Maintenance of Topology in Publish/Subscribe Systems

Sushilkumar N. Holambe
Persuing PhD at
Dr. B.A.M.U. Aurangabad

Ulhas B. Shinde, PhD
Dean
Faculty of Engg. & Technology.
Dr. B.A.M.U. Aurangabad

Shital S. Biradar
Persuing ME at College of Engg,
Osmanabad

ABSTRACT

In this paper we present a protocol for maintaining topology of single tree associated with numeric attributes. In content based publish/subscribe system it is very difficult to provide security to the events and subscriptions. The main concept here is to share data on any distributed systems. Here we provide idea of identity based encryption, provision to attempt authentication, confidentiality and scalability and it also provide pairing based cryptography to maintain security for the publisher and subscriber even if there is a loose coupling between publishers and subscribers.

General Terms

Security, Maintenance protocol for single attribute tree.

Keywords

Identity based encryption, Content based, Publish/Subscribe systems.

1. INTRODUCTION

As we are providing scalability for number of users, our traditional PKI (Public Key Infrastructure) is insufficient for a large number of subscribers, as each event need to be encrypted with individual public key. Here subscriber maintains credentials according to their subscriptions and publisher encrypt all the events with the help of credentials.

Credential is nothing but it is having two parts:

1) Capability of peer
2) Proof of its identity

We are using Identity Based Encryption (IBE) [1] [2] to ensure that 1) a particular subscriber can decrypt only if there is a match between credentials associated with event and key. 2) To allow subscriber to verify authenticity of received events by implementing maintenance protocol. This paper also provides two achievements 1) to use searchable encryption [8] method by using identity based encryption. 2) To implement multicredential routing in the system [6] [7].

This paper also provides-

Authentication: To avoid publications that are not eligible, only authorized publishers should able to publish events in System. Similarly subscribers should only receive those Messages to which they are authorized to subscribe [1].

Confidentiality: In a Broker-less environment, two points are important that the events are only visible to authorized Subscribers and also protected from modifications and subscriptions must be confidential [2].

Scalability: The secure content based publish/subscribe system should scale with number of subscribers in the system [2].

2. RELATED WORK

In content based publish subscribe systems there are two users

1) Publisher
2) Subscriber

And both do not trust on each other. In the system only valid events are allowed by authorized publishers. These events are encrypted by the publisher and spread over the network. After that only those subscribers can decrypt that event who was subscribed that event, because only valid subscribers can receive keys for the decryption of the events from the key server.

2.1 Identity based Encryption

In this cryptosystem, the secure communication between users is allowed without exchanging public key. Master public key is known to every user and key server maintains public and private keys. The communication is without using third party [1].

The advantage of using Identity Based Encryption is that less number of keys has to be managed by the key server. We can also create more than one copies of the key server over the network. Master Public key is used for the encryption by the sender. The master public key is nothing but it is an identity of the receiver to whom that publisher wants to send the message securely. After that receiver receives the master private key according to their identity from the key server and decrypt that message.

The process of Identity based encryption is as shown in following figure.

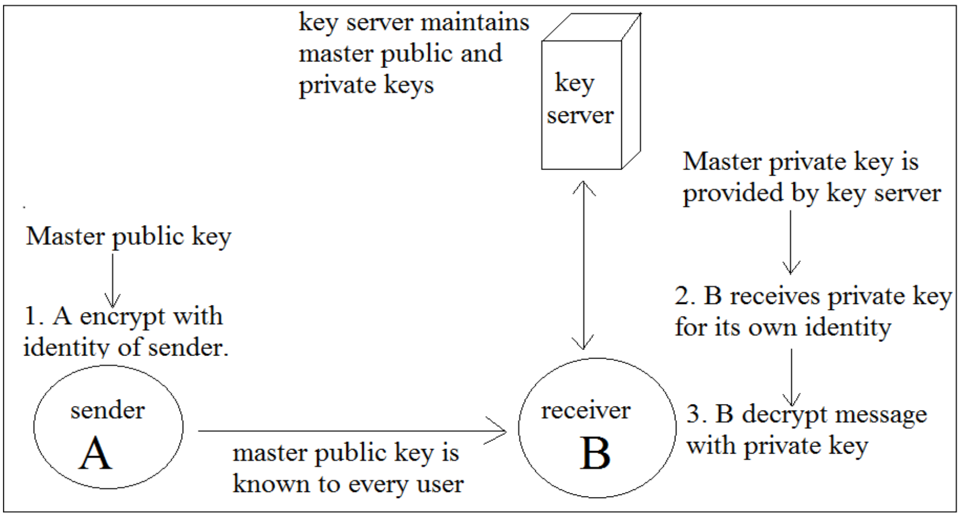
key server maintains master public and private keys
key server
Master private key is provided by key server
Master public key
1. A encrypt with identity of sender.
2. B receives private key for its own identity
sender
A
receiver
B
3. B decrypt message with private key
master public key is known to every user

Fig.1 Steps in Identity Based Encryption (IBE)

2.2 Publisher/Subscriber technique

Publisher/Subscriber technique is very simple. In that publisher spread messages over the network and Subscribers can receive those messages according to their subscription. Here, for the purpose of security publisher and subscriber provide credentials to the key server and receive keys according to the capabilities of credentials. Those keys can be used to encrypt, decrypt and sign messages in system that is authorization of credentials is done by key server.

Restriction is that publisher must have to encrypt messages and subscriber can decrypt only if they are having private keys. Subscribers receive private keys only for subscribed messages.

2.3 Content based publish/subscribe system

This system is used for the routing events from publisher to subscriber. An event is nothing but the combination of the attributes and associated values. We use advertisements of the events before the publishing set of events, to authenticate the publishers.

Message routing decisions are based on content of the message. Messages are only delivered to those points of communication which are “interested” communication end points[4].

2.4 Attacker Model

In our system we are having two users publishers and subscribers and attacker model is same as *honest but curious* [9] [10] model. Users of the system are honest but do not trust on any other user of the system.

However curious Subscribers are interested to see the content of those published messages to which they are not authorized. Similarly curious Publishers want to see the events that are published by other Publishers.

We are considering that there is a presence of secure channel for the transmission of keys from key server to the

Publisher and Subscriber. Transport layer security can be used for the realization of the secure channel such as transport layer security (TLS) or secure socket layer (SSL).

2.5 Identity Handling

Identity is very important because for providing large number of services and functionalities in the content based publish/ subscribe systems. IP addresses are used for the identification of the computers in its simplest form. IP addresses are used in combination with the Domain Name System (DNS) [7].

3. PROPOSED WORK

Here we are providing maintenance protocol in some easier form for maintaining topology. It is because to avoid the violation of the weak subscription confidentiality [2]. Here we are dealing with single tree having a numeric attribute. Each subscriber is interested in single credential.

In this tree subscribers are connected according to the containment relationship between their credentials. By using this protocol, the decision is taken about new subscriber. According to that decision new subscriber Sc is connected to the proper node in tree and at the same time containment relationship is preserved. For example suppose subscriber is having credential 11, then that subscriber can connect to subscribers with credentials 1 or 11.

Protocol is as shown in Algorithm 1.

Algorithm 1. Maintenance protocol at peer Sc

```
After receiving event (CR of Sn from Sp) do
 if there is match between credentials of Sn and Sc
    Decrypt the event
       if decryption is successful then
          if degree of Sc is available then
            Connect Sn to Sc
          else
          CR is forwarded to childs and parent excluding Sp
 if decryption is not successful then
    if Sp is parent then
       Sp send its own CR to Sn
    else
       Forward to parent
```

CR- Connection Request
Sn - New Subscriber
Sp - parent
Sc- child

As per algorithm, decryption of the event is possible only if there is a match between credentials. If the parent cannot have more children then a child Sc receives CR (Connection request of new subscriber Sn) from the parent Sp. If credential of Sn is coarser than credential of Sc, then it tries to exchange its position with Sn by sending CR (Connection Request).

If Sc (child whose parent Sp has got connection request from Sn) cannot connect or swap with Sn (new subscriber) then there is no containment relationship between credentials of Sc and Sn. In such a case for connecting a new subscriber to the tree parent should disconnect one of its children.

In content based publish subscribe systems there is an interaction between publisher and subscriber. The keys are generated according to the credentials of the publishers and subscribers and these are provided to the publisher and subscriber.

At the time of publishing events, publisher at first encrypt the event using public key and then it is disseminated over the network. Then receivers receive that event and try to encrypt that message. It can be encrypted if and only if there is a match between credentials of event with credential of subscriber. Because subscriber has only the private key (for decryption) related to credentials they are having.

The data sharing between publishers and subscribers can take place by various techniques:

3.1 Numerals Attribute

Here data is provided in the form of the spaces. The space is divided into two halves recursively at each time. These divided subspaces provide limitation between subscribers and publishers according to the credentials. Divided subspaces are represented by 0 and 1 then after the division of the first part it is represented as 00 and 01. When space is divided into two halves represented by 00 into two halves, then these two halves are represented as 000 and 001. There is a containment relationship between spaces. For example 0100 is an event enclosed by five subspaces 0100, 010, 01, 0 and ε.

This process can be graphically demonstrated by using decomposition binary tree [2]. In each next level each space of previous level is divided in two halves. As shown in following figure.

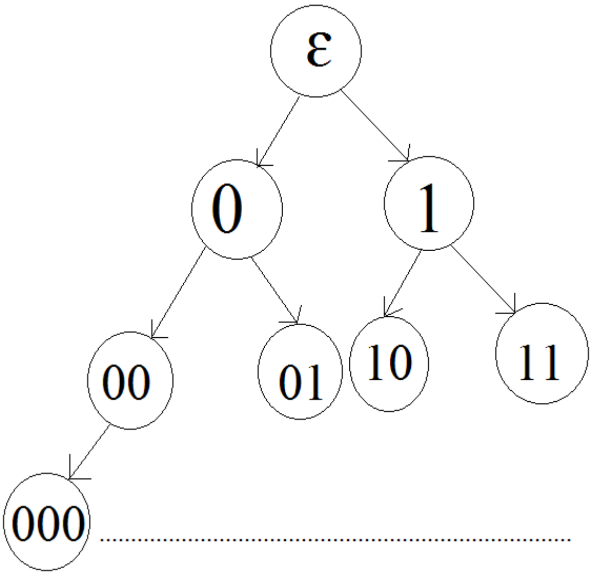

Fig.2 decomposition Binary tree.

3.2 Alpha string Attribute

Credentials for the string attributes is performed by using the process of prefixing the node. Here tree is generated with the preservation of prefix matching technique called as trie.

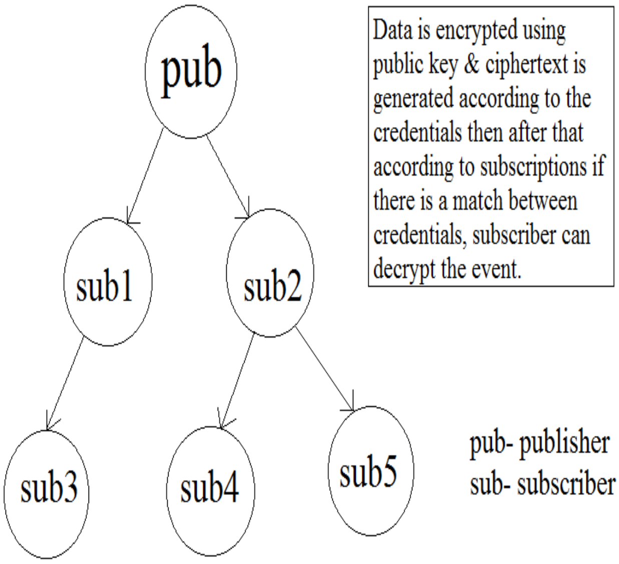
pub
sub1
sub2
sub3
sub4
sub5
Data is encrypted using public key & ciphertext is generated according to the credentials then after that according to subscriptions if there is a match between credentials, subscriber can decrypt the event.
pub- publisher
sub- subscriber

Fig.3 Data Sharing between publisher and subscriber.

This figure shows that while maintening tree there is necessity of maintenance protocol.

3.3 Range Attribute

In case of this attribute, separated credentials are provided to a subscriber along with the keys for each attribute. In the network a specific range is described. Data or event is sent in the specific range of the subscribers.

4. APPLICATIONS

Security is provided by using this model in publish subscribe system, therefore publishers and subscribers can communicate securely over the network.

By using the topology maintenance algorithm all subscribers are connected in tree according to containment relationship so it becomes easy to manage large number of subscribers.

This system also provides authentication and confidentiality. It provides efficient key management as compare to the Public Key Infrastructure (PKI).

5. CONCLUSION

Scalability is provided by increasing total number of subscribers. Subscribers are maintained using topology maintenance protocol by forming a tree of attributes. We have adopted IBE (Identity Based Encryption) technique for the conformation of decryption of cipher text and it takes place only when there is a match between credentials of event and its private keys. This also provides authentication and confidentiality in a broker-less content based public subscribe system . Hence users (publishers and subscribers) can securely use Publish/subscribe system.

6. REFERENCES

[1] D. Boneh and M.K. Franklin, "*Identity-Based Encryption from theWeil Pairing*," Proc. Int'l Cryptology Conf. Advances in Cryptology, 2011.

[2] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel" *Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption*" IEEE transactions on parallel and distributed systems, vol. 25, no. 2, February 2014.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "*Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*,"Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2010.

[4] Sean O, Mealia and Adam J.Elbirt "*Enhancing the Performance of Symmetric –key cryptography via Instruction set instruction*" IEEE transactions on very large scale integeration vol.18 no.11 November 2011.

[5] Ming li,Shucheng Yu.Yao Zheng,Kui Reng, Weiging Lou "*Scalable and secure sharing of personal data in cloud computing using attribute-based encryption*"IEEE transaction on parallel and distributed computing 2013.

[6] Legathaux Martins and Sergio Duarte "*Routing Algorithms for Content based publish/subscribe system*"IEEE commm-unications and tutorials first quarter 2010.

[7] Karl aberer, Aniwitaman datta and Manfred Hauswirth "*Efficient Self Contained Handling of Identity in Peer to Peer System*"IEEE transaction on know- ledge and data engineering, 2004.

[8] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT), 2004.

[9] A. Shikfa, M. O ¨ nen, and R. Molva, "Privacy-Preserving Content- Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.

[10] M. Srivatsa, L. Liu, and A. Iyengar, "EventGuard: A System Architecture for Securing Publish-Subscribe Networks," ACM Trans. Computer Systems, vol. 29, article 10, 2011.