ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Provisioning of Authentication and Confidentiality for Content Based Publish/Subscribe System

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

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

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

ABSTRACT: In today's era, messaging plays a very important role in every aspect. One such a messaging system is Publish/Subscribe system. Publish/Subscribe System becomes a prominent communication medium for distributed environment. It allows publishers to publish messages/events and subscriber has the provision to receive the same as per their subscription. Presently, such messaging systems uses broker as a middleware to communicate between two parties.The main drawback of such a system is broker failure at any time leads whole system down. To remove this bottleneck, the proposed system is provided with the broker-less architecture for the content based publish/subscribe system. Here, publisher and subscriber are loosely coupled and having no trust on each other. In this case, it is difficult to achieve security mechanisms such as authentication and confidentiality. The proposed system uses new approach to achieve authentication and confidentiality in a content based and having broker-less publish/subscribe system using the identity based encryption.

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

I. INTRODUCTION

With the rapid development of web technology, there is rise in the information sharing between the people using different ways and entities. These entities are nothing but the human being. The entities are distributed globally, so their location and behaviour becomes vary. It requires highly efficient and reliable ways of information sharing to bring these distributed entities more closely and to make them scalable. The distributed entities are uncountable and hence, challenging to handle. The peer to peer and synchronous communication models are unable to satisfy these requirements. The publisher/subscriber system is an asynchronous messaging system which is gaining highest popularity because of its inherentunlinking characteristic. In this, event producers (publishers) shares information with the event consumers (subscribers). System infrastructure types are topic based systems and content based systems. Itfocusing on content based systems. The use of decoupling feature is to keep publishers to be unknown from subscriber regarding time, space and synchronization. Using publish/subscribe system publishers sends information and subscribers registers to get liking messages/events using subscription.Unknowingly, messages are routed to the relevant subscribers [1].

Traditional systems uses broker as a middleware to transfer the events/messages from publishers to subscribers. Such systems can be vulnerable to security attacks. At the time of routing, the broker can read the plain text information and hence, can be malicious. Also, broker failure badly affects the whole running system. Therefore, it's a challenge to secure a publisher/subscriber system. To address this problem, an event forwarding overlay is used [3] in recent system having a broker less publisher-subscriber architectures.

Subscribers have to subscribe the event first and then can receive the published events. The ways of specifying the subscriptions are Topic Based Subscription and Content Based Subscription. Topic based subscription, allows one particular topic to be specified and all the relevant events to that topic will be sent to the related subscribers. Topic

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

based model does not have restriction on the message content. The most expressive model is content based subscription model. In this, message contents can have restrictions or constraints defined by the subscribers. Content based subscription model is useful for large scale distributed applications such as environmental monitoring, stock exchange, news distribution, public sensing and traffic control. Considering thecharacteristics such as expressiveness and asynchronous, proposed system uses content based model.

Security of system is one major challenge to address. For this, to propose a novel approach with authentication and confidentiality to achieve security in a broker less publish subscribe system. Using this new approach all the subscribers can maintain their credentials according to the subscription. Private keys associated with the subscribers are also labelled with the credentials. The credentials can be numbers or string attributes. Each encrypted event is to be map 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. RELATED WORK

This section discusses previous research papers considering the traditional broker architecture. Previous papers mainly focuses on the scalability and expressiveness characteristics of the system but does not considers the security aspect fully. The proposed system majorly focus on the security. Following paragraphs provide brief review of previous research papers.

A Ciphertext Policy Attribute Based Encryption system [4] kept the encrypted data secret even if the storage server is unsecure. The 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).

The broker system [5] presented in the paper allows each user to submit a list of subscriptions to a broker. Broker is responsible for routing data from publisher to the subscribers. But the message contents may be unsafe from the broker. This is the drawback of such system.

In a loosely coupled publish/subscribe system [6] applications interacts indirectly and asynchronously. There is a broker's 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.

It should also allow event filtering to route the events to intended subscribers. These are the weak points of existing systems.

An Event Guard framework [7] is for the construction of secure wide area pub-sub systems. Event Guard mechanisms provides the security guarantees, systems 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 publish-subscribe network design that recovers quickly from the difficult situations.

A set of security mechanisms [8] given in the paper allows privacy-preserving forwarding of the encrypted contents based on subscribers 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.

A content-based publish/subscribe system [9] 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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

The concept of "Hermes" [10] is described in the paper. It 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.

The first identity based signcryption scheme [11] 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 is 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

A. SYSTEM DESIGN:

This proposed system makes use of content based model for routing the published content from publisher to the appropriate subscriber. The message/event to be published has an ordered set of attributes. These attributes have a unique name, types of data and its field. The 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.

The pub/sub overlay proposed is similar to DPS system with modifications to ensure subscription confidentiality. For evaluate performance and scalability of the proposed pub/sub system only with respect to the security mechanisms and omit other aspects. In particular, to evaluate the performance of this system the overlay construction time and the event dissemination delays. To measure the average delay experienced by each subscriber to connect to a suitable position in an attribute tree. Delay is measured from the time a subscriber sends association request message to a random peer within the tree until the time the association is really established. The evaluations area unit performed just for one attribute tree. It shows that the common association time (delay) will increase with the quantity of peers within the system owing to the rise within the height of the attribute tree (each new hop will increase the network delay in addition as time to use security methods).

Input style is that the method of changing a user-oriented description of the input into a computer-based system. This style is very important to avoid errors within the information input method and show the right direction to the management for obtaining correct data from the processed system. it's achieved by making easy screens for the info entry to handle massive volume of knowledge. The goal of coming up with input is to form information entry easier and to be free from errors. The info entry screen is intended in such the simplest way that everyone the info manipulates may be performed. It also provides record viewing facilities.

When the information is entered it'll check for its validity. Knowledge is entered with the assistance of screens. Applicable messages are provided as once required in order that the user won't be in maize of instant. so the target of input style is to form input layout that's straightforward to follow.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

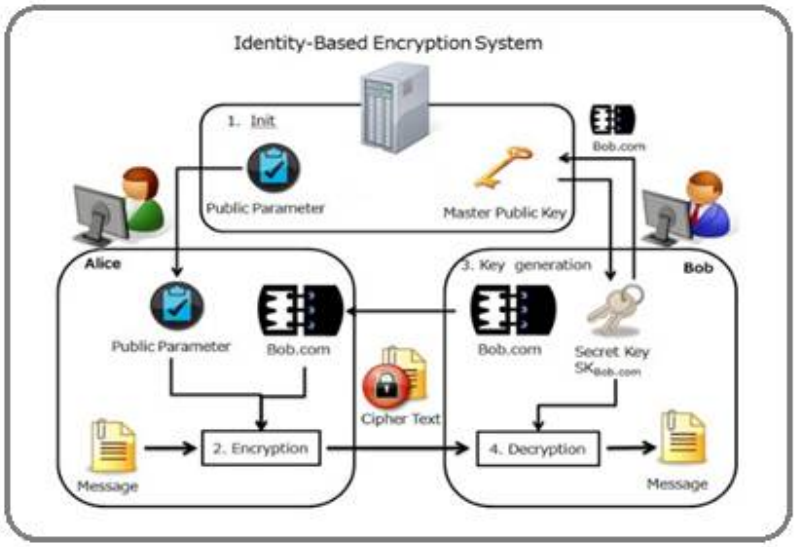

Fig.1 Identity Based Encryption mechanism

Proposed system uses the identity based encryption to provide the authentication and confidentiality in the broker less content based publish/subscribe system. Identity based 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 Fig. 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. Subscriber gets private key from key server to decrypt the message successfully.

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.

B. SYSTEM ARCHITECTURE:

The first step in planning package is to outline the design and include parts and layers of package. System design is that the abstract style that defines the structure and behaviour of system. Design may be a formal description of a system organized in a very manner that supports reasoning regarding the structural properties of the system. It defines the parts of the system or building blocks and provides an inspiration from that product will be procured. The system design is shown in Fig.2.

The above Fig.2 shows the System Architectureof Proposed System. The system consists of following basic modules which are listed and explain below in detail.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

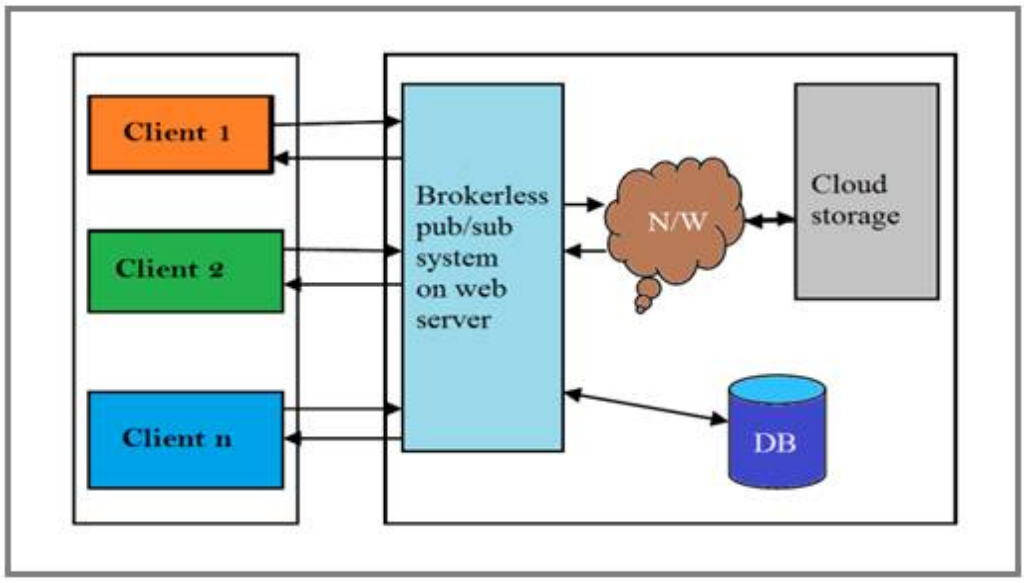

Fig. 2 System Architecture

- **Subscriber**: Subscribers are the client system, can able to register themselves and receive their access key.
- **Broker-less pub/sub system**: Broker-less pub/sub system is also known as gateway which is an intermediate between the publisher and subscriber.
- **Publisher:** Publisher will store the file in proxy server and accessed by authorized subscriber. Publisher specifies the access policy for each file, access policy is 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.

C. MATHEMATICAL MODEL

The proposed system S is defined as follows:
S: {I, E, O}
Where,
I = {I1, I2, I3, I4, I5}: A set of input to system
E= {E1, E2, E3, E4, E5}: an intermediate operation
D= {O1}: A set of output.

Input Set
I = {I1, I2, I3, I4, I5}:
Where,
I1=Graph Data.
I2=Publisher.
I3= Subscriber
I4= Credential.
I5= Query.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Intermediate Output Set.
E= {E1, E2, E3, E4, E5}
Where,
E1=Public Key
E2= Private Key.
E3= Credential Checking.
E4= Authentication.
E5=Process Query.

Final Output Set.
D= {O1}
Where,
O1= Result Graph.

Fig. 3 shows the Mathematical model of system using set theory.

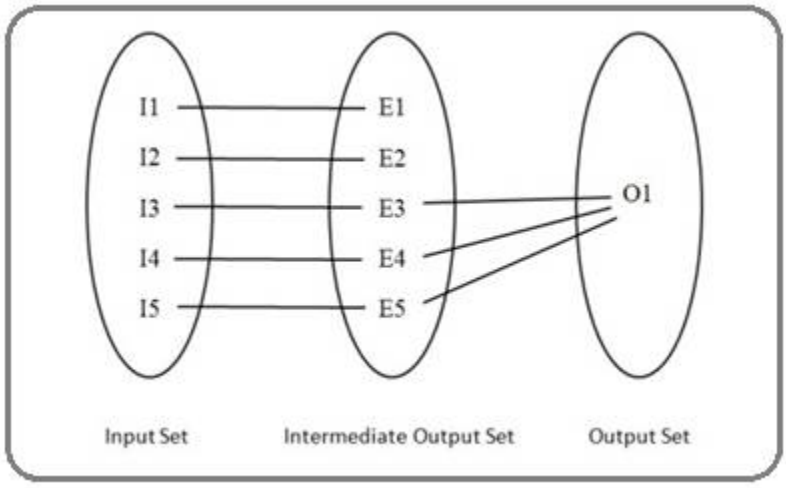

Fig.3 Mathematical Model

D. ALGORITHMS:

Algorithm 1. Secure overlay maintenance protocol at peer Sq.

1: upon event Receive (CR of s_{new} from s_p) do
2: if decrypt_request(CR)==SUCCESS then
3: if degree (s_q) == available then //can have child peers
4: connect to the s_{new}
5: else
6: forward CR to {child peers and parent} - s_p
7: if decrypt_request(CR)== FAIL then
8: if s_p ==parent then
9: Try to swap by sending its own CR to the s_{new}.
10: else
11: forward to parent

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

A $s_q$is a child peer which receives Connection Request (CR) of new subscriber s_{new} from the parent s_p only if the parent cannot adapt more children. If s_q sends its own CR to s_{new} if s_{new}'s credential is coarser than that of s_q i. e., s_q swaps its position with s_{new} (lines 7-9). However, if none of the children of parent s_p can connect or swap with s_{new}, then there is no containment relationship between the credentials of the children and s_{new}. In this case, a parent should disconnect one of its children to ensure the new subscriber is connected to the tree.

Algorithm 2:Message Digest algorithm

The algorithm used for Encryption and Decryption of messages/events is **MD5**. It is a Message Digest algorithm MD5 is a Message Digest algorithm which is quite fast and produces 128-bit message digests.MD5 is a quite fast algorithm.

The pseudo code for this algorithm such as:

1. Pad message so its length is 448 mod 512.
2. Append a 64-bit original length value to message
3. Initialize 4-word (128-bit) MD buffer (A,B,C,D)
4. Process message in 16-word (512-bit) blocks:

(a) Using 4 rounds of 16 bit operations on message block and buffer

(b) Add output to buffer input to form new buffer value

5. Output hash value is the final buffer value.

The time complexity of this algorithm is **O(n)** for content based publish/subscribe system.

IV. IMPLEMENTATION DETAILS

A peer to peer simulator [12] is used to perform the simulations of a system. The number of peers for Simulations areup to 2048 peers. For implementing security mechanisms the pairing-based cryptography library [13] is used. The complex subscriptions used during the evaluations contain conjunction of predicates defined on up to d= 16 different attributes.The implementation uses a 160-bit elliptic curve group based on the super singular curve $y^2 = x^3 + x$ over a 512-bit finite field.

V. RESULTS AND DISCUSSION

A publisher has each encrypted event with its own set of credentials. To accommodate identity based encryption mechanism a relative revision of the systems is presented here. Table 1 shows the Gains and Losses of various security systems. Every Encryption scheme has its advantages and disadvantages. According to the current scenario, it is observed that still there have a lot of challenges in publish/subscribe systems.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

Table 1
Encryption scheme

Encryption	Scalable Key Management	Access control	Subscription type
Symmetric	No	No	Content based
TLS	No	Yes	Content based
Asymmetric	Yes	Yes	Topic based
Asymmetric	Yes	No	Content based
Asymmetric	Yes	Yes	Content based
Asymmetric	No	Yes	Content based
Commutative	Yes	Yes	Content based
Symmetric	No	Yes	Topic based
SDE	Yes	No	Content based
Asymmetric	Yes	No	Content based
ABE	Yes	No	Content based
ABE,SDE	Yes	Yes	Content based
ABE	No	No	Content based
Asymmetric, Symmetric	Yes	No	Content based
Asymmetric, Symmetric	Yes	Yes	Content based

Performance of Publish/Subscribe System:

Fig. 4a to measures the average delay experienced byeach subscriber to connect to a suitable position in anattribute tree. Fig. 4a shows that the average connection time (delay)increases with the number of peers in the system because ofthe increase in the height of the attribute tree (each new hopincreases the network delay as well as time to applysecurity methods). Furthermore, Fig. 4a shows that there isan overhead of approximately 230-300 ms due to securitymechanisms.

Fig. 4b shows that for a fixed set of peers(i.e., 1,024 peers for this experiment), the average delayexperienced by subscribers decreases significantly with theincrease in out-degree mainly because the resultant disseminationtree is fat (i.e., tree with smaller height).

Fig. 4c measures the average time needed by the eventto be disseminated to all the relevant subscribers in thesystem. For each subscriber, the time is measured from thedissemination of the event by the publisher till it issuccessfully decrypted and verified by the subscriber.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

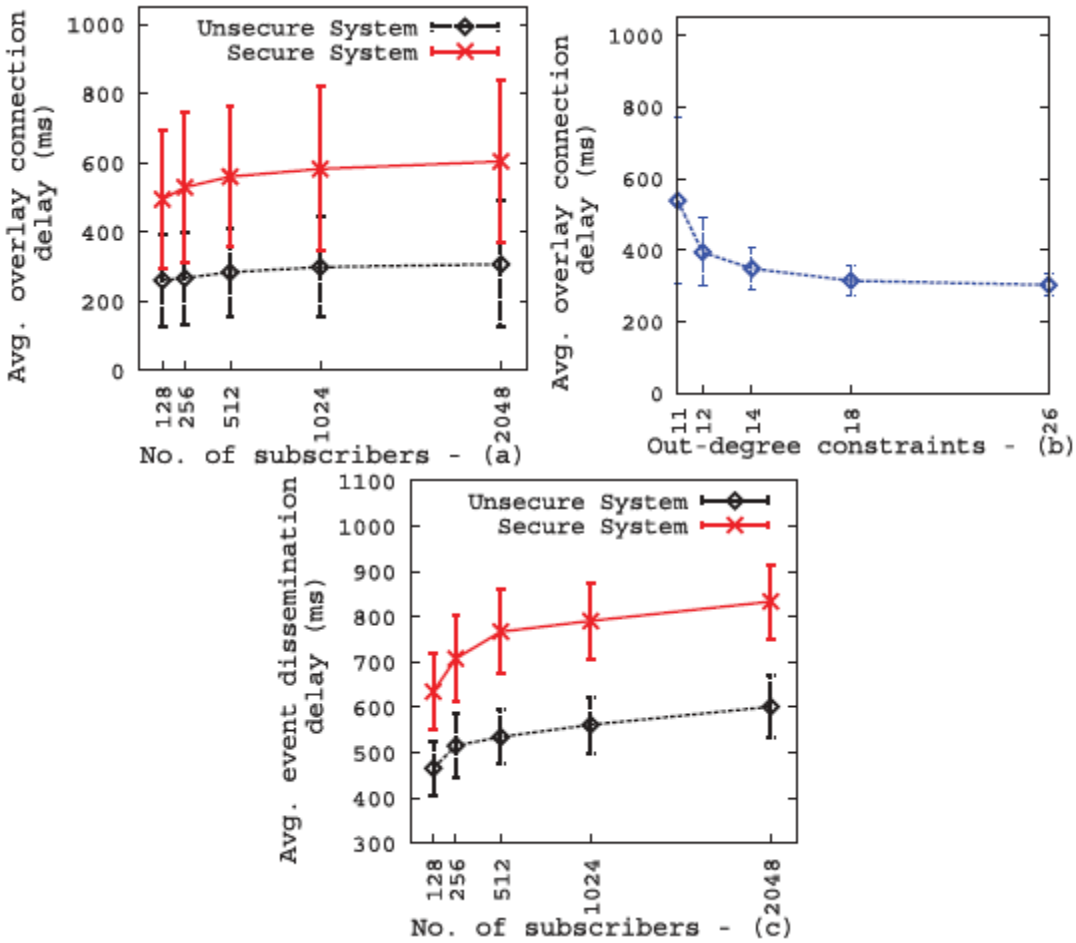

Fig.4Performance evaluations

VI. CONCLUSION AND FUTURE WORK

A wide area pub-sub system is often implemented as a collection of spatially disparate nodes communicating on top of a peer-to-peer overlay network. Due to the loose coupling between the publisher and subscriber, it is essential to address the security challenge of the system. To achieve this, proposed system 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, which can be used in Large-scale distributed applications such as news distribution, environmental monitoring, traffic control, and public sensing.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 11, November 2016

ACKNOWLEDGMENT

It's my pleasure to thank my project guide Prof. K. N. Shedge for his kind support and valuable guidance. He help me every time to improve the quality of project work in all respects. I am also thankful to the Head of Computer Engineering Department. I would like to thank my colleagues and friends who guide me directly and indirectly to complete the paper work. I would also thankful to all the staff members of Computer Engineering Department and Librarian, who gives their valuable guidance to me. Specially, I am thankful to my family members for their support and co-operation during this Project work.

REFERENCES

[1] Mühl, Gero, Fiege, Ludger, Pietzuch,Peter.Distributed Event-Based Systems[M].Springer,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] 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.
[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp.Security and Privacy, 2007.
[5] 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 Applications: Part I, 2010.
[6] 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.
[7] 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.
[8] A. Shikfa, M. O¨ nen, and R. Molva, "Privacy-Preserving Content- Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.
[9] 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 Distributed Event-Based Systems.IGI Global, 2010.
[10] P. Pietzuch, "Hermes: A Scalable Event-Based Middleware," PhD dissertation, Univ. of Cambridge, Feb. 2004.
[11] Y. Yu, B. Yang, Y. Sun, and S.-l. Zhu, "Identity Based Signcryption Scheme without Random Oracles," Computer Standards & Interfaces, vol. 31, pp. 56-62, 2009.
[12] M. Jelasity, A. Montresor, G.P. Jesi, and S. Voulgaris, "PeerSim: A Peer-to-Peer Simulator," http://peersim.sourceforge.net/, 2013.
[13] B. Lynn, "The Pairing-Based Cryptography (PBC) Library," http://crypto.stanford.edu/pbc/, 2010.