IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 101-103
www.iosrjournals.org

Enhancing Security Of Publish/Subscribe System Using Identity Based Encryption Model

Shital S. Biradar[1], Prof. Sushilkumar N. Holambe[2]
[1,2] *(CSE, T.P.C.T's College of Engg, Osmanabad, India)*

Abstract: *In a content based publish subscribe system providing security related to the events or messages and subscriptions is very difficult. This paper presents approach to provide security in a Broker-less Publish/Subscribe system by using identity based encryption (IBE) model. The main concept of such systems is to share the secured data on any distributed systems. Identification is very important mechanism in content based publish/subscribe system. Here we provide 1) idea of identity base encryption (IBE) 2) Provision of security in the content based publish/subscribe system . 3) Creation of public and private keys for the users of the systems that is for the publishers and subscribers.*
Keywords: *content based, Identity Based Encryption, publish/subscribe system, security*

I. Introduction

Nowadays Publish/Subscribe system [7] is very commonly used and it is very popular model. We are using content based publish/Subscribe system [7]. In this system messages or events are routed according to the content of the message or event, as it is indicated by its name that is nothing but Content based Publish/Subscribe system [7] [5].

Publish/Subscribe systems contain two types of users:

i) Publisher : The user who publishes the events or messages over the network.
ii) Subscriber: The user who subscribe events or messages according to their interest.

In such systems publisher provide information into the publish/subscribe system [7]. Subscriber subscribes their interested messages or events and then after that particular subscribed message or event is forwarded towards the subscriber without knowing each other. This paper presents a novel approach that enhances the capability of the system in case scalability. Here we are using identity based encryption [1] to enhance security of the system.

II. Related Work

Existing system uses the concept of encryption for the security purpose. At the time of using encryption the private and public keys must be maintained for each user of the system. This system encrypts messages and then they are routed over the network [5]. When message is received by the subscriber then it is decrypted by using related key. This is the overall mechanism used in existing system.

As our system is content based publish/subscribe system [7], it means messages are routed according to the content of the message. For the security purpose systems were using public key infrastructure (PKI) that allows encrypting data to a particular user. Sender and receiver are strongly coupled that is before a sender can encrypt a message; the receiver must generate a public/private key pair and communicate it to the sender. Here we are using content based publish/subscribe system[7] and for the security purpose we are encrypting the message but here question is that how to route that encrypted message to the correct destination. The answer is given by the use of concept that is searchable encryption means public key encryption with keyword search [6]. It allows decrypting message without learning anything else from the message and can determine that keyword is present in the message or not. It is also called as "non interactive public key encryption with keyword search" [6].

2.1 Identity based encryption

In this Identity based encryption [1] the concept of encryption is same as general concept of encryption and decryption but the difference is that here we are using unique identity of each user that can be a publisher or subscriber. This unique identity of the user can be public key of the user. Identity of the user is nothing but the, any valid string which uniquely identifies a user. A key server maintains a single pair of public and private master keys. With the use of master public key message is encrypted and it can be forwarded to the user with any identity. For successfully decrypting that message at the receiver side, the receiver must obtain private key from the key server, that private is for its own identity. Figure shows basic idea of the identity based encryption [1]. Identity of the user is provided in the credential. Credential is nothing but the

i) Capability of a peer

ii) Proof of its identity

Private keys and events or messages are also labelled with credentials. If there is a match between credential related to key and event or message then only subscriber can decrypt the message. It means that only after matching private key is provided to the subscriber by the key server and that key is used for the decryption of the event. This is done by the key server, credential is provided by the user to the key server and then after matching credential key is provided by the key server.

This IBE looks like a centralized solution but its features are suitable for highly distributed applications. The important thing is that sender must know master public key to communicate with any identity. Like this receiver only obtains private keys for own identities. We can replicate the central key server within the network as per the requirement of the system. The concept of identity based encryption [1] is as shown in figure 1.

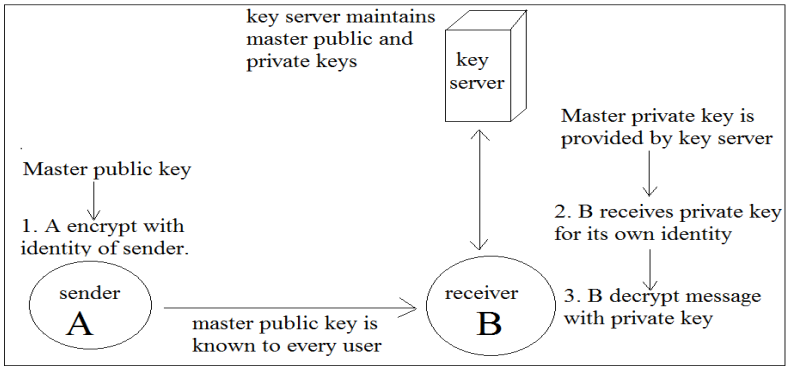

Fig.1 Process of Identity Based Encryption (IBE)

III. Proposed Work

Key Generation

Keys are generated by the key server. At the time of key generation we have to consider identity based encryption [1]. The real implementation of IBE is done by using pairing based cryptography (PBC). It establishes mapping between two groups by using bilinear maps. Here bilinear maps are used for the implementation of basic security mechanism in the publish/subscribe system [7].

Let G1 and G2 be cyclic group of order q, where q is some large prime. A bilinear map is a function ê: G1XG1→ G2 that associates pair elements from G1 to elements in G2. We have to choose four cryptographic hash functions H1, H2, H3 and H4. A bilinear map satisfies the following conditions:

1. Bilinearity . $\hat{e}(x^u, y^v) = \hat{e}(x^v, y^u) = \hat{e}(x,y)^w$, for all x,y ϵ G1and u,v ϵ Z
2. Nondegeneracy. ê(x,y)!=1, for all x,y ϵ G1.
3. Computability. Ê can be efficiently computed.

Initially we are choosing $\alpha, \varphi \epsilon Z$ and also chooses $g^2, u', m' \epsilon$.

Publisher keys:

Before starting to publish events publisher must register in the content based publish/subscribe system[7]. Here we are using attribute based encryption[3]. After that publisher contact with key server and provide credentials for each attribute. The public key for credi,j is generated as

$Pu^{P}_{i,j}$ = (credi,j ‖ Ai ‖ PUB)

credi,j is a credential with label j for the attribute Ai. Credential itself contains proof of its identity , in this way here identity based encryption is used.

The key server will generate the related private keys as follows:

For each credential credi,j and publisher P by applying hash function Vp = H1($Pu^{P}_{i,j}$) be a string of length n_u. The key server chooses $\gamma_{i,j} \epsilon Z_q$ at random and computes

$$Pr^{P}_{i,j} = \left(g_2^{\alpha} \left(u' \prod_{k \epsilon l_{i,j}} uk \right)^{\gamma_{i,j}}, g^{\gamma_{i,j}} \right)$$

= ($Pr^{P}_{i,j}[1]$, $Pr^{P}_{i,j}[2]$)

Vp[k] denote kth bit

Let $l_{i,j}$ {1,2,….,n_u} be set of all k for which Vp[k]=1

Subscriber keys:

Similarly to receive matching events with its subscription , a subscriber must contact the key server and receive the private keys.

$Pu^{s}_{i,j}$ = (credi,j ‖ Ai ‖ SUB)

The key server chooses $\gamma s \in Z$ at random , $\gamma i,j \in Zq$

$$Pr^{s}i,j = \left(g_2{}^{\gamma s} \left(u' \prod_{k \in li,j} uk \right)^{\gamma i,j} , g^{\gamma i,j}, H_3 \left(u' \prod_{k \in li,j} uk \right) \right)^{1}$$

$= (Pr^{s}i,j[1], Pr^{s}i,j[2], Pr^{s}i,j[3])$

$Pr^{s}i,j[3]$ is not used to decrypt events but it provides routing[5] of encrypted events from publishers to subscribers.

In this way keys are generated by the key server and these are used to encrypt and decrypt events in the content based publish subscribe system. We are using symmetric key cryptography[4] and Advanced encryption standard (AES)[8] algorithm for the creation of keys.

IV. Simulation Results

All our measurements were made on a 2GHz Intel core Duo with 3GB RAM, running Windows 7 operating system. The simulation studies involve the Content based publish/Subscribe system [7] over a system and also we are using tomcat server. Standard AES [8] algorithm is used for the encryption purpose. It is based on principle known as a substitution-permutation network, and uses symmetric key encryption [4].

For the simulation purpose at one moment system is having three subscribers and two or more publishers. The message is spread or disseminated over the network and it is subscribed by only one subscriber. This message is routed or shared over the network and these are in the encrypted form and only the user of the system who is subscribed that event or message gets key for decryption therefore performance graph looks as shown in fig 2. As the number of subscribers increased the average event or message dissemination delay increases in proportion with the increase in the number of subscribers.

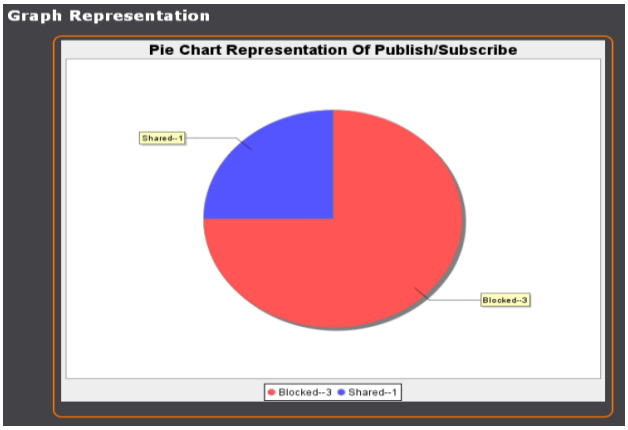

Fig. Pie chart representation of publish/subscribe system.

V. Conclusion

This paper provides a new approach to enhance capability of the content based Publish/Subscribe system. We are enhancing the capability in the sense that we can do use of cryptography [4] very easily because of the identity based encryption model and use of the Advanced Encryption Standard (AES) [8] algorithm. We have adopted Identity based Encryption technique (IBE) for the confirmation of decryption of cipher text takes place only when there is a match between credential of event and its private keys. So our system is secure [2] as compared to simple content based publish/Subscribe system.

References

[1]. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil 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]. Legathaux Martins and Sergio Duarte "Routing Algorithms for Content based publish/subscribe system"IEEE commm-unications and tutorials first quarter 2010.
[6]. 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.
[7]. H.-A. Jacobsen, A.K.Y. Cheung, G. Li, B. Maniymaran, V. Muthusamy, and R.S. Kazemzadeh, "The PADRES Publish/Subscribe System," Principles and Applications of DistributedEvent-Based Systems. IGI Global, 2010.
[8]. F.P. Miller, A.F. Vandome, and J. McBrewster, Advanced Encryption Standard. Alpha Press, 2009.