International Journal of Engineering Research and General Science Volume 3, Issue 6, November-December, 2015
ISSN 2091-2730

Provision of Credential Based Security in broker-less publish/Subscribe System

Shital S. Biradar , Sushilkumar N. Holambe

pursuing ME at College of Engg,Osmanabad. Email- Sbiradar999@gmail.com. , contact no- 9422033718.

Abstract— Publish/Subscribe system is a system used for sharing data between the users of the system. Here we are considering content based Publish/Subscribe [9] System. In Content based Publish/Subscribe [9] System messages are routed according to the content of the message. This System can also be called as messaging System. This paper presents an approach to provide security in the publish/subscribe system by using the credentials of the user and it uses broker-less network for the dissemination of the message. Here we are providing identity based encryption [1] for the security purpose and message can be decrypted by only those subscribers who are having credentials with the message. In this system users are divided into two classes .The user can be Publisher of the system (who is providing information to the system in the form of messages or events) and second is subscriber (who is consuming information provided by the publisher according to their subscriptions). This paper presents mechanism for providing authentication, Confidentiality and Scalability.

Keywords— content based, security, publish/subscribe, identity based encryption, confidentiality, broker-less, peer-to-peer.

INTRODUCTION

In Publish/Subscribe system there is a loose coupling between two types of users that is publishers and subscribers. Therefore this system has been very popular and also these can be used with many distributed applications due to the loose coupling. In the existing system there is a use of broker architecture. In that message is passed or forwarded towards the subscribers by the publishers through the broker. It means every application is connected to the central broker and there is communication with the help of intermediate broker for each communication, therefore there is no authentication and confidentiality. To avoid such problems in a broker-less content based publish subscribe system [2]; we are using Pairing based cryptography mechanism.

Publisher publishes events/messages over the network, and subscriber subscribes interested messages. These published messages can be decrypted by subscribers who are having match between credentials of subscriptions and published messages or events.

To provide security hear we are supporting basic security mechanisms such as confidentiality and access control [11]. In case of confidentiality it requires that the content of message should not be disclosed to the routing infrastructure and subscribers should get messages off all interested subscriptions without disclosing its subscription to the system. In case of access control ,It require only authenticated publishers are allowed to publish the message in the network and only those published messages are provided only to the authorized subscribers.

Our traditional Public key Infrastructure (PKI) will not maintain loose coupling between publishers and subscribers so here we are using Identity based mechanism for encryption. In this system all subscribers maintain credentials for their relevant subscriptions and specific private key is provided to the subscribers by the key server depending on the credential. publisher also maintain credential with the encrypted messages and that private key can decrypt only that cipher text whenever there is a match between credential of the subscriptions and credential of the message event.

LITERATURE SURVEY

The Publisher/Subscriber communication technique has become very popular because of its natural loose coupling between publishers and subscribers related to the time, space and synchronization. Publisher disseminate information into the publish/subscribe system, and subscribers can receive that published information by making the interested subscriptions. Published information / messages / events are routed over the network and provided to the relevant subscriber. Publisher having no any knowledge about the group of subscribers who are subscribing their events or messages, and subscribers are also unknown about the publishers. This system is useful for large scale distributed applications such as stock exchange prize information, news feed, traffic control, environmental monitoring etc.

It is very important to provide security supports such as access control [11] and confidentiality. It is the requirement of every user of the Content based Publish/Subscribe system [9]. So there is a requirement to route the event /messages without knowing each

other (publishers and subscribers) for the security purpose. Existing mechanism for the secure publish/subscribe system [10] depend only on the traditional broker network. By using such traditional mechanism it is very difficult to achieve fine grained access control and scalability. This paper presents new approach to provide confidentiality and authentication in publish/subscribe system with broker-less infrastructure.

METHODOLOGY

In content based publish/subscribe system [9], for the routing of events from the publishers to the specific subscriber we are considering event space. It is denoted by Ω and consist of ordered set of n attributes(Ai): Ω={A1,A2,A3,……..,An} . Every attribute is having unique name, its data type and its domain. Data type can be any one of the following types: integer, floating point and character strings. The domain is nothing but the range of attribute values bounded by two values that is lower and upper value.

A subscription function f is nothing but the equation that contains predicates combined with and operator that is,

f = {p1^p2^…..^pj}

p1,p2,….,pj – are the predicates.

Predicate is nothing but the combination of the three items that is attribute A, operator (op) and value. Predicate pi can be denoted as (Ai, opi, vi). Operators consist of equality and range operations for the numeric attributes and prefix or suffix for the string attributes. Events include attributes and its related values. The event is said to be matched with the subscription f is nothing but the value of attribute in the event satisfy the constraints provided by subscriptions.

Here we are using attribute base d encryption [3] [5], so for our implementation we require that at first we have to create credentials as this can be done in following way.

1. Numeric attributes-

   Here we are considering event space as a data, and each time this space is divided into two halves. These two halves are indicated as 0 and 1. Then first half part is again divided into two halves and it is denoted as 00 and 01. Second half part after division is denoted as 10 and 11. For example consider two attributes in terms of space means it is two dimensional space and its division is as follows.

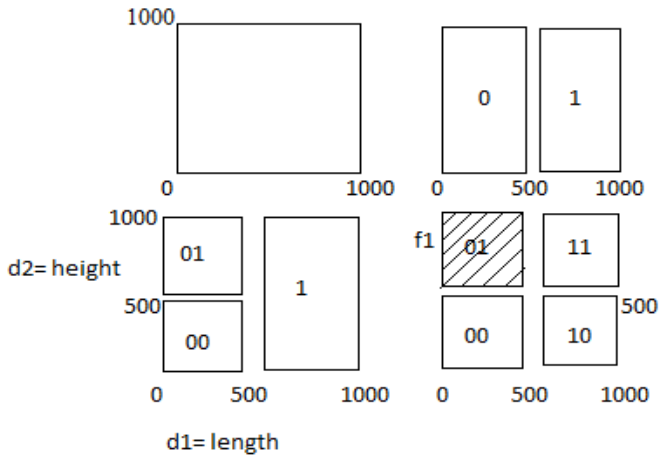


Fig1. Numeric attributes

Function f1={ length = [0,500], height = [500,1000] }

2. String attributes-

   In this technique we are creating credentials for string operation such as prefix matching can be generated using a trie. Trie is like a tree in which each node is labeled with a string. Each node is considered as a prefix string that is common to all its descendants. For example operation prefix matching tree is generated as,

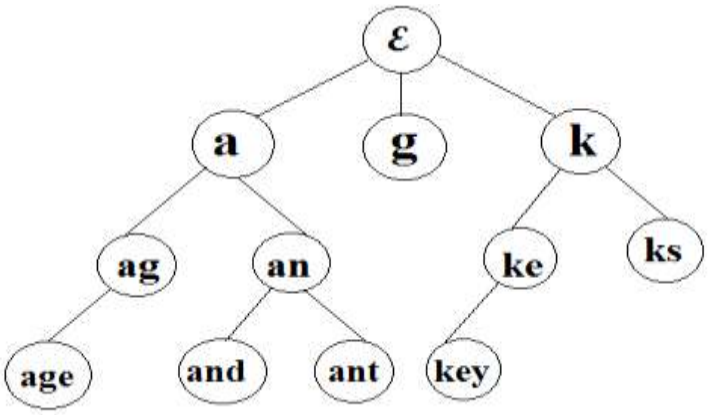


Fig2 . Prefix matching

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

Here with the help of Identity based encryption [1] over the broker-less infrastructure, we are going to provide scalability, authentication and confidentiality.
These security issues can be implemented by creating four modules in our project, these are as follows.

I. Content Based Publish/Subscribe module-

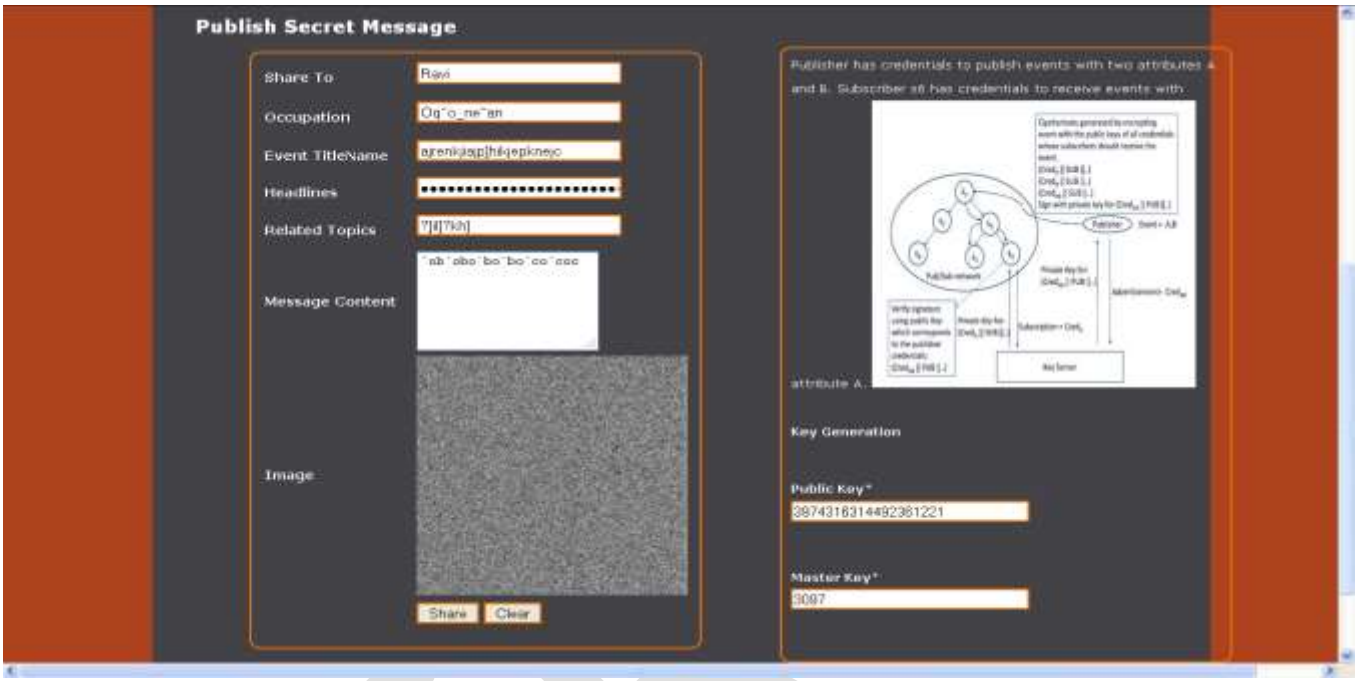
Publishers and subscribers participate as peers in the overlay structure for the maintenance. For the routing of the events from publisher to the specific subscriber we are using content based publish/subscribe system [9]. In this system event is routed according to the content of event. The publisher must be authenticated and this is done by the use of advertisements in which publisher announces set of the events which he wants to publish.

II. Identity based Encryption module-

In this project we are using Identity based encryption [1] and it is implemented in this module. Publisher and Subscriber communicate with the key server. They provide credentials to the key server and then receive keys according to their credentials.
Credential is nothing but it is having two parts.
I) Capability of peer

II) Proof of its identity.

Event is encrypted with identity of the receiver. Identity [7] is nothing but the public key and there is no need to transfer the public keys. Private keys are used to decrypt the encrypted event and it is done only if the credentials of the event and the key are same. That is the credential becomes authorized by the key server. Here cipher text is also labeled with credentials. For each authorized credential private keys are maintained by the publishers and subscribers. Here we are using searchable encryption [8] for the routing of the event since our system is content based publish/subscribe system.



III. Key generation for publisher/Subscriber module-

Publisher keys:

Before publishing events over the content based publish/subscribe system, a publisher has to communicate with key server. Publisher passes credentials for each attribute in its events of advertisement to the key server.

If publisher is authenticated then he can publish events according to the credentials, and that events are encrypted by using the private keys generated by the key server [4]. Key server generates separate private key for each credential. Public key for a publisher for credi,j is generated as,

$Pui,j := (Credi,j \| Ai \| PUB)$

PUB is nothing but the identity of publisher. Credi,j is notation of credential j of attribute Ai.

Subscriber keys:

In the same manner, before receiving the event , subscriber communicate with the key server and only those private keys are received by them which are having matching credentials with the subscriptions of the subscribers. Credentials are associated with each attribute A. in case of subscriber Public key is given as,

$Pui,j := (Credi,j \| Ai \| SUB)$

SUB is nothing but the identity of subscriber.

In our implementation private keys for publishers and subscribers are generated by using advanced encryption standards (AES) [12]. It is described in following sections.

IV. Secure overlay maintenance module-

In this module we are implementing secure overlay maintenance protocol is used for maintaining tree of subscribers. In this tree subscribers are connected to each other according to their containment relationship. It means that subscriber is connected to subscriber having coarser credentials. In other words subscriber generates cipher text by using private keys and cipher text is attached with the connection request(CR) and that request is passed to the random node in the tree, that node is nothing but subscriber(peer). A connection is allowed only if the peer can decrypt any of the cipher text using its private keys.

Algorithm for secure overlay maintenance protocol-

1. on receiving connection request of new subscriber (Sn) from any subscriber (Sp)do
2. If(credential of Sn == credential of Sp)
3. Event is decrypted.
4. If decrypt (CR) is successful
5. If degree is available
6. Then establish a connection
7. Else CR is forwarded to other node excepting Sp.
8. If decryption is failed then
9. If Sp is parent then
10. Sn receives CR from Sp
11. Else
12. Move CR towards parent
13. If any node is not suitable for establishing connection with Sn.
14. Then there is no containment relationship.

METHODS FOR EVENT DISSEMINATION

Here we are describing two methods for event dissemination.

i) One-hop flooding-
In this method parent forward each successfully decrypted event to all child assuming that they have same credentials. All children also forward each successfully decrypted event to their children and so on. In this method child may receive false positives because child may have finer credentials than its parent.

ii) Multicredential routing-

In this method there are no false positives. It is done by restricting parents to forward events to all nodes on each attribute tree. Events are forwarded only to the child who is having matching credentials with the parent.

ADVANCED ENCRYPTION STANDARDS

In this project, we are using AES algorithm [12] [4] for the key generation. It is a block cipher intended to replace DES. It uses 128-bit block size and a key size of 128,192 or 256 bits. AES structure consists of full round having 4 functions: byte substitution, permutation, arithmetic operations over a finite field and Xor with a key. Depending on number of rounds length of the key is determined as follows.

No. of rounds	Key length (bytes)
10	16
12	24
14	32

It is a symmetric key encryption standard.

RESULTS AND DISSCUSION

In this project, we are considering security of the publish/subscribe system. As we are using Identity based encryption [1], so this content based publish/subscribe system became very powerful because every publisher and subscriber is authenticated. Before publishing events publisher have to login into the system using its own id and password. Only that publisher can login into the system who is already registered, so illegal publisher cannot publish vulnerable events over the network.

To subscribe event, subscriber also have to login into the system and then they can get the message or event, if it is allowed by the publisher. If subscriber is eligible for accessing the message, then key is provided for the decryption of the message because message is in encrypted form. Message can be translated into the plaintext if that key is correct. The correct key is provided only if subscriber is authorized. Therefore as compared to simple content based publish/subscribe system this project implements secure content based publish subscribe [9] system. Here with the encryption message is routed [6] properly because we are using searchable encryption [8]. In this project some delay occurs due to the tasks like encryption, decryption and for the connection of new subscriber at proper position in the attribute tree. The delay is normally 150 to 200 milliseconds as compared to the system that is not having security mechanism. So our performance is also better and it is with the security, it doesn't take very long time to do security related tasks. So this project is very useful for the secure event dissemination over the network. System is also having scalability that is any number of subscribers and publishers can use the system.

CONCLUSION

This paper gives a new approach to provide security in content based publish/subscribe system. Our system became secure as we are using identity based encryption to provide security and also using advanced encryption standards (AES) algorithm [12] for the key generation. Event can be decrypted by the subscriber only if there is a match of credential.

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.

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

[12] F.P. Miller, A.F. Vandome, and J. McBrewster, Advanced Encryption Standard. Alpha Press, 2009.