SECURED DATA SHARING IN PUBLISHER/SUBSCRIBER TECHNIQUE USING IDENTITY BASED ENCRYPTION

[1]MEENAL BHOYAR, [2]RANJANA SHENDE

[1]M.Tech, Department Of Computer Science And Engineering, G H Raisoni institute Of Engineering And Technology For Women, Nagpur, Maharashtra, India
[2]Assistant professor, Department Of Computer Science And Engineering, G H Raisoni institute Of Engineering And Technology For Women, Nagpur, Maharashtra, India
E-mail: [1]meenal.bhoyar23@gmail.com, [2]ranjana.shende@raisoni.net

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 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 encryption in which the third party provides the public and private key to the publisher and subscriber through one of its unique information it has provided during the time of submission of credentials.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 helps 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 the 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 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.

In the pub/sub model, subscribers typically used the subset of the messages and the publisher only published that set of data. Filtering is the process of selection of the messages and processing it through the network .In the past the pub/sub system mostly rely on the traditional system where this restricted security by using only keyword matching routing events or rely on semi trusted system. Building on the result paper presents allows subscriber to maintain credentials according to the subscriptions.

Access control in pub/sub system means only authenticated publishers are allowed to dissipate events and only authorized subscriber should receive the events. Loose coupling in the end to end authentication used in the content based authentication possess achallenge. Hence new mechanism is needed Where encrypted events should be routed to subscribers without knowing the subscription and publishers should be unknown to each other even after getting the authentication. This paper 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 present 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 pub/sub environment, two aspects of confidentiality are of interest that the events are onlyvisible 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) participatingin 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 interactwitha 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 toencrypt, decrypt, and sign relevant messages in the content based pub/sub system, i.e., the credential becomes authorized by the key server. A credential consists of two parts:

a binary string which describes the capability of a peer in publishing and receiving events, and

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].In identity based encryption any valid string is called the identity of the user which is called public key. A sender needs to know only the master key and receiver needs to private key which he can obtain frm the key server .For practical implementation of identity based encryption pairing based cryptography is implemented which establishes mapping by usng bilinear maps

A bilinear map from G1 × G2 to G_t is a function of:e : G1 × G2 → Gt such that for all u ∈ G1, v ∈ G2, a, b ∈ Z,$e(u^a,v^b)=e(u,v)^{ab}$

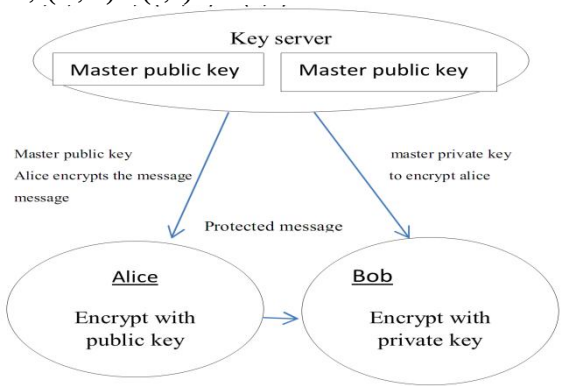

Fig 1: Identity Based Encryption

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 networkingis 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

Subcribers 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. Credentials will be used for authentication and whether the capabilities matches the individual. The public will be generated by concatenation of the strings of a credential by using the age, the event for key generation. The public key will be generated by the key server and will be distributed to the authorized subscribers. The admin will keep track of the number subscribers and publishers in the network and has also rights to remove the irrelevant data from the network. The age

restriction also helps to restrict the data from the subscribers who can no longer accessed the information. To maintain the topology the subscriber sends the coonection request in the network before it reaches the right publisher. To make it possible the subscribers should know the subscriptions of the parent and child.The event space is generated and is decomposed in subspaces, on generation of the event the three techniques will get simultaneously and helps to maintain confidentiality and security.

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 numbers. One of the attributes is numerals.

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 subscribers. The subscribers has to enter the string provided by the key server.

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. The range attribute is satisfied if all the predicates in the system are satisfied. To make secure the confidentiality the keys must be bound together, so that the keys associated with different subscription should not be combined together.The and combination of the numerals and string will access to the subscriber to the text or video.

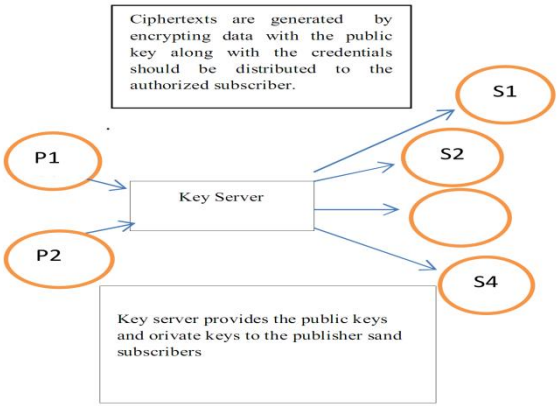

Fig: Generalize view of Data sharing between publisher and subscriber using identity based encryption

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 theWeil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, 2011.

[3] Karl aberer, Aniwitamandatta and Manfred Hauswirth "Efficient Self Contained Handling of Identity in Peer to Peer System"IEEE transaction on know- ledge and data engineering,2004.

[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] Ming li,ShuchengYu.YaoZheng,KuiReng, Weiging Lou "Scalable and secure sharing of personal data in cloud computing using attribute-based encryption"IEEE transaction on paralllel and distributed computing 2013

[6] Legathaux Martins and Sergio Duarte "Routing Algorithms for Content based publish/subscribe system"IEEEcommm- unications and tutorials first quarte 2010.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2010

[8] D. M. Goldschlag,M. G. Reed, and P. F. Syverson, "Hiding routing information,"inProc. Information Hiding, 1996, pp. 137–150, Springer-Verlag.

[9] L.Willenborg and T.Waal, Elements of Statistical Disclosure Control,ser. Lecture Notes in Statistics. New York: Springer, 2001, vol. 155.

[10] S. S. Shepard, R. Dong, R. Kresman, and L. Dunning, "Anonymous idassignment and opt-out," in Lecture Notes in Electrical Engineering,S. Ao and L. Gleman, Eds. New York: Springer, 2010, pp. 420–431.

[11] A. Karr, "Secure statistical analysis of distributed databases, emphasizingwhat we don't know," J. Privacy Confidentiality, vol. 1, no. 2,pp. 197–211, 2009.

[12] D.Angluin, "Local and global properties in networks of processors (extended abstract)," in Proc. 12th Ann. ACM Symp. Theory of Computing(STOC '80), New York, 1980, pp. 82–93.

[13] W. Fokkink and J. Pang, "Variations on itai-rodeh leader election for anonymous rings and their analysis in prism," J. Universal Comput.Sci., vol. 12, no. 8, pp. 981–1006, Aug. 2006.

[14] J. W. Yoon and H. Kim, "A new collision-free pseudonym scheme in mobile ad hoc networks," in Proc. 7th Int. Conf. Modeling and Optimizationin Mobile, Ad Hoc, and Wireless Networks (WiOPT'09), Piscataway, NJ, 2009, pp. 376–380, IEEE Press.

[15] J.W. Yoon and H. Kim, "A perfect collision-free pseudonym system,"IEEECommun.Lett., vol. 15, no. 6, pp. 686–688, Jun. 2011.