to provide communication privacy and integrity. While peer-to-peer security is a mature and well developed field, the secure group communication remains relatively unexplored. Contrary to a common initial impression, secure group communication is not a simple extension of secure two-party communication. There are two important differences. First, protocol efficiency is of greater concern due to the number of participants and distances among them. The second difference is due to group dynamics. Communication between two-parties can be viewed as a discrete phenomenon. It starts, lasts for a while, and ends. Group communication is more complicated. It starts and the group members leave and join the group and there might not be a well-defined end. A group key agreement (GKA) is another well-understood cryptographic primitive to secure group oriented communications. A conventional GKA allows a group of members to form a common secret key via open networks. However, whenever a sender wants to send a message to a group, he must first join the group and run a GKAs protocol to share a secret key with the intended members. More recently, and to overcome this limitation, Wu et al. introduced asymmetric group key agreement, in which only a common group public key is negotiated and each group member holds there different decryption key. However, neither conventional symmetric group key agreement nor the newly introduced asymmetric GKA allow the sender to unilaterally exclude any particular member from reading the plain text. Hence, it is essential to find more flexible cryptographic primitives allowing dynamic broadcasts without a fully trusted dealer. Contributory Broadcast Encryption (CBE) primitive, which is a hybrid of GKA and BE.

II. SYSTEM STUDY

As part of our presented system Group key agreement (GKA) is another well-understood cryptographic primitive to secure group-oriented communications. A conventional GKA allows a group of members to establish a common secret key via open networks. However, whenever a sender wants to send a message to a group, he must first join the group and run a GKA protocol to share a secret key with the intended receivers.

More recently, and to overcome this limitation, Wu et al. introduced asymmetric GKA, in which only a common group public key is negotiated and each group member holds a different decryption key.

However, neither conventional symmetric GKA nor the newly introduced asymmetric GKA allow the sender to unilaterally exclude any particular member from reading the plaintext. Hence, it is essential to find more flexible cryptographic primitives allowing dynamic broadcasts without fully trusted providers.

Challenges with Existing System:

The major challenges have been noticed under presented systems i.e

- Key management Issues
- User Revocation Problem i.eupdate the keys when users join or leave in network

2.1.Understanding of BE:

Broadcast encryption is the cryptographic problem of delivering encrypted content over a broadcast channel in such a way that only qualified users can decrypt the content. The challenge arises from the requirement that the set of qualified users can change in each broadcast emission, and therefore revocation of individual users or user groups should be possible using broadcast transmissions, only, and without affecting any remaining users. As efficient revocation is the primary objective of broadcast encryption

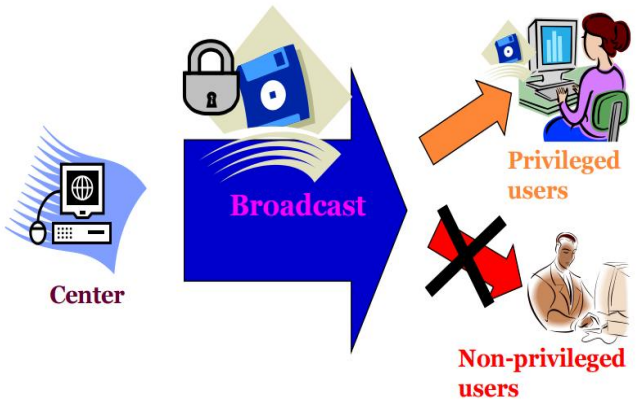

Fig 1.Message Broadcasting

In the above figure we have navigated how securely transmit a message to all members of the privileged subset How broadcast encryption works?

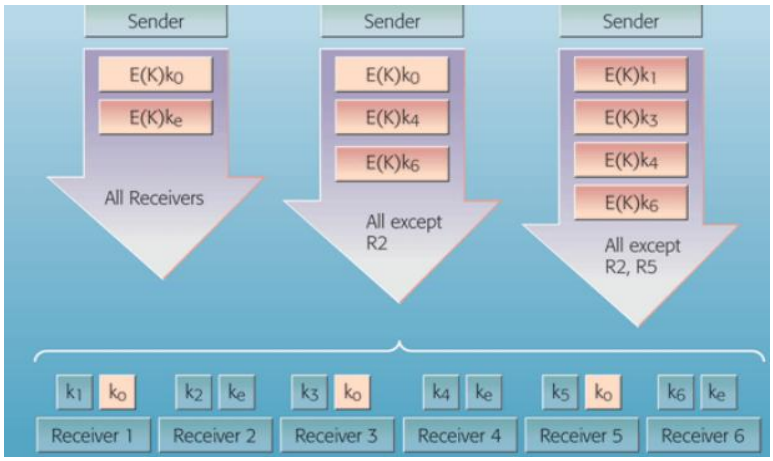

Fig 2.Broadcast encryption

Broadcast encryption [5] enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data. A. Fiat [5] described a broadcaster encrypts messages and transmits these to a group of users who are listening to a broadcast channel and use their private keys to decrypt transmissions. Cecile described dynamic broadcast encryption scheme involves two authorities: a group manager and a broadcaster. The group controller's grants new members access to the group by providing to each new member a public label lab and a decryption key dk. The generation of (lab, dk) is performed using a secret manager key. The broadcaster encrypts messages and transmits these to the whole group of users through the broadcast channel. In a public-key broadcast encryption scheme, the broadcaster does not hold any private information and encryption is performed with the help of a public group encryption key E(k)containing. When the broadcaster encrypts a message, some group members can be revoked temporarily from decrypting the broadcast content.

III. PROPOSED SYSTEM

In this paper we have proposed Symmetric key broadcast encryption (SKBE) which leads the above issues effectively than our presented system.

Symmetric Key Broad Encryption

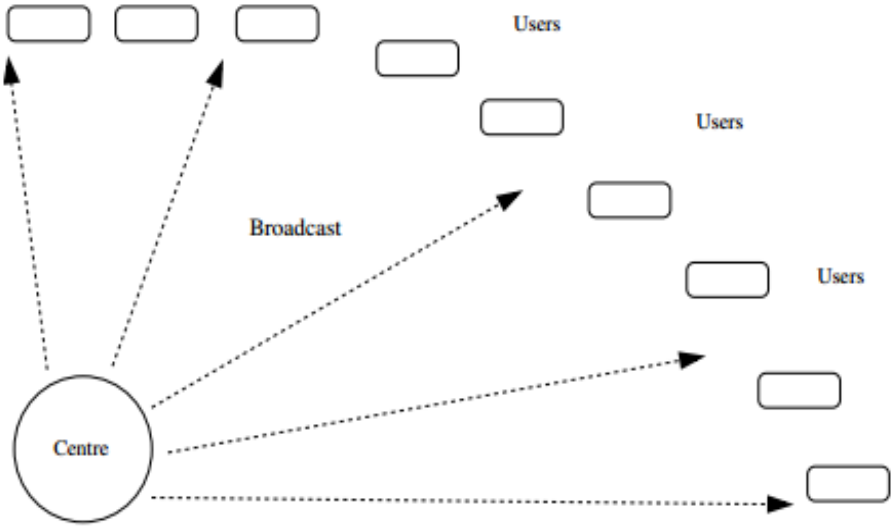

Fig3. Symmetric Key Broad Encryption

The centre pre-distributes secret information to the users. A broadcast takes place in a session. For each session: Some users are privileged and the rest are revoked. The actual message is encrypted once using a session key. The session key undergoes a number of separate encryptions. This determines the header. Only the privileged users are able to decrypt. A coalition of all the revoked users gets no information about the message.

Subset cover schemes

Identify a collection S consisting of subsets of users. Assign keys to each subset in S. To each user, assign secret information such that it is able to generate secret keys for each subset in S to which it belongs; and no more. During a broadcast, form a partition $\{S_1, \ldots, S_h\}$ of the set of privileged users with $S_i \in S$. The session key is encrypted using the keys for $S_1, \ldots, S_h$. Each privileged user can decrypt; no coalition of revoked users gains any information about the session key (or the message).

3.1. Optimized Key Management

The maintenance and the distribution of the keys (which involves re-keying also) for encryption/decryption is commonly called Group Key Management

The major security concern in broadcasting is key management. Traditional group key agreement protocols [1]-[3] are based on the traditional public key cryptography and hence require public key infrastructure (PKI) to issue and manage the public key certificates, which suffers from key escrow problem. The protocols generally requires O (n) or O (log n2) communication rounds for n number of participants. The issue of key management can be simplified by ID-based cryptosystem which overcomes the burden of heavy public key certificate managements [4]. In ID- based system user's unique identifiers itself functioned as its public key and often requires an offline trusted authority for generating their private key.Existing key management systems are implemented with two approaches called group key management and key distribution system [6].Group key agreement allows a group of users to negotiate a common secret key via open networks [7]. Then any member can encrypt any confidential message with the shared secret key and only the group members can decrypt. BE scheme in the literature are classified into two categories: **symmetric BE** and **public key BE**.

In the symmetric key setting, a common secret key is used for encryption and decryption. In broadcasting scenario, the broadcaster has to negotiate on a common shared secret key which involves a lot of communication among the different legitimate users, broadcast controllers and group controllers etc. In the public key setting, in addition to the secret keys for each user, the broadcaster also generates a public key for all the users. Conventional methods can avail the key pairs from the Private Key Generators (PKG) which suffers from key escrow problem. From the literature there exists taxonomy of key management schemes that can be used for secure group communication.

Each membership change in the group requires re-keying and the group may be highly dynamic, the major challenge of group key management is how to assure re-keying using the minimum bandwidth overhead and without increasing the storage overhead.

3.2.Key Distribution

This approach uses the centralized approach wherein usually a central authority who manages the entire multicast groups and its memberships. At the same time, the burden of managing the group of users is under the control of Group Controllers. The GC is responsible for the generation and distribution of identities to the group of users. Content is encrypted using a group key which is known to a group of users in many scenarios, When users leave or join the group, the group key must be changed and Prevent leaving members from decrypting content in the future ,Prevent joining members from decrypting previous content (backward secrecy) , O(n) messages

When a group member leave, GC (Group controller) must change the group key and inform all group members The GC computes the key share and unicast to the BC. Upon receiving all the keyshares from all valid groups, BC computes the final symmetric key.

Some of the primitive Key properties

1. Collusion freedom requires that any set of unauthorized scrupulous users

2. Key independence: a protocol is said key independent if a disclosure of a key does not compromise other keys.

3. Minimal trust: the key management scheme should not place trust in a high number of entities. Otherwise, the effective deployment of the scheme would not be easy.

3.3.User Revocation:

User revocation means when a user leave from the group, such users are treated as revoked users, they are not supposed to broadcast the data over subset group members due to user revocation .

User revocation can managed by following two mehods

1. Forward secrecy requires that the users who left the group should not have access to any future key. This ensures that a member cannot decrypt data after it leaves the group. To assure forward secrecy, a rekey of the group with a new Data Encryption Key (DEK) after each leave from the group is the ultimate solution.

2. Backward secrecy requires that a new user that joins the session should not have access to any old key. This ensures that a member cannot decrypt data sent before it joins the group. To assure backward secrecy, a re-key of the group with a new DEK after each join to the group is the ultimate solution.

IV. CONCLUSSION

In this paper, we formalized the Symmetric key broadcast encryption (SKBE). In SKBE, 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. In this paper we have been analysed broadcast encryption (BE) and its challenging issues as our proposed system we we formalized the Symmetric key broadcast encryption (SKBE)which leads the above issues effectively than our presented system.

REFERENCES

[1] ShanyuZheng, David Manz, and Jim Alves-Foss. “A communication computation efficient group key algorithm for large and dynamic groups”.Comput.Netw., 51(1):69–93, January 2007.

[2] Jim Alves-Foss. “An efficient secure authenticated group key exchange algorithm for large and dynamic groups”. In IN PROC. 23rd NATIONAL INFORMATION SYSTEMS SECURITY CONFERENCE, pages 254– 266, 2000.

[3] Yongdae Kim, Adrian Perrig, and Gene Tsudik. “Group key agreement efficient in communication”. IEEE Transactions on Computers, 53(7):905–921, 2004.

[4] D. H. Phan, D. Pointcheval and M. Strefler, “Decentralized Dynamic Broadcast Encryption,” in Proc. SCN 2012, 2011, vol. LNCS 7485, Lecture Notes in Computer Science, pp. 166-183

[5] A. Fiat and M. Naor, “Broadcast Encryption,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[6] Deepa S. Kumar and M. Abdul Rahman,”Design of ID-based Contributory Key ManagementScheme using Elliptic Curve Points for BroadcastEncryption”. International Journal of Computer Applications (0975 – 8887) Volume 129 – No.11, November2015

[7] M. Steiner, G. Tsudik and M. Waidner, “Key Agreement in Dynamic Peer 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 Dynamic Groups Using One-way Function Trees,” IEEE Transactions on Software Engineering, 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-ExitTree Amortization and Scheduling for Contributory Key Management,” IEEE/ACM Transactions on Networking, vol. 14, no. 5, pp. 1128-1140, 2006

[11] TL Praveena, V Ramachandran ,” Attribute based Multifactor Authentication for Cloud Applications” International Journal of Computer Applications ,2003.

[12] L Bandarupalli, VR Chandran, KS Babu,” Provision of an Effective Approach for Offering Improvised Results of Search Technique”, International Journal of Scientific Engineering Research 2016

[13] SH VRchand,” A Secure File Handling System using Modified Hash Based indexing”, International Conference on Advances in Soft Computing & Communication 2014.

[14] SAR Vedantam,” Innovative Cost-Effective Intranet-Based Chatting System using Android Wi-Fi” , 3rd International Conference on Reliability, Infocom Technologies and .. 2014

[15] BS Babu, V Ramachandran, "A Customized Search Engine for user Search Goals using CAP Algorithm", International Journal of Engineering Research and Technology 2014.

[16] DR Sridevi Sakhamuri , V.Ramachandran, "Misusability Weight Measure Using Ensemble Approaches", International Journal of Engineering Trends and Technology 2013

[17] DR Santhi Kolli , V.Ramachandran , "Personalized Query Results using User Search Logs" International Journal of Engineering Trends and Technology 2013

[18] V Ramachandran, RS Kishore, K Ramakalyani, "An Unmanned aerial vehicle model for Disaster analysis", International Journal of Advances in Computer, Electrical & Electronics ,2012.

[19] V RAMACHANDRAN, ES REDDY "A COMPREHENSIVE RADIOGRAPHIC DATABASE IMAGE RETRIEVAL SYSTEM FOR A COMPUTER AIDED DIAGNOSIS" , International Journal of Computer Science & Information Technology Research 2012

