International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 2, Issue 8, August 2015

Securing Publisher Subscriber System Using Layered Encryption

[1]Reethalakshmi M D,[2]Dr. Sunitha N R
[1][2]Dept. of CSE, SIT, Tumkur, India
[1]reethumd1@gmail.com,[2]nrsunithasit@gmail.com

Abstract: **Providing security mechanism such as authentication and confidentiality is a challenging issue in a publisher subscriber system due to loose coupling of publisher and subscriber. In this paper we present an approach to provide authentication, confidentiality in the publisher subscriber system. The authentication of publisher and subscriber as well as confidentiality of events is ensured by the use of pairing-based cryptographic mechanism such as cipher text policy attribute based encryption. The novelty of this work is that we use the layered encryption to increase the security with less overhead of key management. Here we have considered tree structure to maintain the subscriber requirements and each level in tree is considered as zone and different security level is provided for each zone.**

Keywords— **Layered encryption; Identity based encryption; Security**

I. INTRODUCTION

The Publisher and Subscriber (pub/sub) system is a well-established information exchange paradigm that allows any number of publishers to communicate with any number of subscribers in offline mode and anonymously. The Publisher is the one who uploads the articles. The subscriber is the one who can download the articles. The subscriber subscribes by expressing his interest in the articles by paying the subscription fees. The published article should be routed to specific subscriber.

There are two types of publisher subscriber systems 1. Topic based publisher subscriber system, 2. Content based publisher subscriber system. In a Topic based publisher subscriber system the Subscribers will get all messages published on the topics to which they have subscribed for. In a Content-based Pub/sub system, messages are only send to a subscriber content of those messages match conditions defined by the subscriber.

Because publisher and subscriber are unknown to each other and as they also need to exchange information irrespective of their location, security is one of the most important issues we need to consider in this pub/sub system.

The security parameters that are generally considered are Authentication, Authorization, Confidentiality, and Scalability. Authentication is a procedure of verifying the identity of the user. This is done in the login phase by using user id and password. Authorization is a procedure of checking whether the user has access rights to the system and this process is done after authentication. Confidentiality is the procedure of avoiding sensitive information from reaching the wrong people. Here scalability refers to availability of the system to any number of users without compromising on the security of the system.

The access control in the context of publisher and subscriber means that only authorized and authenticated publisher need to publish event in the pub/sub system. Similarly, the authenticated subscriber should receive the information from the pub/sub system.

To provide the security in the publisher subscriber system the most common method is to use broker in between publisher and subscriber, where broker should responsible to send the published article to specific subscriber. In this type of system there is no security provided from intermediary broker to sensitive data as broker himself can see all the data before routing it to specific subscriber. Also, there is a limit on the number of users that broker can handle due to various constraints like area to which the broker belongs, language of the articles, investment done by the broker and so on. And this affects the system scalability.

There are also broker-less publisher subscriber systems where there is no broker involved in between publisher and subscriber. To route information to specific subscriber there is a key server which is responsible for routing and key generation for both publisher and subscriber. It also groups the subscriber of similar subscription and maintains the subscribers in a predefined structure.

II. RELATED RESEARCH

In [1] [2] the authors rely on broker to provide security for published articles against malicious users. The Publishers and subscribers are unknown to each other. They are connected by brokers. When articles are published by publisher, broker is responsible to route that article to particular subscriber. Here the author's provide security based on filters. The filter is specified by the subscriber. Attribute based encryption [3] and an encrypted search scheme is used to archive security. The system scalability is limited due to the broker's limitation.

In [4] [5] [6] the authors use semi trusted brokers, where broker is not a completely trusted party. The authors allow the broker to work on encoded data to route it to a specific subscriber from publisher. Here the key exchange between publisher and subscriber is necessary before the start of the transaction which is an overhead. As the broker needs to work on encoded data there is additional overhead of system resources.

In [7] the authors remove the concept of broker and introduce broker less publish subscribe system. Instead of broker they use key server to interconnect publisher and subscriber. Key server maintains the subscriber in containment relationship and route the published articles to specific subscriber and it generates the key for publisher and subscriber when they request for keys. So, there is no need of key exchange between publisher and subscriber before start of the transaction. Authors use identity based encryption [8] [9] to create keys instead of public key encryption. Because of using identity based encryption, overhead of key management is reduced in key server. Here the rekeying concept is used. In rekeying concept the new keys are generated after some specified period. This increases the load on the key server.

In [10] the authors work on broker less publisher subscriber system. They have removed the concept of rekeying. To generate the keys, the authors use Attribute based encryption which is basically based on identity based encryption. They use the concept called credentials. Both key and published article are labeled with the credential. If there is a match between the credential of key and credential of published article then only a subscriber can decrypt the massage.

The Authors of the paper [11] have discussed about the layered encryption. Layered encryption provides ability to disclose different parts of data to different parties. This paper addresses the problem of how one user can perform selective delivery of data to different users. In this layered encryption the data can be encrypted with multiple encryption algorithms or it may use same algorithm multiple times to generate multiple keys. Layered encryption also performs selective decryption i.e. the end node in a connection decrypts the entire packet and any intermediate node will be given keys to decrypt only certain parts of a packet.

In [12] the authors of the paper have introduced the layered encryption method to provide security to data in the critical infrastructure. The attacks considered by authors in communication links are eavesdropping attack and man in middle attack. Based on the required security level, the users are grouped into zones. A zone is able to get all the data from zones with lower or the same security level. Here hash chain technology is used for key management and key distribution. The keys are stored in the hash chain and the key is selected from generated hash chain based on the security level. The key management and key distribution is the main challenging issue in this work.

Our work is built on the basis of [10], we use the Cipher text policy attribute based encryption to generate the keys and the novelty of our work is that by using layered encryption method the subscribers who are put in different zones access the published articles securely.

The remainder of the paper goes like this. In third Section we discuss about existing broker less publisher subscriber system. In the fourth section we discuss our proposed layered encryption publisher subscriber system. And lastly in fifth section we conclude the paper.

III. EXISTING SYSTEM

In the existing system, the authors have worked to provide basic security such as confidentiality, scalability, and authentication in content based broker-less publisher subscriber system. Because of the direct interconnection of publishers and subscribers, the authentication of publishers and subscribers is difficult to achieve. Likewise, confidentiality of events and subscriber subscriptions incompatible with content-based routing.

The existing system implementation is based on the identity based encryption instead of public key encryption, so they gain the advantages of identity based encryption because in public key encryption the key server need to maintain public and private key pair of every user which increases system management overhead. By using the identity based encryption the key management overhead is avoided.

In the existing system approach subscribers keeps credentials according to their subscriptions. Private keys assigned to the subscribers are labeled with the credentials. A publisher associates each encrypted event with a set of credentials. They adopt identity-based

Encryption mechanism 1) to make sure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the published article and the key and 2) to permit subscribers to check the authenticity of received events.

To provide security mechanisms in publish subscriber system the existing system uses the principles of identity based encryption and uses other identity based encryption schemes such as attribute based encryption.

Credentials express the capability of publishers and subscribers. Credentials are made up of two parts 1.Binary digit which represents the subscriber subscription and publisher advertisement, 2.Id which represents the subscriber identity. The credentials are created by dividing the event space, event space contain 'n' of distinct attributes i.e. topics and each divided space is represented by binary digits. The division of event space is performed hierarchically as shown is Fig1.

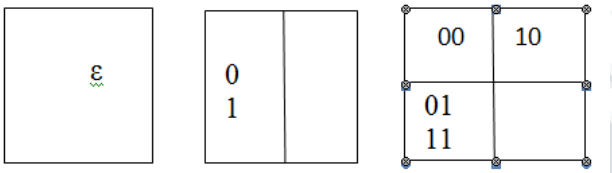

Fig. 1. Hierarchical decomposition of event space

In the existing approach, the publishers and subscribers involved directly with the key server. They provide credentials to key server and in turn they receive the keys which are used to encrypt and decrypt the messages and also to sign and verify as shown in Fig.2

When new subscriber wants to join the tree, they send the connection request (CR) to any node in the subscriber network. The connection request contains the subscriber subscription. The node which receives the CR will compare the received credential with its own, if credential matches then it accepts new node as its child else it forwards to its parent .

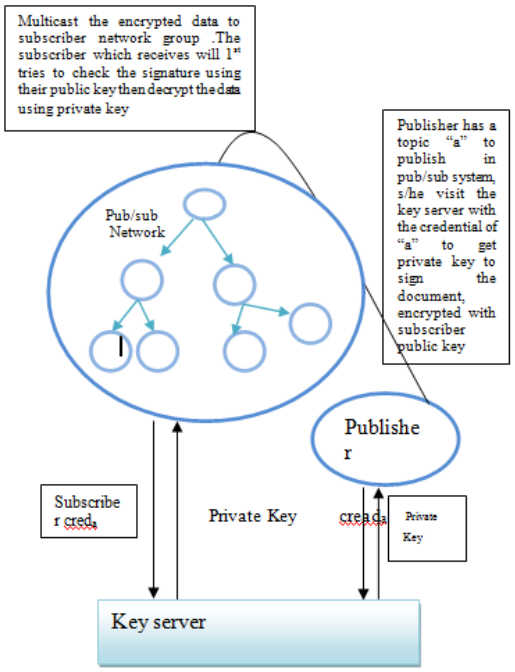

Fig. 2. Overall working procedure of existing system

In the existing system the sender needs to perform two actions and receiver also needs to perform two actions. Sender action is to encrypt the sending data and sign on the encryption data. Sender uses public key of all receiver to encrypt the data and sign the encrypted data with the private key and then s/he multicast the data to the pub/sub network. The subscriber who receives the signed encrypted data will first verify that whether the received data is sent by authorized publisher by verifying the signature using the public key of publisher. If it is sent by authorized publisher then it tries to decrypt the data by using private key. If it fails to decrypt, it forwards it to its parent node.

For key generation the ciphertext policy attribute based encryption algorithm is used which is based on the identity based encryption .In our proposed method we use the same Cpabe algorithm to take the advantages of Cpabe.

In this method, all subscribers should have different keys even though the subscriber subscribes for the same topics. Though this increases the security, the overhead of the key management in the key server increase. Therefore we propose a new scheme to reduce the overhead in the key server.

IV.

IV. PROPOSED SYSTEM

In this section we will discuss how the layered encryption [11][12] method applied to existing system which provide more security with less key management overhead. In our proposed system we are allowing publisher to publish the events in bulk which means allowing publisher to publish multiple events at a time. Each event may be subscribed by different subscribers.

As we know that the subscribers are maintained in the containment relationship i.e. using tree structure, the subscribers are maintained such that the coarse subscribers are placed near the root and fine subscribers are the child of the coarse subscribers. Fine subscribers forward the information to coarse subscribers i.e. bottom up approach is used to forward the published article. The same thing is shown in Fig.3.

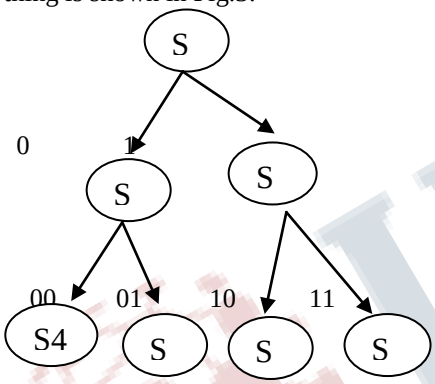

Fig. 3. Binary tree which shows Subscriber containment relationship

As we know credentials are represented by binary digits and each binary digit represents different topics. When publisher publishes the event, any leaf node in the tree will receive the published event and tries to decrypt it. If it fails, it forwards the event to its parents.

In our proposed system we have considered tree level as zone .To each zone we are providing different security level. As shown in Fig.4 the tree levels are divided into zones such that the nodes which belong to level 1 become zone 1 nodes and the node which are in level 2 become zone 2 nodes and so on. We are using bottom up approach to route the published article to a specific subscriber and we are placing coarse subscriber near the root and fine subscribers are children of coarse subscriber.

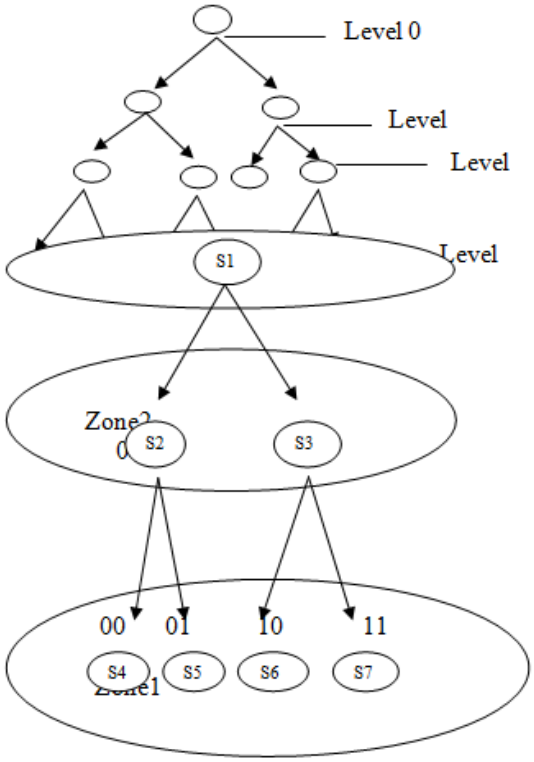

Fig. 4: Levels and zones in the binary tree

Layer encryption is applied to every zone and in each zone the security level is different. The number of keys used to encrypt and decrypt increases with each zone.

Event space (ε) Ex (computer science dept.)

(a)

0 (CSE)	1 (CNE)

(b)

00(ada, dbms, os,nm)	10(ADE,Cn,CSP,Np)
01(Ns, SE, Aka, Cg)	11(wsn,wmn,pe,on)

(c)

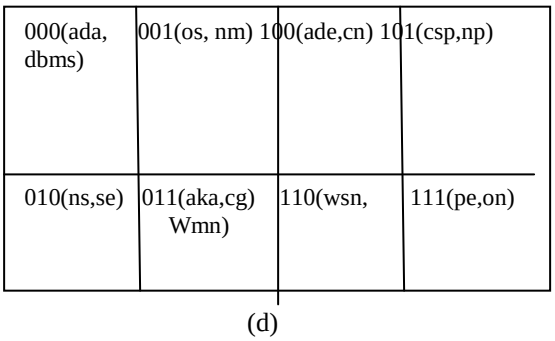

Fig. 5 . Example of creation of credential by dividing the event space hierarchically

When publisher publishes the event 000, it can be decrypted by the subscriber who subscribed for 0, 00,000. In the example, 000 represents the "ada" and "dbms" topics, and same topic is subscribed by 00 and 0 subscriber. If publisher publishes only topics which is represented by '0' credential then all the topics can be decrypted by 0 credential subscribers and the other subscribers i.e., '01' '00' should be able to decrypt the select part of the published data.

Layered encryption mechanism is based on hash chain technology. A hash function, says H, can be applied on a publishing article repeatedly or else we can use different hash functions for different zones until all the levels of the tree are reached. To decrypt the data the user need to apply hash functions of respective zone.

For example if publisher wants to publish the event say 000 then the publisher needs to encrypt the data 0,00,000 with the key generated by 'H1','H2'and'H3' hash functions respectively. To decrypt the data, the Zone1 user should apply 'H1' hash function, Zone2 user 'H2' hash function and Zone3 user 'H3' hash function to generate the decryption key. So the zone1, zone2, zone3 user will get 0, 00 and 000 respectively.

In the Layered encryption the disadvantage is overhead of key management and distribution. In our proposed system we use key server to maintain keys and distribute the keys to subscribers and publishers. We don't use any broker in this operation which makes the system scalable to any number of users.

To generate key we can use multiple key generation algorithms or else by using same algorithm we can generate multiple keys and those keys are used to encrypt and decrypt the events.

In our proposed system we take advantage of ciphertext policy attribute based encryption (CPABE), the keys are generated by using CPABE algorithm. CPABE allows publisher to encrypt the data and sign on the encrypted data and allows subscriber to make sure that the received data is sent by authorized publisher and then it decrypts the data. To get the key, both publisher and subscriber should visit the key server with credentials. Based on the credentials, key server will provide the required key. As the subscribers are allowed only to read the published article, we provide same keys for all the subscribers who have subscribed for same topics. Therefore the number of keys in the key server is reduced in our scheme compared to all other previous work.

CONCLUSION

In this paper, we have introduced a new approach to provide authentication, confidentiality and scalability to Publisher subscriber system. The use of the layered encryption approach has made the system scalable in terms of number of subscribers and publishers in the system. The number of keys maintained by key server is also reduced. In particular, we have developed mechanisms to assign credentials to publishers and subscribers according to their subscriptions and advertisements. We have adopted identity based Encryption technique. We use the layered based encryption which is based on the hash technology to increase the security in publisher subscriber system with less over head of key management.

REFERENCES

[1] Mihaela Ion1, Giovanni Russello, and Bruno Crispo, " Supporting Publication and Subscription Confidentiality in Pub/Sub Networks" , Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm),2010.

[2] J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch, "Access Control in Publish/Subscribe Systems,"Second ACM Int'l Conf. Distributed Event-Based Systems (DEBS), 2008.

[3] Susan Hohenberger and Brent Waters," Attribute-Based Encryption with Fast Decryption"2008.

[4] S. Choi, G. Ghinita, and E. Bertino, "A Privacy-Enhancing Content-Based Publish/Subscribe System Using Scalar Product Preserving Transformations," 21st Int'l Conf. Database and Expert Systems Applications: Part I, 2010.

[5] P. Pietzuch, "Hermes: A Scalable Event-Based Middleware," PhD dissertation, Univ. of Cambridge, Feb. 2004.

[6] A. Shikfa, M. O nen, and R. Molva, "Privacy-Preserving Content- Based Publish/Subscribe Networks,"

Emerging Challenges for Security, Privacy and Trust.
[7] M.A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, "Providing Basic Security Mechanisms in Broker-Less Publish/Subscribe Systems," Proc. ACM Fourth Int'l Conf. Distributed Event- Based Systems (DEBS), 2010.
[8] Brent Waters, Amit Sahai ,"Fuzzy Identity-Based Encryption ".
[9] Dan Boneh_ Matthew Frankliny "Identity-Based Encryption from the Weil Pairing" 2001.
[10] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel ,"Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption", transactions on parallel and distributed systems, vol. 25, no. 2, February 2014 .
[11] Manish Karir John S. Baras," LES: Layered Encryption Security".
[12] Huayang Cao, Peidong Zhu, and Xicheng Lu, , China Andrei Gurtov, Helsinki,"A Layered Encryption Mechanism for Networked Critical Infrastructures", IEEE Network January/February 2013.