CONFIDENTIALITY AND AUTHENTICATION IN CONTENT BASED PUBLISH/SUBSCRIBE SYSTEM

Ms. Nileema R. Hiray (Author)[1], Prof.K.N. Shedge (Guide)[2]

[1,2] *Sir Visvesvaraya Institute Of Technology,*

Nashik,(India)

ABSTRACT

Publish/Subscribe System is Associate in emerging communication model that runs in distributed atmosphere. It'san electronic communication system, wherever the messages/events square measure revealed by publishers and received by subscribers supported their subscription. Within the existing electronic communication systems, broker acts as a middleware in between 2 parties and every one the communication is finished through the broker. During this case, the broker failure will be the bottleneck of whole system. To beat this disadvantage, there's a system planned that uses broker-less design for the content based mostly publish/subscribe system. In publish/subscribe system, publisher and subscriber square measure loosely coupled and don't keep trust on one another. So, the basic security mechanism like authentication and confidentiality is difficult to achieve and hence, a challenging task. The proposed system provides to achieve authentication and confidentiality in a broker-less content based publish/subscribe system using the identity based encryption.

Keywords :Brokerless(Non mediator), Content-based, Identity Scheme,Publisher, Security,Subscriber

I. INTRODUCTION

Internet is a rapidly growing and there is a need arise to transfer information between different entities. These entities are nothing but the human being. The uncountable entities are widely spread globally and hence their locations and behavior becomes vary. Therefore, to bring these distributed entities to be closer and to make them scalable, more efficient and reliable techniques are required for information distribution. The synchronous peer to peer communication models are not able to satisfy these requirements. So, the publisher/subscriber asynchronous messaging system has been experiencing highest popularity due to its inherent decoupling feature. This system allows distribution of information from event producers i.e. publishers to event consumers i.e. subscribers.

The publish/subscribe system's decoupling feature allows publishers to be unknown from subscriber with the aspects such as space, time, synchronization. Publishers transfers information using publish/subscribe system, subscribers registers events/messages of interest using subscriptions. Without knowing the subscriber details to publisher and vice versa the events are routed to the relevant subscribers [1].

In traditional systems, broker is used to route the events or messages from publishers to subscribers. This leads to security questions. Broker can be malicious while routing and can read the plain text information. Failure of

brokers can leads to the whole system down. So, providing security to the pub/sub system becomes a challenging task. To address this issue, recent systems come with a broker-less publisher-subscriber architectures. For this event forwarding overlay is used [3].

Subscribers can receive the published events only on the subscription of that event. There are two ways/models for specifying the subscriptions: 1) Topic Based Subscription 2) Content Based Subscription. In a topic based subscription, one particular topic is specified and all the events relevant to that topic are sent to the related subscribers. There is no restriction on the message content in the topic based model. Whereas, content based subscription model is the most expressive in nature. Using this model subscriber can define the restrictions or constraints on message contents. Content based model for subscription is helpful for large scale distributed applications such as environmental monitoring, news distribution, public sensing and traffic control. By considering the expressiveness and asynchronous characteristics, so there are using the content based model in our proposed system.

Now, the question of security comes in picture. To provide a security in a broker-less publish/subscribe systems a new approach with authentication and confidentiality is proposed. In this approach, according to the subscription all subscribers are allowed to maintain their credentials.

II. RELATED WORK

In this section, studied previous research papers related to the traditional broker architectures. These papers focused only on the scalability and expressiveness characteristics of the system but consider little aspects of security. The major focus on security is given while developing the proposed system. The brief review of previous research papers is as follows:

A. Sahai [11] presented a system having Cipher text Policy Attribute Based Encryption. Using this technique, the encrypted data is kept secret even if the storage server is unsecure.

S. Choi [4], presented a broker system. In this, each user submits a list of subscriptions to a broker. Broker is responsible for routing data from publisher to the subscribers. Publisher sends notification message (contains value) to the broker, if the value in the notification matches with the subscriptions then only broker will forward it to the subscriber. In most cases, data to be published is confidential and its contents must be safe from the broker. This is a challenging task for the future systems.

B. Crispo[5] presented a publish/subscribe system which is loosely coupled. In this system, applications interact 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.

L. Liu [6] presented an Event Guard framework 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 a publish-subscribe network design that recovers quickly from the difficult situations.

B. Maniymaran, [8] presented a content-based publish/subscribe system which 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. It can also filter, aggregate, correlate and direct any combination of historic and future data. Several applications are also presented in detail that can benefit from the content-based nature of the pub/sub system and take advantage of its scalability and robustness features. While developing large-scale distributed systems that are going to be used on the Internet, it should have a proper middleware support, to handle the communication needs of those application clients in a scalable and efficient way, and without loosing traditional middleware features.

P. Pietzuch [9] described the concept of "Hermes". 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.

B. Yang [10] invented the first identity based signcryption scheme. Their scheme 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 have seen above. It will focus on broker-less 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. 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.

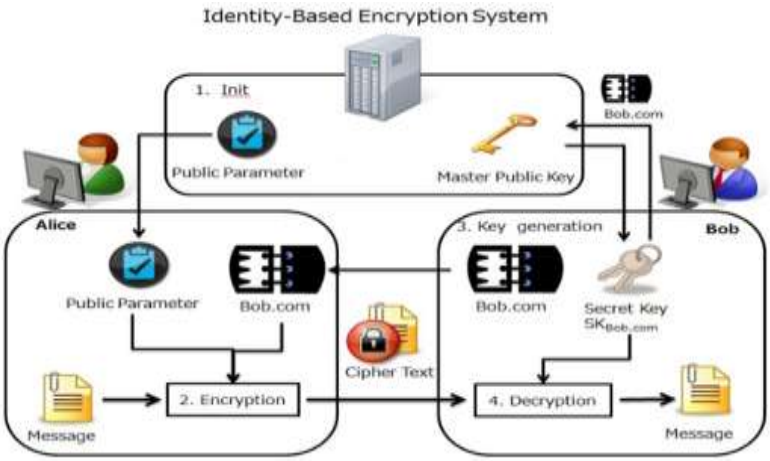

Fig.1 Identity Based Encryption mechanism

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.

IV. 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.

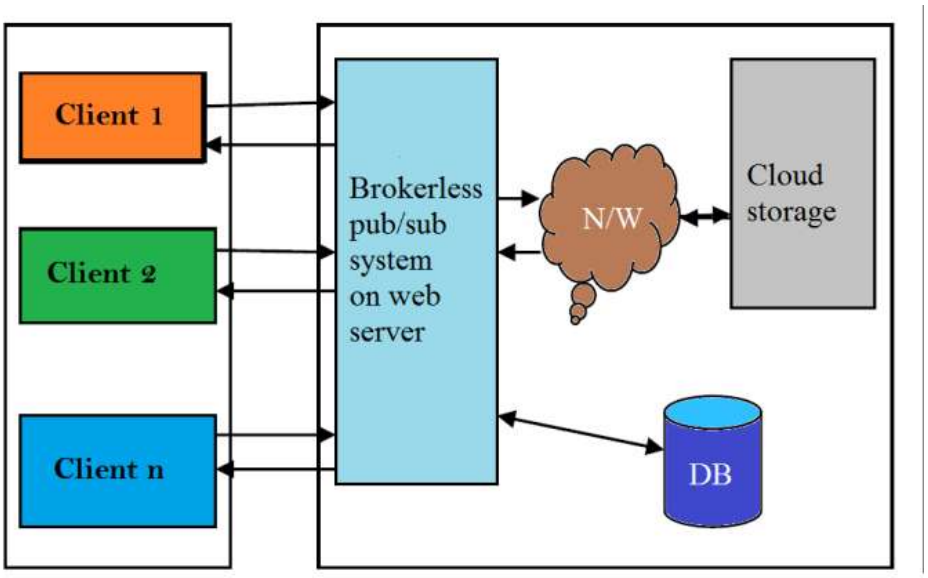

Fig.2 System Architecture

- **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.

V. IMPLIMENTATION DETAILS

5.1.Mathematical Model

Set Theory Let I be a set of Input to system and E is intermediate operation and D is setof output.

Input Set

I= {I1, I2, I3, I4, I5}

Where,

I1=Graph Data.

I2=Publisher.

I3= Subscriber

I4= Credential.

I5= Query.

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.

Following fig. 3 shows Mathematical model of system

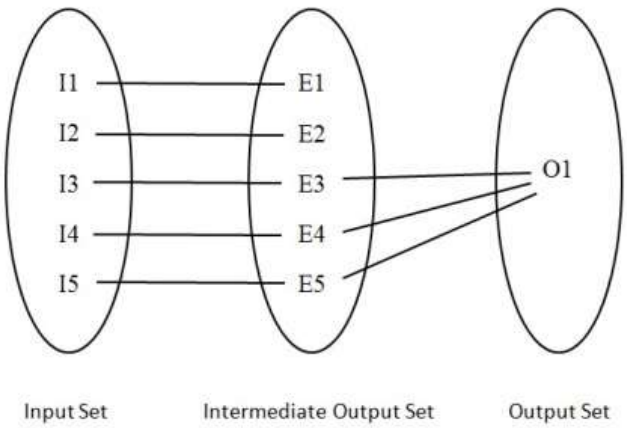

Fig.3 Mathematical Model

5.2 Algorithm

MD5 Algorithm used for Encryption and Decryption. MD5 is a Message Digest algorithm which is quite fast and produces 128-bit message digests.

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.

For this algorithm complexity is Big O (n) for content based publish/subscribe system.

5.3.Experimental Setup:

Simulations are performed using PeerSim [11]. Simulations are performed for up to N=2048 peers.The security mechanisms are implemented by the pairing-based cryptography library [14]. 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.

VI. RESULT AND DISCUSSION

A publisher associates each encrypted event with a set of credentials. To adapted identity based encryption mechanisms a relative revision of the systems is presented here. The Gains and Losses of various security systems are concluded in Table. Every Encryption scheme has its pros and cons. According to the current scenario, it is observed that still there have a lot of challenges in publish/subscribe systems.

The Data input the proposed system is operations on which are stored over network listed in following table.

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

VII. AKNOWLEDGEMENT

It is my privilege to acknowledge with deep sense of gratitude to my guide Prof. K. N. Shedge for him kind help and cooperation. Salutation to my beloved and esteemed institute for having well qualified staff and labs furnished with necessary equipment.Also I would like to thank my colleagues and friends who helped me directly and indirectly to complete this Paper. Lastly my special thanks to my family members for their support and co-operation during this Project work.

VIII. CONCLUSION

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.

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] 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.

[5] 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.

[6] 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.

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

[8] H.-A . J acobsen, A.K.Y. Cheung, G . Li, B. Maniymaran, V . Muthusamy, and R.S. Ka zemzadeh, "The PADRES Publish/Subscribe System," Principles and Applications of Distributed Event-Based Systems. IGI Global, 2010.

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

[10] 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.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, 2007.

[12] W. C. Barker and E.B. Barker, "Sp 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm Block Cipher," technical report, Nat'l Inst. of standards and Technology, 2012.

[13] Handore Jayshree Shrikant, Prof. Shivaji R. Lahane, "A Review on a Highly Scalable Privacy Preserving Content-Based Publisher/Subscriber System using Event Based Encryption," International Journal for Computer Science and Information Technologies, vol. 5 (6), 2014.

[14] H. Pang and K. Mouratidis, "Authenticating the query results of text search engines," Proc. VLDB Endow., vol. 1, no. 1, pp. 126–137, 2008.