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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on Data Security and Identity Based Crypto System for Secure Communication

Niveditha S[1], Ramalakshmi K[2], Sharmasth Vali Y[3]

B.E. Student, Dept. of C.S.E., Dhanalakshmi College of Engineering, Chennai, India[1,2]

Assistant Professor, Dept. of C.S.E., Dhanalakshmi College of Engineering, Chennai, India[3]

ABSTRACT: Secure Group Communication is very critical for applications like board-meeting, group discussions and teleconferencing. Secure group communication is usually required in modern collaborative and distributed application such as multi-party interactive computations. In general, group communications involve over open networks. Managing a set of secure group keys and group dynamics are the fundamental building blocks for secure group communication systems. A popular approach to secure group communication is to exploit Group Key Agreement (GKA). The Asymmetric Group Key Agreement (AGKA) helps a group of members to dynamically establish a public group encryption key while each member has a different secret decryption key in an identity based cryptosystem. In the real world, most group communication is dynamic, meaning that user can join or leave group frequently. Identity-based Authenticated Asymmetric Group Key Agreement (IBAAGKA) was proposed without key escrow.

KEYWORDS: Sender restriction, key management, identity based crypto system, Asymmetric group key agreement, Trust authority.

I. INTRODUCTION

Security enhanced group communication is usually required in modern distributed and collaborative applications such as multi-party interactive communications, peer-to-peer file sharing and distributed social networks. One of the popular approaches to secure group communications is to exploit group key agreement (GKA). Existing GKA protocols allow a group of members to interact over an open network to establish a common secret key. And then the group members can securely exchange messages using this shared key. With this protocol when a sender wants to send a secret message to n receivers, the sender has to first form the group with the receivers and run a GKA protocol (Fig 1). GKA is suitable for communication over open network.

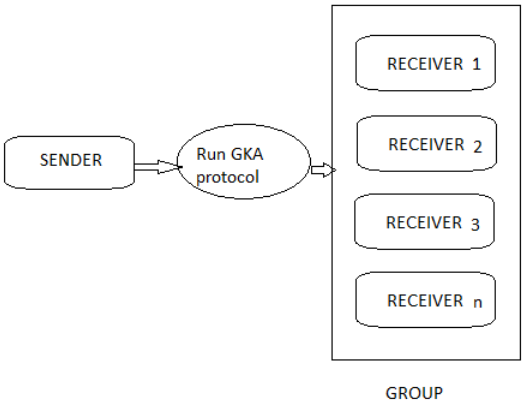

Figure 1 Sender running GKA Protocol to form a group

But in case of secured group communication GKA has some limitations. The limitation is that when the sender has to change dynamically he has to create a group with the group of receivers. So the conventional GKA protocol has *sender restriction* problem. Further, with the standard round notion of *key management* the best-known GKA protocols require two or more rounds to establish a secret key.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Another way to secure the group communication is to exploit the GKA called the AGKA. AGKA allows the members of the group to negotiate on a common group encryption key while holding different decryption keys. Any user may access the group encryption key and securely encrypt to the group members. Thus, AGKA is *sender-unrestricted.*

Since our environment is dynamic a authenticated AGKA protocol is used. This is based on strongly unforgeable state full identity-based batch multi-signatures (IBBMS). This method allows a signer to generate a batch identity-based signature to a set of messages carrying a piece of state information. Signatures from multiple signers, provided that these signatures were generated on the same messages under the same state information, can be partially aggregated into a batch multi-signature. The individual multi-signatures are valid if and only if the resulting batch multi-signature is valid.

The IBBMS scheme produce a new multi-signature for a previously signed message under the same state information, even if the attacker is allowed to adaptively choose messages and state information to query signatures. In this paper, we show that the scheme in is provably secure under the computational Diffie-Hellman assumption.

Based on the strongly unforgeable stateful IBBMS scheme, we extend the static protocol in into a dynamic IBAAGKA protocol without key escrow. In the dynamic protocol, we require a group manager to record the messages sent by other members. However, unlike a trusted dealer which is assumed to distribute secret keys, the group manager could be any member of the group and even leave the group.

Even if the long-term private key of the group manager is corrupted, the previously generated decryption keys of group members remain secure. The dynamic protocol is a one-round protocol. Specifically, if a member leaves the group, the group manager should only broadcast a message to other members. Further, if a user wants to join the group, the user only needs to send a message to the other members. The security of our dynamic protocol is proven under the *k*-bilinear Diffie-Hellman exponent assumption (which is widely used).

II. LITERATURE SURVEY

Title	**Techniques Employed**	**Benefits**
Entity authentication and key distribution[1]	Key distribution protocols	Without the assumption of trusting an individual authentication server, are needed where clients have no reason to trust individual servers
Realizing fully secure unrestricted ID-based ring signature in the standard model based on HIBE [2]	Hierarchical Identity-Based Encryption	User identities are arranged in an organizational hierarchy. Anyone can encrypt a message to any identity in the system using the public parameters.
Non-Interactive Key Establishment for Bundle Security Protocol of Space DTNs [3]	Bundle protocol (BP) in space delay/disruption tolerant networks (DTNs),	time-evolving topology model and two-channel cryptography to design efficient and non interactive key exchange protocol
Authenticated asymmetric group key agreement based on certificate less cryptosystem [4]	Asymmetric Group Key Agreement (AGKA)	construct distributed and one-round group key agreement protocols
Identity Based Authenticated Key	Identity based authenticated key agreement protocols using	Avoid key escrow by a Trust Authority (TA),

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

Agreement Protocols from Pairings [5]	the Weil or Tate pairings	
Identity Based Authenticated Group Key Agreement Protocol [6]	Tree-based Group Diffie-Hellman	Extending the Identity based two-party Authenticated Key Agreement protocol using the One-way function trees.
Provably secure one-round identity-based authenticated asymmetric group key agreement protocol, [7]	Identity-Based Authenticated Asymmetric Group Key Agreement (IB-AAGKA).	Constructs efficient identity-based batch multi-signature

III. SCOPE

The scope of this project is to provide a group of member to perform a secure communication. An intruder can't simply eaves drop a group communication because web socket protocol was proposed without key escrow. By knowing the group encryption key, any entity can encrypt to the group members. This can be used in high security information sharing areas like military bases and confidential meetings between higher organizations which need a secure line to pass the information. Files are also shared between multiple clients with same as the above process. Digital forensics and information system auditing also has to send their collected information, at that point this project is used to transfer secure information.

IV. DRAWBACKS OF EXISTING SYSTEM

- If all group members' private keys are leaked, then the previously established secrets will be exposed to the attacker and the protocol is no longer secure.
- Security is less, because the active and passive attackers intrude the data easily.
- All users have to stay online to finish the protocol before they can receive any encrypted contents.

V. NEED FOR PROPOSED SYSTEM

In the existing system the sender is restricted and the network is static. This is inefficient because the sender may change frequently. Group Key Agreement protocol requires two or more rounds to establish a secret key.

VI. BENEFITS OF PROPOSED SYSTEM

- It provides a group encryption key and respective secret decryption keys for each participant.
- An intruder can't simply eavesdrop a group communication because IBAAGKA protocol was proposed without key escrow.
- The group is dynamic, that is user may join or leave the group.
- It provides communication efficiently.
- This system is key escrow free.
- An attacker cannot break the secrecy of previous protocol runs even if the attacker obtains all the members long-term private keys.
- General session is maintained between the Server and Client.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

VII. ARCHITECTURE

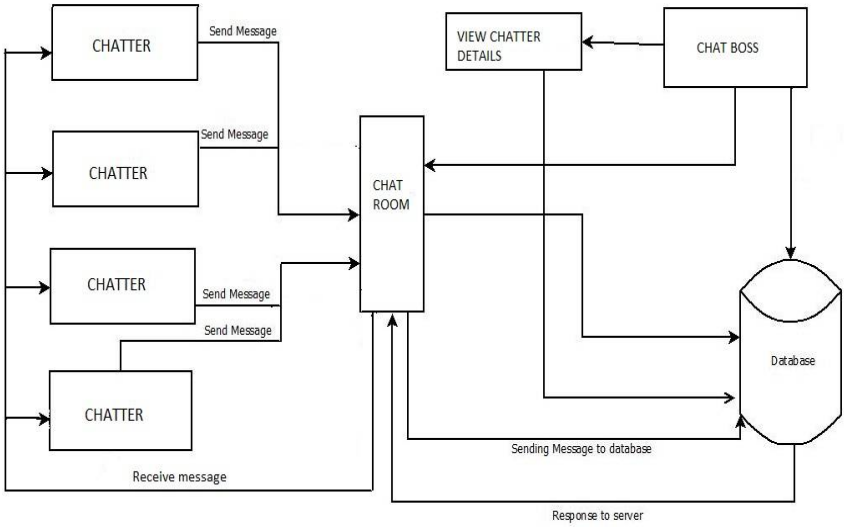

Fig.3 System Architecture

In this architecture the sender first registers himself with the admin. The admin is the overall controller of the communication system. By registering with the admin the user creates an account for him and becomes a member of the group. The user details and his login credentials are stored in the database and is verified when he tries to login again. Thereafter he can start sending messages in the group. The messages sent by a user are also stored in the database and is broadcasted to all the members of the group.

VIII. SPLINTERS

After careful analysis the system has been identified to have the following modules:

- User (Chatter)
- Admin (Chat boss)
- Group chat
- Solo chat
- Chat management

User :

In this module, the user side login will be authenticated and session is maintained. User registration must be needed in this module. The user login and registration is common for both the Server and Client. To begin the secure communication between the clients, initially server-side must run the application. This feature helps group of people to share or exchange information in a group without loss of data. The entire member in the group can able to interact with each other. Members in a group are allowed to join or leave the group. Information which is shared within the group member is securely maintained by using the encryption and decryption process.

Admin:

In this module, the Admin side login will be authenticated and session is maintained. Here the Admin role will be IP configurations are provided to group members. So that unauthorized persons can't able to enter into the group. Admin can able to view the member of the group that are created. In case if members of group need to be update, the admin can able to make the changes. If any member's account has to be removed from group, the admin have authority to proceed.

Group chat:

In this module the client after logging in to the account becomes a member of the group. The group chat page opens and all the users who are present in the group can be seen. The chatter is displayed with the previous conversation messages that are been sent in the group. Now the current user also becomes a member and he can send the messages.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

The chatter can also attach various kinds of attachment files like text, audio, video and graphics contents. The message sent by a user is stored in the database and is then broadcasted in the group. The messages are secured using the Asymmetric group agreement using K-linear Diffie Hellman algorithm.

Solo Chat:
In solo chat the chatting is done between two individual users of the group. These messages can be viewed between two users only. This message is also stored in the database and is then sent to the other user. Similar to the group chat in solo chat also the chatters can send all the types of files as an attachment.

Chat management:
The chat management is carried out by the admin or the chat boss. The chat management includes verifying the chatter or user details from the database. The admin can also view the current status of a user whether he is online or not. Also the messages sent by the user can be viewed. All the users' activities are monitored by the admin in the chat management module.

IX. CONCLUSION

We have defined the security model for dynamic IBAAGKA protocols using the k linear Diffie Hellman algorithm. Using this the communication system is dynamic without the sender restriction problem. The group communication is identity based and is secured using multiparty signatures. To provide dynamic secure group communications by proposing a one-round dynamic asymmetric group key agreement protocol which allows a group of members to establish a public group encryption key while each member has a different decryption key in an identity- based cryptosystem.

X. FUTURE ENHANCEMENTS

- In future, the group admin can mute a single person chat in a group to avoid unwanted Circumstances.
- Based on the user requirement it is possible to implement the video communication for my web application.

XI. ACKNOWLEDGEMENT

We would like to thank our Project Guide, Mr.Sharmasth Vali Y, for the guidance, inspiration and constructive suggestions that helped us in coming so far in the project. We are grateful to him. We also thank our Head of Department, Dr.Sivasubramanian S, for his support and valuable suggestions. We also acknowledge our colleagues who have helped us in building the project so far.

REFERENCES

[1] M. Bellare and P. Rogaway, "Entity authentication and key distribution," in Proc. 13th Annu. Int. Cryptol. Conf. (CRYPTO), 1994,pp. 232–249.
[2] M. H. Au, J. K. Liu,W. Susilo, and J. Zhou, "Realizing fully secure unrestricted ID-based ring signature in the standard model based on HIBE," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1909–1922, Dec. 2013.
[3] X. Lv, Y. Mu, and H. Li, "Non-interactive key establishment for bundle security protocol of space DTNs," IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, pp. 5–13, Jan. 2014.
[4] X. Lv, H. Li, and B. Wang, "Authenticated asymmetric group key agreement based on certificate less cryptosystem," Int. J. Comput. Math., vol. 91, no. 3, pp. 447–460, 2014.
[5] L. Chen and C. Kudla, "Identity based authenticated key agreement protocols from pairings," in Proc. 16th IEEE Comput. Security Found. Workshop (CSFW), Jun./Jul. 2003, pp. 219–233.
[6] K. C. Reddy and D. Nalla, "Identity based authenticated group key agreement protocol," in Proc. 3rd Int. Conf. Cryptol.India (INDOCRYPT), 2002, pp. 215–233.
[7] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "Provably secure one-round identity-based authenticated asymmetric group key agreement protocol," Inf. Sci., vol. 181, no. 19, pp. 4318–4329,
2011.