IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

A Review on Confidentiality and Authentication in Content Based Publish/Subscribe System

Nileema R. Hiray[1], Prof. K. N. Shedge[2]

PG Student, Computer Engineering Department, S.V.I.T. Chincholi, Nashik, India [1]

Assistant Professor, Computer Engineering Department, S.V.I.T. Chincholi, Nashik, India[2]

Abstract: Publish/Subscribe System is an emerging communication model which runs in distributed environment. It is a messaging system, where the messages/events are published by publishers and received by subscribers based on their subscription. In the existing messaging systems, broker acts as a middleware in between two parties and all the communication is done through the broker. In this case, the broker failure can be the bottleneck of whole system. To overcome this drawback, there is a system proposed which uses brokerless architecture for the content based publish/subscribe system. In publish/subscribe system, publisher and subscriber are loosely coupled and do not keep trust on each other. So, the basic security mechanisms like authentication and confidentiality are difficult to achieve and hence, a challenging task. The proposed system provides the novel approach to achieve authentication and confidentiality in a brokerless content based publish/subscribe system using the identity based encryption.

Keywords: Publish/subscribe, Content-based, Broker-less, Publisher, Subscriber, Security, Identity based encryption.

I. INTRODUCTION

Now a days, Internet is a rapidly growing and there is a need arise to transfer information between different entities. These entities are nothing but the human being. The uncountable entities are widely spread globally and hence their locations and behaviour becomes vary. Therefore, to bring these distributed entities to be closer and to make them scalable, more efficient and reliable techniques are required for information distribution. The synchronous peer to peer communication models are not able to satisfy these requirements. So, the publisher/subscriber asynchronous messaging system has been experiencing highest popularity due to its inherent decoupling feature. This system allows distribution of information from event producers i.e. publishers to event consumers i.e. subscribers. There are different types of system infrastructure such as topic based systems and content based systems.

The publish/subscribe system's decoupling feature allows publishers to be unknown from subscriber with the aspects such as space, time, synchronization. Publishers transfers information using publish/subscribe system, subscribers registers events/messages of interest using subscriptions. Without knowing the subscriber details to publisher and vice versa the events are routed to the relevant subscribers. In traditional systems, broker is used to route the events/messages from publishers to subscribers. This leads to security questions. Broker can be malicious while routing and can read the plain text information. Failure of brokers can leads to the whole system down. So, providing security to the pub/sub system becomes a challenging task. To address this issue, a recent system comes with a broker less publisher-subscriber architectures. For this event forwarding overlay is used [1].

Subscribers can receive the published events only on the subscription of that event. There are two ways/models for specifying the subscriptions: 1) Topic Based Subscription 2) Content Based Subscription. In a topic based subscription, one particular topic is specified and all the events relevant to that topic are sent to the related subscribers. There is no restriction on the message content in the topic based model. Whereas, content based subscription model is the most expressive in nature. Using this model subscriber can define the restrictions or constraints on message contents. Content based model for subscription is helpful for large scale distributed applications such as environmental monitoring, stock exchange, news distribution, public sensing and traffic control. By considering the expressiveness and asynchronous characteristics, we are using the content based model in our proposed system.

Now, the question of security comes in picture. To provide a security in a broker less publish/subscribe systems a new approach with authentication and confidentiality is proposed. In this approach, according to the subscription all subscribers are allowed to maintain their credentials. Private keys associated with the subscribers are also labelled with the credentials. These credentials can be numeric or string attributes. For mapping each encrypted event with a set of credentials, an Identity Based Encryption (IBE) mechanism [2] will be used to ensure the decryption of event by the subscriber only on successful match between the credentials with the event and the private key. IBE also allows subscribers to verify the authenticity of the received event.

II. LITERATURE SURVEY

In this section, we have studied previous research papers related to the traditional broker architectures. These papers focused only on the scalability and expressiveness characteristics of the system but consider little aspects of security. The major focus on security is given while

DOI 10.17148/IJARCCE.2015.41240

developing the proposed system. The brief review of previous research papers is as follows:

A. Sahai [3] presented a system having Ciphertext Policy Attribute Based Encryption. Using this technique, the encrypted data is kept secret even if the storage server is unsecure. In the systems previous to this, attributes are used by the Attribute Based Encryption systems to describe and specify the encrypted data and policies into user's keys while this authors system uses attributes to describe a user's credentials. A policy for who can decrypt the cipher data is determined by the sender party (responsible for encrypting data).

S. Choi [4], presented a broker system. In this, each user submits a list of subscriptions to a broker. Broker is responsible for routing data from publisher to the subscribers. Publisher sends notification message (contains value) to the broker, if the value in the notification match with the subscriptions then only broker will forward it to the subscriber. In most cases, data to be published is confidential and its contents must be safe from the broker. Also, subscription may contain sensitive information that must be protected from the broker. So, it is a need to route the data from publisher to subscriber without an intermediary broker who can learn the data from publishers notifications and subscribers subscriptions. This is a challenging task for the future systems.

B. Crispo[5] presented a publish/subscribe system which is loosely coupled. In this system, applications interacts indirectly and asynchronously. There is a brokers network through which publisher sent events to interested subscribers. Broker uses filters for the routing of events. Subscriber can specify their interests by specifying these filters.
The mechanisms used for confidentiality of both event and filters should not require to share the secret keys of publishers and subscribers. It should also allow event filtering to route the events to intended subscribers. These are the weak points of existing systems. So, here proposed a mechanism to address all these issues.

L. Liu [6] presented an Event Guard framework for the construction of secure wide area pub-sub systems. Event Guard mechanisms provides the security guarantees, system's over all simplicity, scalability and performance. The framework has three main components. First is a security guards suite. It is plugged-into a content based pub-sub system, second component is a scalable algorithm for key management that will be used to enforce access control on subscribers, and the third component is a publish-subscribe network design that recovers quickly from the difficult situations.

R. Molva [7] suggested a set of security mechanisms. It allows privacy-preserving forwarding of the encrypted contents based on subscriber's interests. The system ensures both data confidentiality with regards to publishers and the subscribers privacy with respect to their interests in a model where the publishers, the subscribers and the intermediate nodes (brokers) in charge of data forwarding do not trust each other. The scheme uses a multi-layer encryption. In this, it is possible for intermediate nodes to manage forwarding tables and to perform content forwarding not only using encrypted content but also using encrypted subscriber messages without accessing the plaintext of the data. This scheme also avoids key sharing between the end-users and targets an enhanced CBPS model where brokers can also be subscribers at the same time.

B. Maniymaran, [8] presented a content-based publish/subscribe system which gives detailed overview of the "PADRES" PADRES is helpful for correlating events, accessing data that is produced in the past and that will be produced in the future, counterbalance the traffic load among brokers, and handle network failures. It can also filter, aggregate, correlate and direct any combination of historic and future data. Several applications are also presented in detail that can benefit from the content-based nature of the pub/sub system and take advantage of its scalability and robustness features. While developing large-scale distributed systems that are going to be used on the Internet, it should have a proper middleware support, to handle the communication needs of those application clients in a scalable and efficient way, and without loosing traditional middleware features.

P. Pietzuch [9] described the concept of "Hermes". Its is a distributed, event-based middleware and provides peer-to-peer messaging techniques for scalable and robust event transmission. For managing the network of event brokers Hermes uses peer-to-peer techniques. It also adds fault-tolerance to its event transmission algorithms in the pub/sub systems.

B. Yang [10] invented the first identity based signcryption scheme. Their scheme still has some security weaknesses and further, proposed a refined version of the scheme to prove its security under the existing security model for identity-based signcryption.

The proposed system will overcome the drawbacks of the previous systems which we have seen above. It will focus on brokerless architecture and also considers the security needs by providing authentication and confidentiality. Content based routing scheme and Identity Based Encryption mechanism will be used by the proposed system. Main aim of the proposed system is to provide the security in a content based publish/subscribe system.

III.PROPOSED SYSTEM

InOur proposed system makes use of content based model for routing the published content from publisher to the appropriate subscriber. The message/event to be publish has an ordered set of attributes. These attributes have a unique name, types of data and its field. Further, event will match with the subscription, if the contents in the attributes suits the constraints required by the subscription then only subscriber can get the event he/she want.
Proposed system uses the identity based encryption to provide the authentication and confidentiality in the broker less content based publish/subscribe system. Identity based

DOI 10.17148/IJARCCE.2015.41240

encryption provides a good way to reduce the number of keys to be managed. In identity based encryption any valid string can be a public key of a particular user which uniquely identifies him/her. As shown in figure 1, there are three components of proposed system a) publisher b) subscriber c) key server which maintains a pair of public and private master keys. Each user in the system knows the public master key, it is used by the publisher to encrypt the messages and sends them to the subscriber with an identity. Subscriber gets private key from key server to decrypt the message successfully.

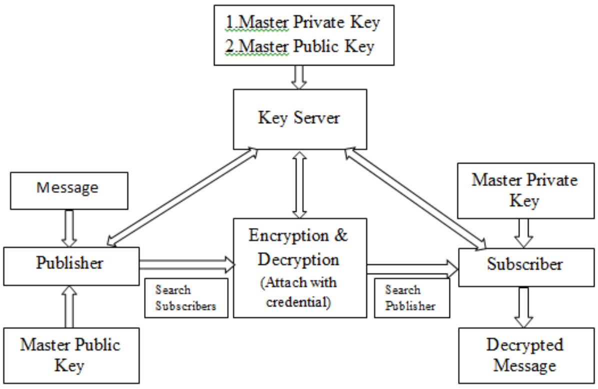

Fig. System Architecture for Identity Based Encryption

Credentials will be used to verify the identity of end user against the key server. It consists of binary string. The keys assigned to publisher and subscriber will label with credentials. The subscriber can decrypt an event/message only if there will be match between event credentials and the key to avoid unauthorized publications. In short, credentials ensures that only the valid publishers can publish events in the system and similarly, subscribers can receive events only to which they have subscribed. In case of confidentiality, credentials ensure that the only authorized subscribers can see the events and the events can't be modified by an unauthorized person.

IV. CONCLUSION

Due to the loose coupling between the publisher and subscriber, it is essential to address the security challenge of the system. To achieve this, we have proposed a novel approach to provide the authentication and confidentiality in a broker less content based publish/subscribe system. The proposed approach also considers the scalability with the view point of number of publisher, number of subscriber and the number of keys. Credentials will assign to the publisher and subscriber as per their advertisements and subscriptions respectively. The public key is nothing but any valid string which uniquely identifies a user. A key server has a single pair of public and private master keys. Sender uses the master public key to encrypt and transfer the messages to a user with any identity. To decrypt the message, a receiver has to obtain a private key for its identity from the key server.

In this way, the secure data sharing will be achieve by the broker less content based publish subscribe system using identity based encryption.

REFERENCES

[1] E. Anceaume, M. Gradinariu, A.K. Datta, G. Simon, andA. Virgillito, "A Semantic Overlay for Self- Peer-to-Peer Publish/Subscribe," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems (ICDCS), 2006.

[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] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute-Based Encryption," Proc. IEEE Symp. Security andPrivacy, 2007.

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

[5] M. Ion, G. Russello, and B. Crispo, "Supporting Publication andSubscription Confidentiality in Pub/Sub Networks," Proc. SixthInt'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm),2010.

[6] M. Srivatsa, L. Liu, and A. Iyengar, "EventGuard: A SystemArchitecture for Securing Publish-Subscribe Networks," ACMTrans. Computer Systems, vol. 29, article 10, 2011.

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

[8] H.-A . J acobsen, 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.

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

[10] Y. Yu, B. Yang, Y. Sun, and S.-l. Zhu, "Identity Based SigncryptionScheme without Random Oracles," Computer Standards & Interfaces,vol. 31, pp. 56-62, 2009.

DOI 10.17148/IJARCCE.2015.41240