ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

Key Generation of Attribute Based Broadcast Encryption

Manali.B.Chaudhari[1], Viral.V.Kapadia[2]

ME Student, Department of Computer Engineering, B.V.M Engineering college, Vallabh Vidhaya Nagar, Anand, Gujarat, India.[1]

Assistant Professor, Department of Computer Engineering, B.V.M Engineering college, Vallabh Vidhaya Nagar, Anand, Gujarat, India[2]

Abstract: Broadcast Encryption (BE) scheme is allows the sender to securely distribute a data to a dynamically changing set of users over a unsecure channel. Attribute based Broadcast Encryption (ABBE) is a excellent approach for broadcasting. Existing BE classical BE approach required an explicitly specified decrypter list. In ABBE differentiate groups of users by their attribute. In ABBE encrypter enforces an expressive access policy composed of one or more attributes. ABBE is more flexible and efficient with reduce storage overhead. Proposed algorithm is ABBE using RSA. Merge the advantage of both the algorithm. Using this scheme reduce the burden of key calculation of ABBE. RSA provide secure transmission over transmission channel. Main advantage of rsa is prime factorization. in this scheme use attribute as a prime number.

Keywords: attribute based broadcasting encryption,RSA,broadcast encryption.

I. INTRODUCTION

Securing a broadcast channel is always been interesting and challenging task for cryptographers. Broadcast encryption is used whenever a sender wants to send a message to more than one recipients using unsecure channel. such a scheme really allows to broadcaster to choose dynamically a subset of privileged users. For example in a online group activity, Thomas may belong to many different activity such as code solution provider for c,c++,java, .net, oracle etc. Thomas want to share his code with those member who are interested in both c and c++ activity. For this broadcasting it is insufficient to use pairwise or public key encryption for each receiver since the ciphertext size is linearly proposed to number of intended recipient in the online group activity.

Many to many communication can be achieved by basic Broadcast encryption scheme.[1] major drawback of this system is sender need to explicitly specify list of intended receiver. for large system it is very difficult to specify a public key of each receiver. As in previous example Thomas may hardly know who are interested in c and c++. Retrieving and storing public key of every intended receiver before performing encryption is very expensive and introduce unacceptable delay. In internet world security is major concern for every transmission. it is need for secure and speed transmission a)encrypter does not explicitly specify list of intended receiver b)number of public key should be small c) access is securely controlled[1]

Attribute Based Broadcast Encryption (ABBE) scheme satisfy the criteria which describe above. In this scheme encryption and decryption is based on attributes. Attributes are descriptive string. Each user is tagged with multiple attributes. And each attribute is shared by multiple users. ABBE scheme overcome the existing broadcast encryption(BE) problem. compared with conventional broadcast encryption, ABBE is separating users into different groups based on attributes.

The broadcast encrypter can define an expressive access policy using the multiple attributes which are define entities who can decrypt the message.

II. BASIC ALGORITHM FOR ABBE.

A. *Concept*

people are identify by their attributes. in ABBE during the encryption process access policy and public key are used to generate ciphertext. At the decrypter side ciphertext along with the set of attributes are used to decrypt the message. Ciphertext size is linearly proportional to the numbers of attributes although ABBE is more efficient and flexible.

B. *ABBE algorithm*

- Attribute-based broadcast encryption scheme with security parameter is a tuple of three randomized algorithms. 1)setup 2)encrypt 3)decrypt.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
Vol. 2, Issue 5, May 2013

- Setup (, n, (B(u))1=u=n): takes as input the security parameter , the number of users n, and groups of users. It outputs an encryption key EK, and n decryption keys (dku)1=u=n.
- Encrypt (EK,BN ,BR): takes as input the encryption key EK and two sets of groups BN and BR. It outputs a header hdr and a message encryption key K . K is a finite set of message encryption keys.
- Decrypt (dku,hdr): takes as input a decryption key given to a user u and a header hdr. If the header hdr comes from an encryption using (BN ,BR)such that BN. B(u)and B(u)n BR = Ø, then it outputs a message encryption key K . K. In the other case, it outputs ⊥.
- In the encryption process, a message M is encrypted with a key K and the resulting ciphertext C is sent together with the header hdr. Users in all groups mentioned in BN (needed groups) and outside all groups mentioned in BR (revoked groups) can compute K from the header hdr and their decryption key dku. Using the key K, a user recovers M from C.

C. *Analysis*

ABBE can be constructed based on existing ciphertext policy attribute based broadcast encryption.[3] in a straight forward manner. In real broadcast applications, one has often to deal with obvious groups of users, because users are classified for instance by subscription package or subscription period. These groups are easily managed by an attribute-based broadcast encryption scheme, by simply using one attribute for each obvious group of users. Unfortunately ABBE suffer from large burden of key generation process.

III. PROPOSED ALGORITHM ABBE USING RSA

In above section discuss about the basic ABBE scheme. Advantage of ABBE is reduce the public key in the system. For broadcasting security is major issue with high speed data transfer. there is another well known algorithm is RSA. This algorithm support public key cryptography it is based on the presumed difficulty of factoring large prime integers.

There is a whole class of cryptographic/security systems which rely on what are called "trap-door functions". The idea is that they are functions which are generally easy to compute, but for which finding the *inverse* is very hard (here, "easy" and "hard" refer to how quickly we know how to do it), but such that if you have an extra piece of information, then finding the inverse is easy as well. Primes play a very important role in many such systems.

A. *Concept*

In proposed system define concept is merge the advantage of ABBE less number of public key and RSA highly secure using prime number. In this paper introduce one system which will work for one or two attributes. In this system we will take attribute as a prime number. Perform operation of RSA.

B. *Proposed algorithm*

ABBE using RSA.

Set up for propsed algorithm

In this algorithm we use k number of attribute into the the system. But here for convince this system will work for one or two attributes.

Take advantage of prime numbers. Here we take attribute as a prime number.

Give one prime number as a ideal number. i.e when user don't want to restrict by any attribute.

Here in this set up we have taken two set of attributes which are describe below:

L is a list of attributes.

L={3=technical,5=nontechnical,7=regional,9= ideal }

U= unique id to each user.

a) When user join a process for 1st time it needs to register itself with two attributes which are listed in L.
b) Each user gets an unique id during the registration process.

First sender will specify the access policy(w) for the intended receiver. Here we restrict this policy by only two attributes.

U1(w)={3,9}

N=p*q; p=3 and q=9;

$\Phi(n)=(p-1)(q-1)$

$d = e^{-1} \bmod \Phi(n)$. e is chosen by user.

$C= M^e \bmod n$;

Public key={e}

Private key={d,L}

In this proposed algorithm we change RSA public and private key as per necessary of system.

At the receiver side receives ciphertext 'C' and knows the public key. Now receiver select proper number of attributes then only receiver can calculate n and it can convert the formula $M=C^d \bmod n$ into intelligible form.

C. *Analysis*

As we have seen both the algorithm.in proposed algorithm take advantage of RSA and fulfill the requirement of ABBE. This algorithm provide excellent secuirty for data communicaion which is basic need for cryptography. main advantage of this algorithm is it reduce the burden of large key calculation of attribute based broadcast encryption.

IV CONCLUSION

Proposed algorithm effectively reduce the burden of calculation of keys for broadcasting at the sender and reciver side. Main advantage of this proposed system is to combine advantage of both the algorithms. It provides highly secure transmission using advantage of RSA and do not require explicitly specify list of decrypter for encryption process.

REFERENCES

[1] Zhinbin Zhou and Dijang Huang,Constructing " Efficient Attribute-Based Broadcast Encryption" publication I the IEEE INFOCOM 2010.
[2] David Lubicz, Thomas Sirvent. Attribute-Based Broadcast Encryption Scheme Made Efficient. Proceeding AFRICACRYPT'08 Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology Pages 325-342
[3] Ryo NOJIMA,Yuichi KAJI, Using" Trapdoor Permutations in a complete Subtree Method for Broadcast Encryption",IEICE TRANS,FUNDAMENTALS,VOL.E88-A,NO.2 February 2005.
[4] MU Ning-bo1(), HU Yu-pu1, OU Hai-wen2 "Broadcast encryption schemes based on RSA" www.sciencedirect.com/science/journal/10058885, February 2009, 16(1): 69–75
[5] Pascal Junod, Alexandre Karlov" An Efficient Public-KeyAttribute-Based Broadcast Encryption Scheme Allowing Arbitrary Access Policies"
[6] Yevgeniy Dodis, Nelly Fazio" Public Key Broadcast Encryption for Stateless Receivers" August 1, 2002
[7] http://x5.net/faqs/crypto/q1.html
[8] Cryptography and Network Security Principles and Practices, Fourth Edition, By William Stallings
[9] J. Bethencourt, A. Sahai and B. Waters.pp 321-334, 2007. "Ciphertext-Policy Attribute-Based Encryption".