International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 5 3433 - 3435

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

Lakshmi Devi K.N
Department of Computer Science and Engineering
Vemana Institute of Technology
Bengaluru, India
Sisal038@gmail.com

Vijaya S.C
Department of Computer Science and Engineering
Vemana Institute of Technology
Bengaluru, India
Vit.vijaya@gmail.com

Abstract – The basic security mechanism such as authentication and confidentiality is highly challenging in a content based publish/subscribe system. Authentication of publisher and subscribers is difficult to achieve due to loose coupling of publisher and subscriber. The authentication and confidentiality of publisher and subscribers of events ensured by adapting the pairing based cryptography mechanism. Furthermore, an algorithm to cluster subscriber according to their subscriptions preserves a weak notion of subscription confidentiality.

Keywords: *Publish/subscribe, security, identity based encryption.*

*****

I. INTRODUCTION

The publish/subscribe communication paradigm has gained high popularity because of inherent decoupling of publishers from subscribers in terms of time, space, and synchronization. Content-based publish/subscribe is the variant that provides the most expressive subscription model. The expressiveness and asynchronous nature is useful for large-scale distributed applications. Access control in the context of publish/subscribe system means only the authenticated publisher are allowed to disseminate events in the network and only those events are delivered to authorized subscriber. Existing approaches toward secure publish/subscribe systems mostly rely on the presence of a traditional broker network.

The approach allows subscribers to maintain credentials according to their subscriptions. The private keys are assigned to the subscribers and are labeled with the credentials. The identity based encryption mechanism, are adopted to ensure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event and the key, and allow subscribers to verify the authenticity of received events.

II. BACKGROUND AND MOTIVATION

The publish/subscribe system consist of three goals, namely authentication, confidentiality, and scalability.

Authentication: Only authorized publishers are able to publish events in the system, similarly subscribers should only receive those messages.

Confidentiality: The events are only visible to authorized subscribers and are protected from unauthorized users.

Scalability: The publish/subscribe system should scale with number of subscribers in the system.

The security mechanism in publish/subscribe use the principle of identity based encryption to support many to many interactions between subscribers and publishers.

The publishers and subscribers interact with key server, they provide credentials to the key server and in turn receive keys. The credential consists of a binary string which describes the capability of a peer in publishing and receiving events and a proof of its identity.

The key assigned to publishers and subscribers are labeled with credentials. The identity based encryption ensures that a particular key can decrypt a cipher text only if there is a match between the credentials of cipher text and key. Publisher and subscribers maintain separate private keys for each authorized credentials.

III. RELATED WORK

In [1], the publish/subscribe is many to many communication paradigm and loose coupling of components, so that the publisher need not know the recipients of their data and subscribers need not know the number and location of publishers. The large scale systems required by government and public bodies for domains.

A publish/subscribe service can be secured, by specifying and enforcing access control policy at the service API, and by enforcing the security and privacy aspects of these policies within the service network itself. Finally the alternative to whole message encryption is appropriate for highly sensitive and long-lived data destined for specific domains with varied requirements.

In [2], in distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. The only method for enforcing such policies is to employ a trusted server to store the data. However, if any

server storing the data is compromised, then the confidentiality of data will be compromised. A system for realizing complex access control on encrypted data that is cipher text-policy attribute based encryption. By using the technique encrypted data can be kept confidential even if storage server is not trusted. Moreover, the methods are secure against collision attacks. Attribute based encryption systems used attributes to describe the encrypt data and built policies into users key, while in proposed system attributes are used to describe a users credentials and encrypting data determines a policy for who can decrypt.

In [3], the user bob who sends email to user Alice encrypted under Alice public key. An email gateway wants to test whether the email contains the keyword so that it could route the email accordingly. Alice, on other hand does not wish to give the gateway the ability to decrypt all her messages. To define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word is a keyword in the email without learning anything else about the email. The mechanism as public key encryption with keyword search.

In [4], publish/subscribe systems supports highly scale, many to many communication among loosely coupled publishers and subscribers. Modern publish/subscribe systems perform message routing based on the messages related to their subscriptions and the current context. However, both content and context encode sensitive information which should be protected from third party brokers that make routing decisions. The approach assures the confidentiality of the message being published and subscriptions being issued while allowing the brokers to make routing decisions without decrypting individual messages and subscriptions. Further, subscribers with a frequently changing context such as location are able to issue and update subscriptions without revealing the subscriptions in plaintext to the broker and without the need to contact a trusted third party for each subscription change resulting from a change in the context.

In [5], the more sensitive data is shared and stored by third party on the internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level. To develop a new cryptosystem for fine-grained sharing of encrypted data we call key-policy attribute-based encryption. In cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

In [6], a content centric privacy scheme for information centric networking is able to support data confidentiality by introducing attribute-based encryption into ICN and making it specific to the data attribute. The approach is unusual in that it preserves ICN goal to decouple publishers and subscribers for greater data, accessibility, scale multiparty communication and efficient data distribution. Moreover, to propose an attribute-based routing scheme that offers interest confidentiality. A prototype system is implemented based on CCN, a popular open source version of ICN, to showcase privacy preservation in smart neighborhood and smart city application.

In [7], the publication specifies the triple data encryption algorithm, including its primary component cryptographic engine, the data encryption algorithm. The TDEA may be used by federal organizations to protect sensitive unclassified data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. The recommendation defines the mathematical steps required to cryptographically protect data using TDEA and to subsequently process such protected data. TDEA is made available for use by federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls.

IV. SYSTEM ARCHITECTURE

The first step in designing software is to define the architecture and consist of components and layers of software. System architecture is the conceptual design that defines the structure and behavior of system. Architecture is a formal description of a system organized in a way that supports reasoning about the structural properties of the system. It defines the components of the system or building blocks and provides a plan from which products can be procured. The system architecture is shown in Figure.1.

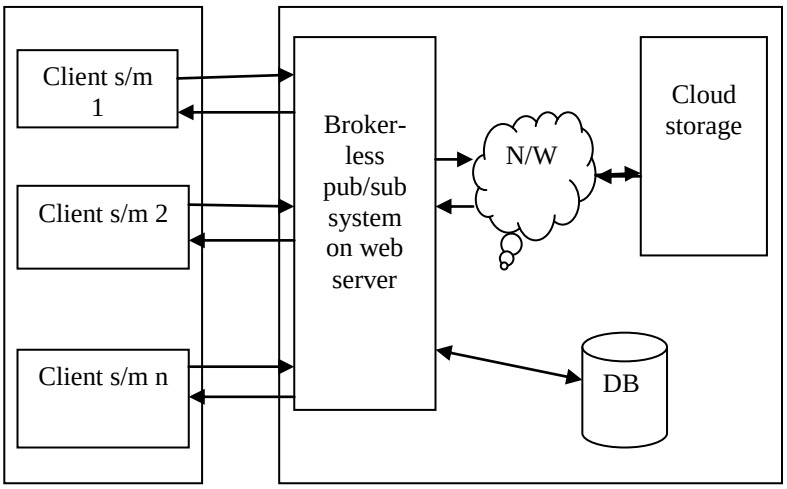

Figure.1. System architecture

Subscribers are the client system, can able to register themselves and receive their access key. Broker-less pub/sub system is also known as gateway which is an intermediate

between the publisher and subscriber. Publisher will store the file in proxy server and accessed by authorized subscriber. Publisher specify the access policy for each file, access policy are set using domain attribute and sub-domain attribute. Suppose the subscriber wants to download any file, first has to select the file from the list and the system ask for the access key, after system getting the access key it will separate the attribute set from the key and check for the access rights, if the user has the access can download the encrypted file which in turn decrypted using decryption key and download to the subscriber local system.

V. CONCLUSION

A new approach used to provide authentication and confidentiality in a broker-less content based pub/sub system and the approach is highly scalable and it provides secure and confident.

VI. ACKNOWLEDGEMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Ms. Vijaya .S.C. for her kind help and cooperation. Salutation to my beloved and esteemed institute for having well qualified staff and labs furnished with necessary equipment. I also thank to my parents and friends for their moral support and constant guidance made my efforts fruitful.

REFERENCES

[1] E. Ancesume, M. Gradinariu, A.K. Datta, G. Simon, and A. Virgillito, ‘ A Semantic Overlay for Self Peer-to-Peer Publish/Subscribe,” proc. 26th IEEE Int’l Conf. Distributed Computing Systems(ICDCS), 2006.

[2] 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.

[3] W.C. Barker and E.B. Barker, “SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher,”technical report, Nat’l Inst. of Standards and Technology, 2012

[4] J. Bethencourt, A. Sahai, and B. Waters, “Cipher text Polict Attribute Based Encryption,” proc. IEEE Symp. Security and Privacy, 2007.

[5] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public Key Encryption with Keyword Search,” proc. Int’l Conf. Theory and Application of Cryptographic Technique on Advances in Cryptology(EUROCRYPT), 2004.

[6] D. Boneh and M.K. Franklin, “Identity Based Encryption from the Weil Pairing,” proc. Int’l Cryptology Conf. Advances in Cryptology, 2001.

[7] S. Choi, G.Ghinita, and E. Bertino, “A Privacy-Enhancing Content Based Publish/Subscribe System Using Scalar Product Preserving Transformations,” proc. 21st Int’l Conf. Database and Expert Systems Application: part I, 2010.

[8] 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), 2006.

[9] M. Jelasity, A. Montresor, G.P. Jesi, and S. Voulgaris, “PeerSim:A Peer-to-Peer Simulator,” http://peersim.sourceforge.net/,2013.

[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.