



Credential Based Publisher/Subscriber Technique Using Identity Based Encryption

¹Ms. Meenal Bhojar, ²Ms. Ranjana Shende

¹M.Tech, ²Assistant Professor

Department of Computer Science and Engineering
G H Raisoni Institute of Engineering and Technology for Women
Nagpur, Maharashtra, India

Abstract: Identification and confidentiality are the main objective of any distributed system. Provision of security operations such as authentication and confidentiality is highly challenging in a content based publish/subscribe system. Identification is an essential mechanism in distributed information systems. The main concept is to share the secured data between the subscribers using attributes, it may be a weak notion but the concept of multi-credential routing makes it robust. This paper presents the mainly 1) The idea of identity (ID)-based public key cryptosystem, which enables users to communicate, a publisher which acts as an admin uses a private key to each user when first joins the networks. 2) It provides the pairing based cryptography to maintain the authenticity and confidentiality of the publisher and subscribers by maintaining the secure layer maintenance protocol. 3) The attributes help to share data by generating a secure route between the publisher and subscriber. 4) The provision to attempt the three goals of secure pub/sub system i.e. authentication, confidentiality, scalability by performing hard encryptions on the data to prevent malicious publishers to enter in the network, a thorough analysis of attacks is performed on the system.

Keywords: confidentiality, security, identity based encryption, multicredential routing

I. INTRODUCTION

In Pub/sub system access control is possible only to the authorized users. Personal details should be kept hidden from the other subscriber in the network and a subscriber should receive all relevant events without revealing its subscription to the system. Afterwards the idea of the identity based encryption is implemented in the system.

For PKI, publishers must maintain the public keys of all interested subscribers to encrypt events. Subscribers must know the public keys of all relevant publishers to verify the authenticity of the received events. This paper allows subscribers to maintain credentials according to their subscriptions. Private keys assigned to the subscribers are labeled with the credentials. A publisher encrypts all the set of events with the help of credentials. We adapted identity-based encryption (IBE) mechanisms [1][2] 1) 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 2) to allow subscribers to verify the authenticity of received events. Steps are taken to improve the weaker subscription between the publisher and subscriber by implementing the secure maintenance protocol. The paper also presents the three objectives in the system [3][6] 1) to implement the searchable encryption method by using the identity based encryption 2) to implement the phenomenon of "multicredential routing" which improves the weak subscription.

3) analysis of different attacks to improve confidentiality and authentication.

There are three major goals for the proposed secure pub/sub system, namely to support authentication, confidentiality, and scalability [3].

Authentication: To avoid noneligible publications, only authorized publishers should be able to publish events in the system. Similarly, subscribers should only receive those messages to which they are authorized to subscribe [1].

Confidentiality: In a broker-less environment, two aspects of confidentiality are of interest that the events are only visible to authorized subscribers and are protected from illegal modifications, and the subscriptions of subscribers are confidential and unforgeable [1].

Scalability: The secure pub/sub system should scale with the number of subscribers in the system. Three aspects are important to preserve scalability [1]: 1) the number of keys to be managed and the cost of subscription should be independent of the number of subscribers in the system,

2) the key server and subscribers should maintain small and constant numbers of keys per subscription, and 3) the overhead because of rekeying should be minimized without compromising the fine-grained access control.

II. RELATED WORK

There are two entities in the System publishers and subscribers. Both the entities are computationally bounded and do not trust each other. Moreover, all the peers (publishers or subscribers) participating in the pub/sub overlay network are

honest and do not deviate from the designed protocol. Likewise, authorized publishers only allow valid events in the system.

However, malicious publishers may masquerade the authorized publishers and spam the overlay network with fake and duplicate events. We do not intend to solve the digital copyright problem; therefore, authorized subscribers do not reveal the content of successfully decrypted events to other subscribers.

A. Publisher subscriber technique

Publishers and subscribers interact with a key server. They provide credentials to the key server and in turn receive keys which fit the expressed capabilities in the credentials. Subsequently, those keys can be used to encrypt, decrypt, and sign relevant messages in the contentbased pub/sub system, i.e., the credential becomes authorized by the key server. A credential consists of two parts:

- 1) a binary string which describes the capability of a peer in publishing and receiving events, and
- 2) a proof of its identity [1].

B. Identity based encryption

Identity(ID)-based public key cryptosystem, which enables any pair of users to communicate securely without exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as a trusted key generation center issues a private key to each user when he first joins the network [2].

C. Identity Handling:

Identification provides an essential building block for a large number of services and functionalities in distributed Information systems. In its simplest form, identification

Is used to uniquely denote computers on the Internet By IP addresses in combination with the Domain Name System (DNS) as a mapping service between symbolic Names and IP addresses. Thus, computers can conveniently Be referred to by their symbolic names, whereas, in The routing process, their IP addresses must be used.[3]

Higher-level directories, such as X.500/LDAP, consistently Map properties to objects which are uniquely identified by Their distinguished name (DN), i.e., their position in the X.500 tree [4].

D. Content based publish/subscribe:

Content-based networking is a generalization of the content based publish/subscribe model. [4] In content-based networking, messages are no longer addressed to the communication end-points. Instead, they are published to a distributed information space and routed by the networking substrate to the "interested" communication end-points. In most cases, the same substrate is responsible for realizing naming, binding and the actual content delivery [5].

E. Secure Key Exchange:

A key-exchange (KE) protocol is run in a network of interconnected parties where each party can be activated to run an instance of the protocol called a session [6]. Within a session a party can be activated to initiate the session or to respond to an incoming message. As a result of these activations,

and according to the specification of the protocol, the party creates and maintains a session state, generates outgoing messages, and eventually completes the session by outputting a session-key and erasing the session state [7].

III. PROPOSED WORK

Subscribers will interact with the publisher. Subscriber will provide credentials to the publisher and in turn receive keys which fit the expressed capabilities in the credentials. The keys are generated using checksum algorithm and it is distributed to the publisher and subscriber. Publisher will encrypt the data with the encryption decryption algorithm and embedded the key with data. The subscriber will login as the publisher sends the acknowledgement by means of email. The subscriber gets the private key to decrypt the data in the email. The various data sharing techniques by which the data will get shared by the publisher to the subscriber are:

A. Numerals attribute:

In this type of attribute the data is distributed in the forms of the spaces. The spaces are decomposed into the subspaces which serves the limited range of enclosure between the publisher and subscriber. Subspaces are denoted by 0 & 1. For example, an event 0010 is enclosed by the five subspaces 0010, 001, 00, 0, hence we have to generate the ciphertext according to the events of the subspaces.

B. Alphastring attribute:

Credentials for alphastring string operations is performed by using the process of prefixing the node using a trie. The root will be given a particular string and same string is given to the descendants using the different prefixes. Each peer is assigned a single credential, which is same as its subscription or advertisement..

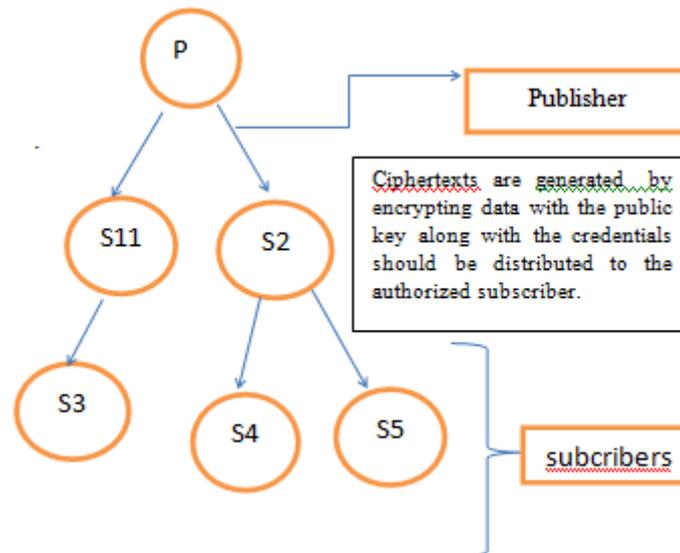


Fig: Data sharing between publisher and subscriber using identity based encryption

C. Range attribute:

For a range attribute, a subscriber receives separate credentials and, thus, keys for each attribute. A particular range is described in the network. Data is sent in the limited range of the subscriber.

IV. CONCLUSION

Scalability is achieved by increasing the number of subscribers. Using public key cryptography the publisher can distribute the private keys to the subscribers once they submitted the credentials, as cipher text are labeled with the credentials to maintain the authenticity in the system. We have adapted a technique from identity based encryption to ensure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event and its private keys to maintain the confidentiality of the subscribers.

REFERENCES

- [1] 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.
- [2] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, 2011.
- [3] Karl Aberer, Aniwitaman Datta and Manfred Hauswirth "Efficient Self Contained Handling of Identity in Peer to Peer System" IEEE transaction on knowledge and data engineering, 2004.
- [4] Sean O'Meara and Adam J. Elbert "Enhancing the Performance of Symmetric-key cryptography via Instruction set instruction" IEEE transactions on very large scale integration 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 communications and tutorials first quarter 2010.
- [7] 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