ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

ADAPTIVELY SECURE BROADCAST ENCRYPTION WITH SHORT CIPHERTEXTS

A.S.Subaira[1],M.Keerthana[2],D.Jeeva[3]

[1]Assistant Professor,[2]Assistant Professor, [3]PGscholar

Department of Computer Science and Engineering,

Mahendra College of Engineering,Salem,

[1]subairaas@mahendracollege.com,[2]keerthanam@mahendracollege.com,[3] jeevadhanapal94@gmail.com

ABSTRACT

An adaptively secure broadcast encryption scheme with short ciphertexts, where the size of broadcast encryption message is fixed regardless of the size of the broadcast group is constructed,here the members can join and leave the group without requiring any change to public parameters of the system or private keys of existing members.This construction has a two fold improvement over previously known best broadcast encryption schemes.This is 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. This scheme immediately yields adaptive security without any increase in the size of ciphertexts or use of a random oracle. Secondly, the proof of security in the proposed scheme is defined in a stronger security model closely simulating an adversary in real world.In this security model, the adversary can selectively query private keys of the group members after the setup and can receive decryption of broadcast encryption messages at any given time.

1.INTRODUCTION

A Network is defined as a group of systems such as windows desktop and server platforms that connect together for the purpose of sharing resources. Typical resources include printers, storage devices and folders that include files and other data that users may wish to use. Networks are used to give centralized access to networked resources and generally, the entire network all connect up to the biggest shared resource in use today – the World Wide Web. Tie all of these dissimilar systems and resources together and you can start to see why so many people have issues connecting to, staying connected to or just plain 'setting up' their networks. Keeping a network operational after it is created is another challenge – especially when you start to use it over unsecured connections.

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms.The businesses create an "intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed. [7] discussed about a system, In this proposal, a neural network approach is proposed for energy conservation routing in a wireless sensor network. Our designed neural network system has been successfully applied to our scheme of energy conservation. Neural network is applied to predict Most Significant Node and selecting the Group Head amongst the association of sensor nodes in the network.

2.EXISTING SYSTEM

The broadcast encryption system for N users is constructed by generalizing the BGW construction where all the parameters such as ciphertext overhead, secret key size, and public key size are poly-logarithmic in N.By increasing the number of users to 2λ, identity-based scheme is achieved with constant-size parameters namely, with no upper bound on the size of the recipient set. However,similar to the BGW scheme, this is only proved statically secure. Boneh, Waters, and Zhandry additionally present a scheme where they are unable to prove security relative to static assumptions, and instead proved security in a generic model for multilinear maps.

Disadvantages

- Adaptive Security is not possible.
- Only Static Security is possible.
- Hash Function SHA-1 is used which may result in collusion.
- Semantic security is not possible because of probability of collusion.
- Number of users has to be defined at the initial stage.

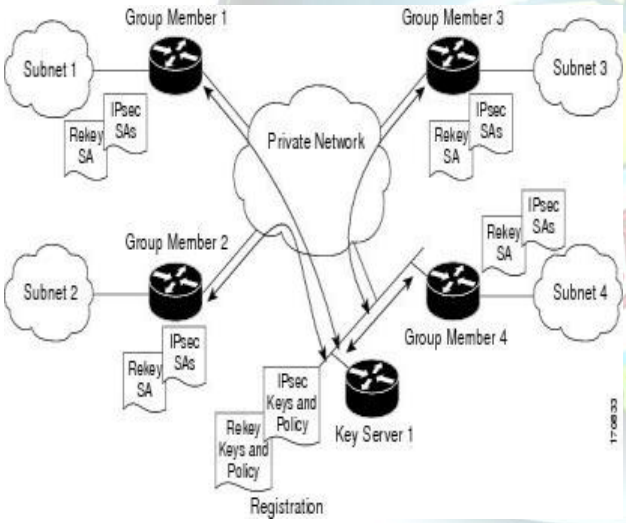
3.PROPOSED SYSTEM

An adaptively secure broadcast system where all parameters such as ciphertexts, secret keys, and public keys are poly-logarithmic in the number of users is constructed. As the number of users is polynomial, such poly-logarithmic terms can be bounded by the security parameter. Thus the parameter sizes can be taken to be independent of the number of users, which is the best possible structure for broadcast encryption. A system is achieved that is provably fully collusion resistant under adaptive attacks. Arguably, this is the right model for security in broadcast encryption systems.The system provides both semantic security and adaptive security where it is impossible for the collusion to occur.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

4. SYSTEM ARCHITECTURE

User login into user window then if it is a valid user means then it can communicate with the cloud server. The registered users can send and receive the data or files. Sender is injecting the information into the server that is encrypted message. The receiver will receive the particular message and can decrypt the message by same. That particular message is routed by identity based routing to clustered receivers .While receiving the message subscriber and publisher are known the same key that is randomly generated key. Finally the decrypted message is received by the subscriber.



System Architecture

Advantages

- It provides Adaptive security .
- Identity-based broadcast encryption (IBBE) is a combination of broadcast encryption and identity-based encryption (IBE) that support exponentially many users as potential receivers.
- Hash function SHA-2 is used which restricts the collusion.
- It provides Semantic Security.
- The number of users can be added or reduced at any point of time

4. MODULE DESCRIPTION

4.1 User Interface design

Application Users need to view the application they need to login through the User Interface. GUI is the media to connect User and Media Database and login screen where user can input the user name, password and password will check in database, if that will be a valid username and password then the user can access the database.

.4.2 Generating Secret key for all Users

Each authority monitors a set of attributes and issues secret keys to users accordingly. To resist the collusion attacks, a user's secret keys are tied to the users GID. Especially, a user can obtain secret keys for the attributes from multiple authorities without them knowing any information about the GID and attributes

4.3 Broadcast Encryption of Data

A Sender associates each encrypted event with a set of credentials. Adapted identity-based encryption (IBE) mechanisms is implemented to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

ensure that a particular receiver can decrypt an event only if there is a match between the credentials associated with the event and the key and to allows the receiver to verify the authenticity of received events. In identity-based encryption, any valid string which uniquely identifies a user can be the public key of the user. A key server maintains a single pair of public and private master keys. The master public key can be used by the sender to encrypt and send the messages to a user with any identity.

4.4 Decryption Analysis for key

The use of searchable encryption to enable efficient routing of encrypted events and routing is in the order of receiver attributes.Extensions of the cryptographic methods is to provide efficient routing events by the use of searchable encryption. For the routing of events from Sender to the relevant receiver, we use the content-based data model. The key is used to decrypt events but rather it facilitates the routing of encrypted events from sender to receiver.

4.5 Group message for all Users

The message is sent to all the group members, the group users want to decrypt the message with respect to secret key. Secret keys assigned to the receivers are labeled with the credentials. Finally,the assumption is made that the presence of secure channels for the distribution of message securely.

4.6 Performance Evaluation

Network performance is the analysis and review of collective network statistics, to define the quality of services offered by the underlying computer network.It is a qualitative and quantitative process that measures and defines the performance level of a given network. It guides a network administrator in the review, measure and improvement of network services. Network performance is primarily measured from an end-user perspective.

5.CONCLUSION

A fully collusion resistant broadcast encryption featuring constant cipher texts using composite order multilinear maps is constructed. Furthermore, the sizes of secret key and public key are both poly-logarithmic in the total number of users. Next, the method of Lewko and Waters is generalized for realizing dual system encryption to the composite order multilinear maps. Then, the adaptive security is proved under three static assumptions in the standard model. How to transform this broadcast encryption system into prime order groups with security from standard assumptions is an interesting topic for the future work.

REFERENCES:

[1] A. Fiat and M. Naor, "Broadcast encryption," in Advances in Cryptology—CRYPTO 1993. Santa Barbara, CA, USA: Springer, 1993, pp. 480–491.

[2] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in Advances in Cryptology—CRYPTO 2005. Santa Barbara, CA, USA: Springer, 2005, pp. 258–275.

[3] D. Boneh, B. Waters, and M. Zhandry, "Low overhead broadcast encryption from multilinear maps," in Advances in Cryptology—CRYPTO 2014. Santa Barbara, CA, USA: Springer, 2014, pp. 206–223.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

[4] T. Laarhoven, J. Doumen, P. Roelse, B. Škori´c, and B. de Weger, "Dynamic Tardos traitor tracing schemes," IEEE Trans. Inf. Theory, vol. 59, no. 7, pp. 4230–4242, Jul. 2013.

[5] B. Chor, A. Fiat, M. Naor, and B. Pinkas, "Tracing traitors," IEEE Trans. Inf. Theory, vol. 46, no. 3, pp. 893–910, May 2000.

[6] D. Boneh and M. Zhandry, "Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation," in Advances in Cryptology—CRYPTO 2014. Santa Barbara, CA, USA: Springer, 2014, pp. 480–499.

[7] Christo Ananth, A.Nasrin Banu, M.Manju, S.Nilofer, S.Mageshwari, A.Peratchi Selvi, "Efficient Energy Management Routing in WSN", International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE), Volume 1, Issue 1, August 2015,pp:16-19

[8] J.-S. Coron, T. Lepoint, and M. Tibouchi, "Practical multilinear maps over the integers," in Advances in Cryptology—CRYPTO 2013. Santa Barbara, CA, USA: Springer, 2013, pp. 476–493.

[9] M. Zhandry, "Adaptively secure broadcast encryption with small system parameters," IACR Cryptology ePrint Archive, p. 757, 2014.[Online]. Available: http://eprint.iacr.org/2014/757

[10] S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters, "Building efficient fully collusion-resilient traitor tracing and revocation schemes," in Proc. 17th ACM Conf. Comput.Commun. Security, Chicago, IL, USA, 2010, pp. 121–130.