International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

SECURING CONTENT BASED PUBLISH/SUBSCRIBE SYSTEM BY ADAPTING PAIRING BASED CRYPTOGRAPHY MECHANISM

ROHITH VAIDYA K[1], NAGARAJA HEBBAR N[2]

[1]M.Tech Student, Department of Computer Science & Engineering, Visvesvaraya Technological University,Belgaum, Karnataka, India

[2]Associate Professor, Department of Computer Science & Engineering, Visvesvaraya Technological University, Belgaum, Karnataka, India

Article Received: 11/03/2015

Article Revised on; 15 /03/2015

Article Accepted on:19/03/2015

ROHITH VAIDYA K

ABSTRACT

Security is one of the extensive and complicated requirements that need to be provided in order to achieve few issues like confidentiality, integrity and authentication. In a content-based publish/subscribe system, authentication is difficult to achieve since there exists no strong bonding between the end parties. Similarly, Integrity and confidentiality needs arise in published events and subscription conflicts with content-based routing. The basic tool to support confidentiality, integrity is encryption. In this paper for providing security mechanism in broker-less content-based publish/subscribe system we adapt pairing-based cryptography mechanism. In this mechanism, we use Identity-Based Encryption (IBE) technique to achieve the needs of publish/subscribe system. This approach helps in providing fine-grained key management, effective encryption, decryption operations and routing is carried out in the order of subscribed attributes.

Keywords—*Identity Based Encryption (IBE), Key server, Credential, Publish/Subscribe, Content-Based.*

©KY Publications

I. INTRODUCTION

General requirement for any system is security. The need for security must be extremely high. It is one of the major requirements to protect or control any sort of failures. There are number of mechanisms which are available to provide security. In that one of the most important mechanisms is encryption. In cryptography encryption is the process of converting plain text to cipher text which is unreadable from unauthorized users. The cryptography mechanism is required in publish/subscribe system.

In publish/subscribe system publisher is one who publishes his content without specifying a particular destination to reach publisher will not program the documents to be delivered to a particular subscriber. Publisher will classify publishing documents based on different criteria and release it and subscriber will show interest on one or more documents and subscribe to that particular one in order to have access over it. This publish/subscribe system is traditionally carried out in broker-less [12] content based routing which forwards or routes the message based on the content of the message instead of clearly routing to an specified destination. Content based routing applies some set of rules to its content to find the users who are interested in its content. Its different nature is helpful for huge-level scattered applications and also provides a high range of flexibility and adaptability to change.

Authorized publisher have permission to publish events in the network and similarly subscribers who likes the content can gets subscribed to an particular published content and have access over it by which high level access control [7] can be achieved. Here published content should not be exposed to routing infrastructure and subscribers should receive content without leaking subscription identity to the system, which is a highly challenging task which needs to be carried out in content-based pub/sub system.

Publisher and subscriber are the two entities and they do not trust each other. Even though authorized publisher publish events, nasty publisher pretend to be the real publisher and may spam the network with fake and duplicate contents similarly subscribers are very much eager to find other users and publishers which are challenging tasks. Finally, Transport Layer Security (TLS) or Secure Socket Layer (SSL) is secure channels for distributing keys from key server to the required.

Existing security approach deals with traditional network and security is based on restricted manner which tells about key word matching [8]. Key management was the challenging task in the existing approach, so to overcome all these, we use new approach called pairing-based cryptography mechanism, which helps in mapping between to end parties so called cryptographic groups. Here, Identity Based Encryption Technique (IBE) [9] is used under this mechanism. New approach IBE provide greater concern towards authentication and confidentiality in the network. Our approach permit users to preserve credentials based on their subscriptions. Secret keys provided to the users are labeled with the credentials. In Identity-based encryption (IBE) mechanisms 1) key can be used to decrypt only if there is match between credentials with the content and the key; and 2) to permit subscribers to check the validity of received contents. Moreover, this approach helps in providing fine-grained key management, effective encryption, decryption operations and routing is carried out in the order of subscribed attributes.

II. LITERATURE SURVEY

Broker in a network [2],[3] which is considered as the trusted third party in the publish/subscribe system. It has got several advantages and disadvantages in the system. It can have a fixed topology or a unfixed topology. In fixed topology it enables the system administrator to construct trusted domains and in that way progress the efficiency of routing by avoiding unnecessary encryptions. An unfixed topology permits the broker network to dynamically re-organize itself when brokers join or leave the network. An event user has to maintain a link to a local event broker, which then becomes publisher-hosting, subscriber-hosting, or both. Subscription privacy in broker network is subscribers would like to keep their subscriptions private from the forwarding brokers, as these force disclose their business policy. All the interactions is passed through the broker. Application will not have any idea about the other application. Only network address of the broker need to be known for the interactions. Broker routes the message to the exact location. Publisher can inject the message to the system and terminate. Subscriber can receive message with the help of broker at any time. If application failure occurs content may be stored in the broker itself. It may misuse the content also. Drawbacks of broker model are requires large amount of network for communication and since all the message need to be passed through the broker it results in bottleneck of the entire system.

The most basic alternative of the publish/subscribe model is topic-based publish/subscribe [4]. In this, Publisher publishes event based on the topic. Similarly, subscriber will subscribe to the interested topic published by the publisher. Hence in group communication topics are seen in groups. So it is simple and efficient. There exists disadvantage in subdividing the event space into topics that it is rigid and may lead to subscribers having to filter events coming from general topics. Some topic-based publish/subscribe systems ease this effect with hierarchical topics that help structure the topic space. A disseminated performance of a topic-based publish/subscribe system is the Information Bus. On a logical information bus that links publishers with subscribers events are published.

In Access control lists (ACL) user is authenticated, than user is permitted for right to use an application or not depending on whether that users is authorized or not. It is highly coarse-grained from that viewpoint. Methods for providing access control [5] on named categories that are typically arranged as a category tree. In a category tree the children of a node gives the more complete data about the same topic than its parent and thus may be considered more confidential. Even though it provides more information it lacks in security purpose. Since it uses coarse grain epoch-based key management and cannot provide fine grain access control in a scalable manner.

Private matching [5] is the foundation of the protected search for and secure table construction primitives is a matching process using encrypted data. Private matching has been brought for correspondence matches and total to more broad settings. But watchful revise of the trouble shows that there is a slight but vital distinction among private matching and the necessities of our scheme. Private matching is Privacy-Preserving Content-Based Publish/Subscribe Networks really a two-party procedure between publisher and subscriber where the subscriber learns at the end the information that he shares with the server. Substring matching [6] is the most significant process implemented on strings in common CBPS architectures. The plan is to crack the string into words and construct a Bloom filter to signal reality of a word in the string. The subscription is a single keyword.

III. SYSTEM ARCHITECTURE

In this paper we come across Content-Based [10],[11] model for routing, that is published contents from the publishers to the appropriate subscriber we use content based model. Each event consists of a overall ordered set of attributes (A). For example attributes are of unique name, types of data, and its field. An event will have set of attributes and related standards. An event is matched next to a subscription, if the standards of attributes in the event suit the equivalent constraints required by the subscription. For the better and efficient confidentiality and authentication we use Identity Based Encryption (IBE) which is technique comes under pairing based cryptography mechanism which is the most efficient mechanism for provisioning of authentication and confidentiality.

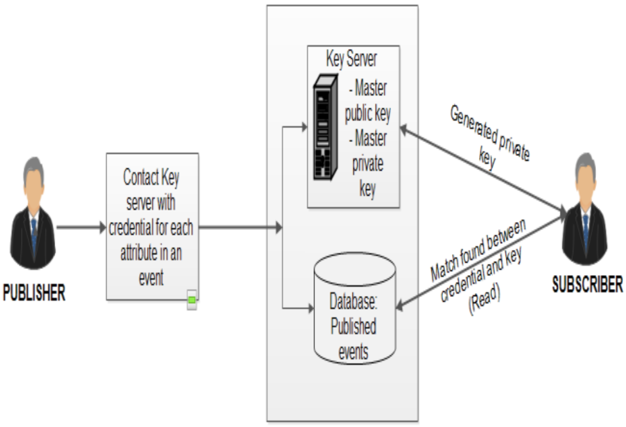

Key Server
- Master public key
- Master private key
Contact Key server with credential for each attribute in an event
Database: Published events
PUBLISHER
SUBSCRIBER
Generated private key
Match found between credential and key (Read)

Fig. 1. System Architecture.

Identity-Based Encryption (IBE) provides a good substitute method to decrease the amount of keys to be managed. In identity-based encryption, user's identity which is a valid string can be considered as the public key of the user. A pair of master public key and master private key is maintained by the key server. Sender sends the encrypted message to a user with user's identity with the help of master public key. User in order to decrypt the message sent by the sender needs to obtain a private key for user identity Fig. 1. shows the clear view of identity-based encryption, whose properties are for extremely disseminated applications.

For communication a sender needs to know about a single master public key with an unique identity likewise, to have the access over the message receiver needs to obtain private keys for its identity from the key server. In addition, an case of central key server can be simply fake inside the network. At last, a single pair of master keys maintained by the key server and hence which can be realized as a smart card provided to the user who are going to participate in the system. IBE comes under pairing-based cryptography which maps two cryptographic groups.

For security mechanisms in publish/subscribe, we influence the ideology of identity-based encryption to carry more and more communications between subscribers and publishers. In IBE, publishers and subscribers act together with a key server Pub/sub give credentials to the key server to receive keys which fit for their suitable credentials. Then, for encrypt/decrypt those keys are used, and mark applicable contents in the content based pub/sub system, that is the credential becomes certified by the key server. Credential consists of binary string and a proof for its identity. Credential is used for verification against the key server and verifies the identity of the end user. The keys will be in cipher text format which are labeled with credentials assigned to publishers and subscribers. The identity-based encryption tells that in order to decrypt a message using particular key there should be match between the credentials of the cipher text and the key. Separate private keys for each authorized credential are maintained by publisher and subscriber. By a string concatenation of a credential, an epoch for key revocation, a symbol € {SUB; PUB} distinguishing publishers from subscribers the public keys are generated. Without contacting the key server or other peers in the system the public keys can be simply generated by any peer. Similarly, encryption of events and their verification using public keys do not require any interaction which is done by their own.

Since there is loose coupling between publishers and subscribers, a publisher does not know the set of appropriate subscribers in the system. Therefore, a published event is encrypted with the public key of all likely credentials, which authorizes a subscriber to effectively decrypt the event. The cipher texts of the encrypted event are then signed with the private key of the publisher.

The whole network is maintained based on the subscriptions done by the subscribers and subscriptions with common events are placed close to the root in the hierarchy and events are forwarded to the subscribers with less common events. Every subscribers need to know about the subscriptions of the parent and child peers in the hierarchy. In this IBE approach subscribers identity and the relationship between subscriptions are not leaked to the system and thus confidentiality can be achieved successfully

IV. EXPERIMENTAL SETUP AND RESULTS

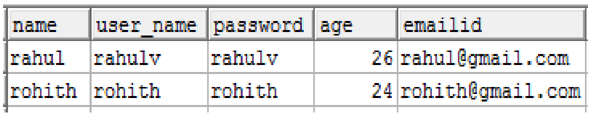
Here we examine few outlook of our system: 1) find the throughput of cryptographic primitives, 2) computation time for publisher and subscriber, 3) average CPU utilization. Evaluation are carried out based on subscriptions having different attributes defined d=14. The security mechanism used here is pairing-based cryptography. In the Table 1, column throughput shows various cryptographic primitive operation to perform encryption, decryption, verification, signature. Here identity based encryption is used to encrypt a random key, later which is used to decrypt the event based on the symmetric encryption. In the Table 1 column computation time indicates the computational time needed for publisher and subscriber in the system and finally the last column shows the average CPU utilization for publisher and subscriber.

TABLE 1: Performance evaluation and results

Operations	Throughput	Computation Time (msec)	Avg CPU Utilization (%)
Encryption(E)	12KB/sec	82.5	3.66
Decryption(D)	12KB/sec	88.48	3.836
Verification(V)	54 verify/sec	19.314	0.83042
Signature(S)	160 sign/sec	91.6	3.71

In this paper, in order to show the experimental setup for the working of Identity-Based Encryption we use IDE net beans and coding language used is java. In order to show the information stored related to publisher, subscriber, contents and subscription details we use my sql database. In the initial stage if a publisher wishes to publish the content, needs to get registered to a particular valid website as shown in example Table 2. In the table shown below we can the details of registered publisher with name, username, password, email id etc. They are meant to be authorized publisher and so they will have the authority to publish their content.

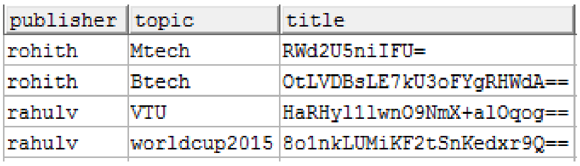
TABLE 2. Example Publisher Registered details



name	user_name	password	age	emailid
rahul	rahulv	rahulv	26	rahul@gmail.com
rohith	rohith	rohith	24	rohith@gmail.com

Once registered, then in order to publish the content, publisher needs to login and inject information into the pub/sub system by encrypting the plain text to cipher text as shown in example Table 3. In the table shown below we can see the published content in the encrypted format. A unique secret key is generated for each publishers content.

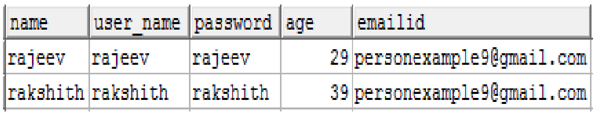
TABLE 3. Example Publisher published content in encrypted format



publisher	topic	title
rohith	Mtech	RWd2U5niIFU=
rohith	Btech	OtLVDBsLE7kU3oFYgRHWdA==
rahulv	VTU	HaRHy111wnO9NmX+alOqog==
rahulv	worldcup2015	8o1nkLUMiKF2tSnKedxr9Q==

By the time publisher publishes the content using the public key, key server will generate the private key randomly upon the published content. On the other end same as the publisher; subscriber needs to get registered as shown in example Table 4. In the table shown below we can the details of registered subscriber with name, username, password, email id etc. They are meant to be authorized subscriber and so they will have the authority to subscribe for the published content.

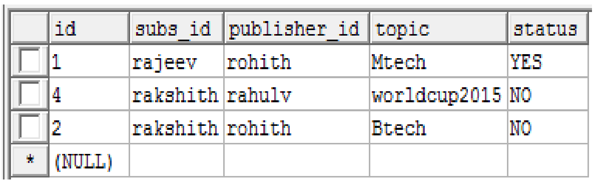
TABLE 4. Example Subscriber Registered details



name	user_name	password	age	emailid
rajeev	rajeev	rajeev	29	personexample9@gmail.com
rakshith	rakshith	rakshith	39	personexample9@gmail.com

And after login to the valid website end user gets to know about the publisher in the form of advertisements. If the subscriber likes the publisher advertisement, get subscribed to the particular advertisement. Upon subscription based on it another private key is generated. Once the subscription is done successfully as shown in example Table 5. In the table shown below we can see the status of the subscribers subscriptions, that is permission granted to access the content or not.

TABLE 5. Example Subscribers subscription details



	id	subs_id	publisher_id	topic	status
□	1	rajeev	rohith	Mtech	YES
□	4	rakshith	rahulv	worldcup2015	NO
□	2	rakshith	rohith	Btech	NO
*	(NULL)				

Publisher will get to know about number of subscribers subscribed for its content and hence publisher will have the authority to give the permission to the subscribers. If permission is given by activating the subscriber, key server will share the key with the particular subscriber via e-mail. Using that key subscriber needs to enter the key into an key field in order to decrypt the message or content and have the access over it. Subscriber can decrypt the message only if there is a match between the credentials associated with the content and the key provided by the key server.

V. CONCLUSION

In this paper, we have presented broker-less approach in content based publish subscribe system for providing authentication and confidentiality. The approach is extremely good for number of subscribers and publishers in the system and the number of keys maintained by them. The keys will be in cipher text format which are labeled with credentials assigned to publishers and subscribers. We adapted techniques from Identity-based encryption (IBE) mechanisms 1) key can be used to decrypt only if there is match between credentials of cipher text and the key; and 2) to permit subscribers to check the validity of received contents.

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

[3] L.I.W. Pesonen, D.M. Eyers, and J. Bacon, "Encryption-Enforced Access Control in Dynamic Multi-Domain Publish/Subscribe Networks," Proc. ACM Int'l Conf. Distributed Event-Based Systems (DEBS), 2007.

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

[5] 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.

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

[7] 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.

[8] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT), 2004.

[9] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, 2001.

[10] H. Khurana, "Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems," Proc. ACM Symp. Applied Computing, 2005.

[11] C. Raiciu and D.S. Rosenblum, "Enabling Confidentiality in Content-Based Publish/Subscribe Infrastructures," Proc. IEEE Second CreatNet Int'l Conf. Security and Privacy in Comm. Networks (SecureComm), 2006.

[12] M.A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, "Providing Basic Security Mechanisms in Broker-Less Publish/ Subscribe Systems," Proc. ACM Fourth Int'l Conf. Distributed Eventt- Based Systems (DEBS), 2010.