An Efficient Approach for Securing Broker-Less Publish-Subscribe System using Identity-based Encryption Scheme

Minahaj. N. Choudhari[1] Dr. Rashmi Racch[2] Soumya. P. Bhandlkar[3]
[1,3]P.G. Student [2]Associate Professor
[1,2,3]Department of Computer Science & Engineering
[1,2,3]VTU PG center, Belagavi, India

Abstract— User identification and confidentiality of data transmitted are the main challenges faced by most of the distributed systems nowadays. Existing publish-subscribe system makes use of brokers but there are issues with this such as guaranteed message delivery. Public key infrastructure is not efficient for large distributed systems as sender needs to obtain the public key from certificate authority. In this paper an Identity-based encryption scheme is proposed which allows fine-grained access control to provide confidentiality of information by encrypting information using a unique identity of user as public key.

Key words: Publish-Subscribe, Confidentiality, Identity Based Encryption

I. INTRODUCTION

The Internet has changed the scale of distributed systems and now these distributed systems all over the world involve thousands of users whose behavior and location may change rapidly. Nowadays, Internet applications need information access across various platforms, organizational boundaries, and a large number of producers and consumers of data [14]. These constraints demand for more flexible systems and models reflecting the decoupled and dynamic nature of the applications. Nowadays the publish/subscribe system is getting more attention as it provides the loosely coupled form of interaction needed in such large scale applications.

A. Publish-Subscribe System

A Publish-Subscribe system is a communication infrastructure which allows accessing the data across large numbers of data publishers and data subscribers, which are spread over the Internet[14]. Here publishers publishes the information or data in the form of data events and subscribers shows their interests in the events by sending subscriptions to the publish-subscribe system network [3]. In the publish-subscribe model, subscribers get only a subset of the total published messages. In many publish-subscribe system, publishers send messages to an intermediary broker and subscribers register their subscriptions with the broker and the broker performs the filtering. Normally the broker does store and forward function to send messages from publishers to subscribers[3].

The publish/subscribe system has gained very much attention because of decoupling of publishers and the subscribers in the terms of space ,time and synchronization. The publish-subscribe system has two important features. First is loose coupling i.e communicating users in publish-subscribe system are loosely coupled means that publishers does not need to know who are information receivers and the receivers also do not need to know from where the information coming[2]. Publishers and subscribers can remain ignorant of system topology and thus regardless of the other they can continue to operate normally. Second is the scalability i.e publish-subscribe system allows for dynamic and flexible communication environment for large number of users. Publish-subscribe system provides the opportunity for better scalability through parallel operation, network-based routing, etc[2]. Publishers publishes information to the publish/subscribe system, and by means of subscriptions the subscribers specify the events of interest. Traditionally sending and receiving data over a broker network ensures this decoupling[1]. Nowadays in more recent systems, publishers and subscribers use broker-less routing infrastructure to organize themselves, forming a secure network [1].

B. Public Key Infrastructure

In the PKI senders and receivers are tightly coupled means that if a sender wants to send a message to a receiver, the receiver has to generate a public/private key pair and he should get its public key signed by a certificate authority and send it to the sender. There is an overhead of getting the receivers public key from certificate authority. Hence a new mechanism is required to overcome this drawback. One such mechanism is encrypting the messages using Identity Based Encryption.

C. Identity based Encryption

Identity Based Encryption is a scheme where the public key of a user is a unique information about of the user[9]. Adi Shamir proposed the first ID-based encryption in 1984. The simplification of certificate management in the e-mail systems was the original motivation to develop Identity based encryption[10]. The complexity of a cryptography system is significantly reduces with the use of this feature. It eliminates the need of generating and managing the users certificates which is time consuming.

II. RELATED WORK

In the publish-subscribe system access control means, only the publishers who are authenticated are allowed to publish information and only these events are sent to authorized subscribers[1]. Many-to-many communication model is a strength of publish/ subscribe system and as well as loose coupling of components. But some data may be sensitive, and for personal reasons its visibility should be carefully controlled. In several large-scale systems like healthcare, transportation and environmental monitoring the event-based system is needed but security is an issue. J. Bacon, et al.[11] have developed a system that includes multiple administration domains that shares a network of brokers. Here the access control functionality is located in the client-hosting brokers, with this "Role Based Access Control (RBAC)" is applied on the publish/subscribe clients.

H.A. Jacobsen, et al.[12] designed a system called as PADRES system (Publish/subscribe Applied to

Distributed REsource Scheduling). In this robustness is achieved with the use of load balancing techniques, alternate message routing paths, and fault resilience techniques which react to broker failures. In this system the publishers post their messages to the intermediate broker and then this broker forwards events to the subscribers according to the matching subscriptions. A number of tools to administer and manage large publish/subscribe network is included in PADRES system.

A. Shikfa, et al.[13] have proposed system that uses a commutative multiple encryption scheme. This scheme allows a broker to perform in-network matching without reading information or content. In the multiple layer encryption, encryption on data is done several times by using different keys.

M. Srivatsa, et al.[14] have proposed a system called EventGuard which is a framework for securing the publish-subscribe system with brokers. EventGuard depends on a trusted meta-service (MS) responsible for creation of keys which are used for securing data and control the access in the publish-subscribe network. EventGuard generates public/private key pairs and certificates for meta-service and for the publishers and subscribers.

But there are issues with the existing systems such as the broker in the publish/subscribe system does not guarantee the delivery of messages means that there may be chances of failure of broker. In case if broker fails the publish-subscribe system may collapse. There is an issue of untrusted brokers and flow of message volume to an individual subscriber may become slow as publishers and subscribers increases. Public Key Infrastructure is inefficient as the sender needs to obtain the receivers public key from the Certificate Authority for encrypting messages.

In this paper an Identity based encryption scheme is proposed to overcome these drawbacks and it uses broker-less publish-subscribe system. This identity based encryption scheme makes use of a valid string to uniquely identify a user which can act as public key of the user. This paper aims to provide confidentiality of data by encrypting data using identity based encryption scheme. This paper ensures that subscribers can decrypt the data only if they have valid key.

III. PROPOSED SYSTEM

Unlike, in the system which uses Public key infrastructure where there is an overhead of getting the receivers public key from certificate authority each time for encrypting data, in this paper an identity based encryption scheme is proposed which makes use of a valid string to uniquely identify a user which can act as public key of the user.

A. Architecture of Identity Based Encryption

Identity based encryption scheme is a public key encryption scheme where the public key can be a valid string of a user. In Identity based encryption a key server generates and maintains a master public key and a master private key. When a sender wants to encrypt a message and send, he uses the master public key with any of unique identity of receiver such as an email address. If a receiver wants to read that message he is required to obtain the private key from the key server.

Pairing-based cryptography is used to implement identity-based encryption scheme. A mapping is established between two cryptographic groups with the use of bilinear maps. The basic security mechanism is ensured by using bilinear maps. A bilinear map is defined by a function

$$e: G1 \times G2 \rightarrow Gt \qquad (1.1)$$

which associates pair of elements from a group G1 and G2 of prime order q to elements in another group Gt.

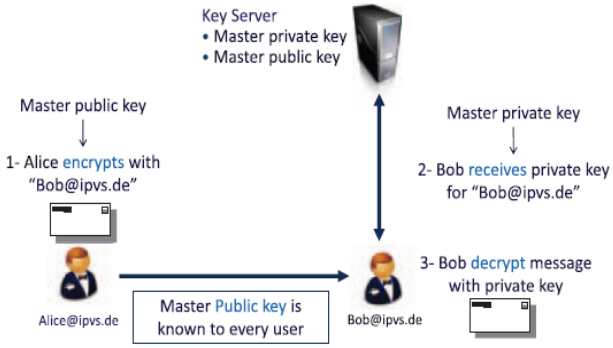

Fig. 1: Identity Based Encryption

The above figure shows the working of Identity based encryption. Here when Alice wants to send an email to Bob at bob@ipvs.de she uses the public key such as bob@ipvs.de to encrypt her message. For Alice there is no need to obtain public key certificate of Bob. When Bob wants to read the message he contacts the key server. Bob should authenticate himself to key server in the way he would authenticates to the certificate authority, and obtain private key from key server. Now Bob is able to read his email sent by Alice. Unlike the existing e-mail infrastructure, now Alice is able to send encrypted message to Bob even if Bob's public key certificate has not yet been setup with the certificate authority.

B. Identity Based Encryption Scheme

Identity Based Encryption is specified by four algorithms namely Setup, Encrypt, Extract, and Decrypt.

1) Setup:

It takes input a security parameter k and gives params P as output which are security parameters that include master public key and a master private key Km often called as master key. The system parameters have a description of a message space $\mathcal{M}$ and ciphertext space C. Here system parameters will be known to public while the master key is only known to the key server.

2) Extract:

It takes input as the master public key , master private key and an user identity ID and it outputs a private key d for that identity.

3) Encryption:

It takes master public key, user identity ID and a data $m \in \mathcal{M}$. It outputs encrypted message $c \in C$.

4) Decrypt:

It takes mastetr public key, user identity ID, a private key d, and ciphertext $c \in C$. It returns the original data $m \in \mathcal{M}$.

IV. IMPLEMENTATION

There are two entities in this system, publishers and subscribers. Publishers publishes information to the publish/subscribe system, and by means of subscriptions the subscribers specify the events of interest. Unlike, in the

Public key infrastructure infrastructure where there is an overhead of getting the receivers public key from certificate authority, in this paper authentication of publishers and subscribers and confidentiality of data are provided using identity based encryption scheme. This paper uses broker-less publish-subscribe system in which there is no intermediate broker.

An Elliptic Curve is curve of the form:

$$y^2 = x^3 + ax + b \qquad (1.2)$$

where a, b, c and x, y are elements of some Field. A finite field is a field where the set is having a finite number of elements. The algorithms based on elliptic curve uses smaller key size compared to other algorithms. This is the main advantage of elliptic curve cryptography. In this paper confidentiality of data is provided by using Ciphertext Policy Attribute Based Encryption (CP-ABE) where identity is passed as policy to encrypt information or message.

A. Authentication of Publishers/Subscribers

In the publish-subscribe system only authenticated users or publishers are allowed to publish data events. Similarly only authenticated users or subscribers are allowed to send request to data events published by publishers. The publisher or subscribers have to first register themselves. If publishers or subscribers are not registered then they cannot publish or subscribe to the data. Authentication of the publishers or subscribers is provided with the use of a userid and password.

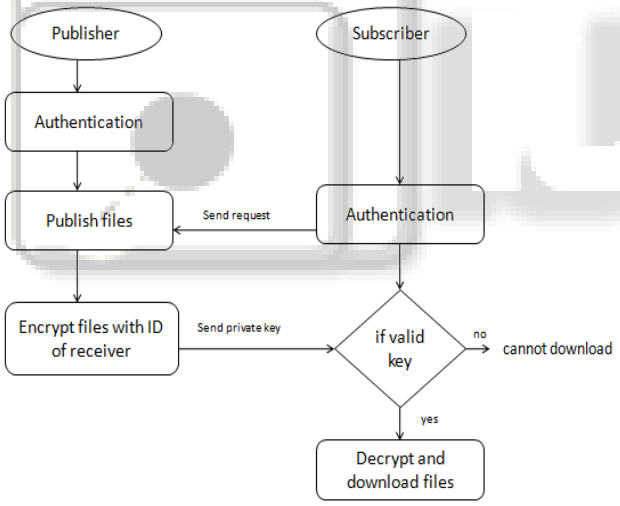

Fig. 2: Flowchart of broker-less publish-subscribe system using identity based encryption

B. Confidentiality of Data

Confidentiality of data is provided by encrypting data using identity based encryption scheme. When a publisher publishes the data, subscriber can send request to data events published by publishers. A publisher receives the subscription requests from various subscribers. Here when the publisher gives access, he takes the subscribers identity such as his email-id to encrypt data using identity based encryption scheme. The publisher computes the private key by taking the subscriber's email-id as his unique identity and sends it to the subscribers email address. When a subscriber wants to access or download the data he has to have the private key to decrypt the encrypted data. This private key is send to his email address by publisher. The subscriber is allowed to read the data only when he has the valid key.

V. Conclusion and Future Scope

In this paper, we have developed a broker-less publish-subscribe system and used an Identity based encryption scheme for publish-subscribe system. This Identity based encryption scheme made use of a string which uniquely identify a user as a public key of that user. Data confidentiality has been provided in this paper by encrypting the information or data using Identity based encryption scheme. It is ensured that a subscriber can decrypt data only if he has the valid key.

In this paper, email address has been used as public key of a user to encrypt data. In future, this Identity based encryption scheme may make use of email address and date to encrypt data and a private key will be generated which will work on that date only. This will be a very useful feature that is "encrypting into future".

References

[1] M.A. Tariq, B. Koldehofe, and K. Rothermel, "Securing broker-less publish-subscribe systems using Identity based encryption" IEEE Transactions on Parallel and Distributed Systems, February, 2014.
[2] Publish-subscribe-pattern, http://en.wikipedia.org/wiki/Publish-subscribe-pattern.
[3] M. Srivatsa, L. Liu, "Secure Event Dissemination in Publish-Subscribe Networks", 27th International Conference on Distributed Computing Systems, 2007.
[4] Fact-Sheet, https://www.priv.gc.ca/resource/fs fi/02_05_d_51_cc_e.pdf.
[5] "Coordination and Events", file:///G:/PROJECT/DFD/No Title.htm .
[6] JoelWeise–SunPSSM, "Public Key Infrastructure Overview",Global Security Practice Sun BluePrints OnLine - August 2001.
[7] "Identity-based-Encryption" http://en.wikipedia.org/wiki/ID-based_encryption.
[8] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, 2001.
[9] J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch, "Access Control in Publish/Subscribe Systems," Proc. Second ACM Int'l Conf. Distributed Event-Based Systems (DEBS), 2008.
[10] 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 Distributed Event-Based Systems. IGI Global, 2010.
[11] A.Shikfa, M.O¨nen, and R.Molva, "Privacy-Preserving Content- Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.
[12] 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.
[13] "Elliptic-Curve-Cryptography" http://en.wikipedia.org/wiki/Elliptic_curve_cryptography.

