RESEARCH ARTICLE OPEN ACCESS

Secure Brokerless System for Publisher/Subscriber Relationship in Distributed Network

Rupali Arun Jairange[#1], A. K. Gupta[*2]
[#] *Student, M.E. Computer, JSCOE, Pune, University of Pune*
[*] *Associate Professor, JSCOE, Pune, University of Pune*

ABSTRACT
Public subscribe systems are more attracted academic and industrial interest in last few years, including certain experiences of development and deployment. The primary requirements of security mechanisms such as authentication and confidentiality in content based publish subscribe system. This system consists of various types of brokers or agents where these brokers are organize their roles. These brokers are information or events are published by publishers and this information is received by subscribers and it depends on their subscription. Publisher and subscriber system is loosely coupled and asynchronous communication and this system is based on distributed system. Broker play vital role in business development and obtain by question mark over the trustworthiness of broker. The used of security coupled system for Brokerless is huge demand. In addition to our previous work [1], this paper contributes 1) Owner key generation 2) Time based key generation 3)Two tier key generation i.e. merging of owner key and time based key 4) Securely encryption techniques using reverse circle cipher encryption 5) Key management 6) Event distribution

Keywords: Publisher, Subscriber, Gaussian distribution, Reverse Circle Cipher.

I. INTRODUCTION

In the use of Internet technology and development of mobile computing, large scale computing as well as Internet of Things technology, a distributed system may contain thousands of nodes that may be distributed across different geographical locations and have different behaviors. These drawbacks make distributed systems need a more flexible communication model to adapt dynamic and scalability. Publish/Subscribe system is loosely couple and asynchronous communication and it is based on distributed system. Publisher insert the information in publish/subscribe system and subscribe establish the events of interest by means of subscriptions.

Financial information system, live feeds of real time data, cooperative working, pervasive computing, network monitoring, network monitoring, news distribution, stock exchange, health sector, traffic control and public sensing these are the application of Brokerless publish/subscribe system and these application used to provide the basic security requirements such as access control and confidentiality of the system.

Advantages of these systems are risk less brokering, secure bond between owner and broker, secure data delivery to end user, data privacy and secure key generation techniques.

Topic based and content based are two types of subscription model for establish the subscription. In topic based subscription model messages are published by their names logical channel. Subscriber collects those entire messages published to topic which they subscribe. In content based subscription model messages are hand over to the subscriber only when the messages are similar to constrains. Unique key is managed over the whole operation of the system and most important used proper key generation algorithms.

In reverse circle cipher technique is the core part of the proposed system and by using this technique we can encrypt key as well as decrypt key. There are many techniques to find generate cryptographic key such as time based and attribute based and that generated key is used encryption as well as decryption. Figure1 shows the reverse circle cipher algorithm.

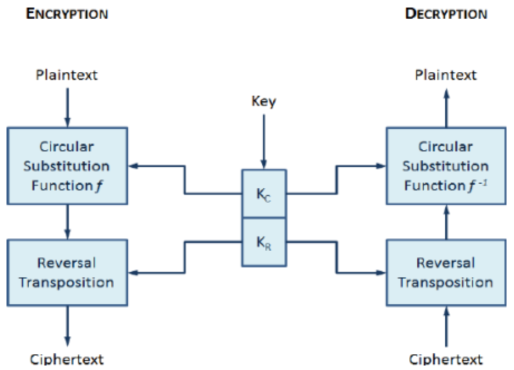

Fig.1 Reverse Circle Cipher Algorithm

Identity based encryption is one of the effective technique in publish/subscribe system and to reduce the number of keys managed. In this technique any valid string which uniquely identifies a user can be the public key of the user. A key server maintains a single pair of public and private master keys. The master public key can be used by sender to encrypt and send the messages to user with any identity, for example an e-mail address. To successfully decrypt the message, a receiver needs to obtain a private key for its identity from the key server. Figure2 show the identity based encryption.

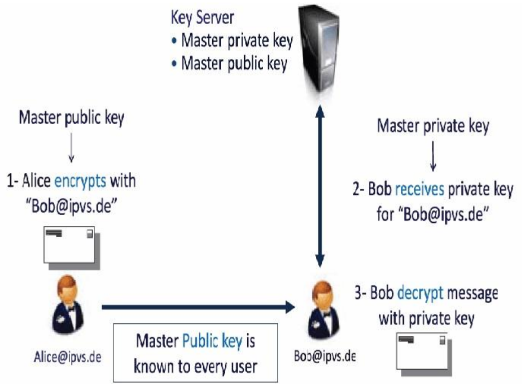
Key Server
• Master private key
• Master public key
Master public key
1- Alice encrypts with "Bob@ipvs.de"
Master private key
2- Bob receives private key for "Bob@ipvs.de"
3- Bob decrypt message with private key
Master Public key is known to every user
Alice@ipvs.de
Bob@ipvs.de

Fig.2 Identity Based Encryption

In Gaussian distribution technique data is distributed by appropriate publisher with high probability distribution of complex value depending on the threshold value. Gaussian distribution is also called as normal distribution and that technique is used easy to find out authorized and trustworthy publisher. Figure3 illustrates Gaussian distribution

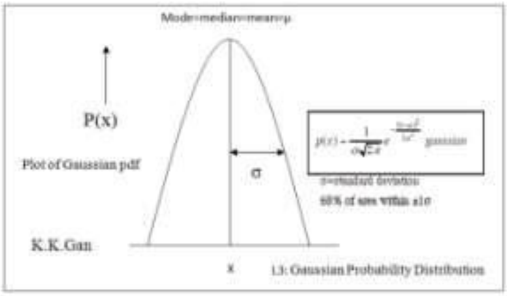

Fig.3 Gaussian distribution

The rest of the paper is organized as follows. Introduction is discussed in section I. literature survey related to this system are discuses in Section II. Proposed System is discusses in Section III. Conclusion is discussed in section IV.

II. LITERATURE SURVEY

Here literature survey is going to illustrates some of the previous works done by the researchers in same domain and also the supporting techniques used in our project. The literature survey related to this project is as follows:

Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel [1], this system explains identity based encryption and also used access key. This system implemented Brokerless system. They can also evaluate different attacks and developed a fine grained key management system. In identity based encryption all the communication is based on identity of the party. If someone can stole the identity then system data can arranged. For example if someone can be stolen the debit card and user also user know the pin number then user can debit some amount also. So this is the withdrawal of identity-based encryption. Solve this is in some aspect by using attribute-based encryption. The major drawback of this model is; it is using only credentials and attributes for the event publishing. If in any case these credentials are leaked then easily attacker can guess the keys to crack the system and relation between subscriber and publisher is not random. So this can cause serious threat to the system.

Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu [2], this system presents a general solution to the privacy preserving information sharing problem and using a coordinator system for brokering systems. Disadvantage of this system is that no inter coordinator communication there to protect system from malfunctioning.

Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi [3], they narrates the block cipher technique used in personal security such as data encryption standard (DES) and advance encryption standard (AES) both of them ineffective for real time data transfer. Reverse circle cipher algorithm uses encryption and decryption. In this papers study the performance of the algorithm against to the size of the plaintext and frequency distribution within the cipher-text and also replacement of character is applied on end of each rotation

Jean Bacon, David M. Eyers, Jatinder Singh, Peter R. Pietzuch [4], they elaborate broker based system and also used Role Based Access Control (RBAC) in this paper. In this model they developed the policy for publisher and subscriber according to their role. This system provides the work in securing publish/subscribe service in a MultiDomain.

J. Bethencourt, A. Sahai, and B. Waters [5], this system introduced complex access control techniques on encrypted data and that data is called as cipher-text policy attributed based encryption. In this technique the encrypted data is fully confidential even if the storage server is untrusted. It also support secure against collision attacks. This system based on Role Based Access Control. The advantages of this system are performance and reliability that means duplicated data can be stored on different locations. The drawback of this technique is that difficulty to support the security of data using traditional methods, where as data is stored at several locations.

Dan Boneh and Matt Franklin [6], this system describes fully functional Identity Based Encryption (IBE). It is based on the weil pairing and this system has chosen cipher text security in random oracle model assuming.

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters [7], this system describe a new cryptosystem for fine-grained sharing of encrypted data it is called as key policy attribute based encryption (KP-ABP). In this type of cryptosystem, cipher-texts are called as set of attributes and private keys and refer to associated with access structures that control cipher-text a user is able to decrypt. In this system maintains delegation of private keys which uses Hierarchical Identity-Based Encryption (HIBE). The difficulty of this system is encrypted data can be collectively shared only at a coarse-grained level.

Lauri I.W. Pesonen, David M. Eyers, Jean Bacon [8], they describe broker based system. This system communicate inter domain and this systems are called as a multi-domain system. Multi-domain means share a network in multiple organization or single organization.

Costin Raiciu and David S. Rosenblum [9], this system narrates the Content Based publish/subscribe networks. It maintains the notification and subscriber confidentiality. In this system there are so many limitations of confidentiality because of the broker based system. The attacks at down problem, finite in differentiate ability, confidentiality generality trade off and trust.

A. Shikfa, M. O nen, and R. Molva [10], this system describes Pohlig Hellman Cryptosystem, key distribution for secure routing and they used Multi-layer Commutative Encryption (MLCE).

Muhammad Adnan Tariq, Boris Koldehofe, Ala Altaweel, Kurt Rothermel [11], this system implements Brokerless publish/subscribe networks and current approach to provide authentication and confidentiality in Brokerless content based publish/subscribe network. Rekeying is drawback of this system. Rekeying means, when any subscriber can arrive or remove then keys of all the subscribers are regenerated.

III. PROPOOSED SYSTEM

Publish/Subscribe system contains two entities: 1) Publisher and 2) Subscriber.

Publisher who is going to insert the information into publish/subscribe system and subscriber it defines the events or action of interest by means of subscription Publish/Subscribe network is loosely coupled, Because of publisher and subscriber are unknown to each other. For smooth working, previously broker is used as a middle person. But there are lots of limitations and it needs extra security techniques to maintain authentication and confidentiality of data. Some broker-based systems are maintaining confidentiality by storing encrypted data in database. But still there is a limitation and trustworthiness issue.

After this publish/subscribe network is implemented by without direct help of broker, so this system is called as broker less publish/subscribe network. This system is implemented with the help of identity based encryption technique. Security is important in publish/ Subscribe network, first only authorized publisher can publish their event and only authorized subscriber can allowed to access that event which they subscribe for the same. Secondly the data is not available or access to any other subscriber that is called as confidentiality. These security issues are make a challenges to create highly secure publish/subscribe network.

3.1 System Overview

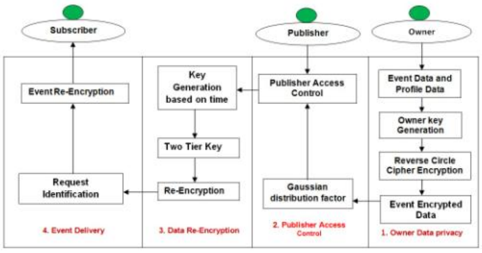

Fig.4 System Overview

System Architecture is nothing but the block diagram of the project. In this diagram, it shows the overall working of the project. Secure broker less system for publisher/subscriber relationship in distributed network is very secure approach in cryptographic techniques. Here, describe secure Brokerless system for publisher/subscriber relationship in distributed network with the below mention steps.

Step1: Owner inserts all the parameter into the system. Then by using owner data and profile data key will be generated. This generated key is called as owner key generation or random key generation.

Step2: In this step owner data is provided by the owner and that data encrypted by the secure cipher technique called reverse circle cipher algorithm.

Step3: Owner data has been distributed to different publisher. It is based on Gaussian distribution model (GDM). It considers the distribution parameter as the number of the published events by the publisher.

Step4: Publisher for whom the event it been assigned by the owner. Create two-tier key which is derive from time based key along with owner key, By using two tier key encrypted data has been re-encrypt again and it is controlled both owner and publisher.

Step5**:** Published data can be view by the subscribers, then they request for the same to the publisher. This data with the new two tier key has been served to the subscriber, which eventually decrypt using reverse circle cipher decryption technique to deliver plain text owner data to the subscriber.

3.2 Mathematical Model

The whole proposed system is expressed mathematically in the below model.

Mathematical Model

1. Let S= { } be as system for Broker less Subscriber request
2. Identify Input as R={ Rq}
Where Rq=Subscriber Request
S= {R}
3. Identify E as Output i.e. Event Data
S= {R, E}
4. Identify Process P
S= {R, E, P}
P= {Kg, Gd, Ka, Rcc}
Where Kg = Key Generation
Gd =Gaussian distribution
Ka= Key Assignment
Rcc =Reverse cycle Cipher
5. S = {R, E, Kg, Gd, Ka, Rcc}
The union of all subset of S gives the final proposed system.

3.2.1 Random Key Generation

$$f(x) = \sum_{i=0}^{n} U_i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

f(x) = user credential concatenation function
n=no of attributes
U_i =profile attribute
n=no of words in query

$$P_{k=}\ P\,(f(x)) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

$P_{k=}$ private key
P (f(x))= random key generation function

3.2.2 Gaussian distribution Equation

$$P(y) = \frac{1}{\sigma\sqrt{2\pi}}\ e^{-(y-\mu)^2} / 2\sigma^2 \ \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

μ= mean of distribution
σ^2 = variance of distribution
y= continuous variable
P(y) = probability of y

3.3 Proposed Algorithms

a) Random Key Generation Algorithm

Input: Set U = $\{u_1, u_2, u_3\ldots\ldots u_n\}$
Output: Random Key (R_k)

```
Step 0: Get the User Profile attribute set U
Step 1: Convert all the attributes to String type
Step 2: Concatenate all the String to get a single String
Step 3: Get the auto incremented User ID as I
Step 4: x=ID mod 7
Step 5: For I=0 to String length
Step 6: Fetch x^th character from the String
Step 7: Continue till 7 characters are selected
Step 8: Concatenate all the 7 characters
Step 9: Return key
Step 10: Stop
```

In random key generation algorithm uniqueness is maintained in new events created by owners and this key having 7 characters in length.

b) Reverse Circle Cipher Algorithm

```
Step 0: Start
Step 1: Get Input String S
Step 2: Initialize a String ENC as empty
Step 3: Divide the string S in N blocks of size 10 characters
Step 4: For I =1 to N
Step 5: Let String BS =10 character of each block
Step 6: Rotate block with I characters in clock wise
Step 7: For I=1 to 10
Step 8: Substitute each character
Step 9: Replace character
Step 10: End of inner for
Step 11: ENC=ENC+BS
Step 12: End of Outer for
Step 13: Stop
```

In reverse circle cipher algorithm data has been divided into blocks which are been indexed to send for the further rotation based on the index value. Then each n character is been rotated based on the index value of the block. This cipher technique produces secure encryption technique over the network.

IV. CONCLUSIONS AND FUTURE SCOPE

Proposed system is efficiently handling the randomly generated keys based on the information provided by the subscriber during the event requisition form the publisher. Here keys are generating by permutation of the characters in run time based on the subscriber requests entities. Again System successfully maintains the key distribution scenario by using Gaussian distribution model. Finally to maintain the privacy of the data over the distributed paradigm system uses secure cipher technique in network like reverse circle cipher. At the end the whole system is tightly coupled to handle number of subscriber requests in run time with proper event publishing schemes.

In future scope the proposed system can be upgrade to develop in heterogeneous network of internet of things using cluster based hierarchy. This makes the system to access perfectly in all possible types of network. System can be developing to maintain multiple hierarchies of the broker and owners.

ACKNOWLEDGMENT

We thank anonymous referees whose comments improved this paper.

REFERENCES

[1] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel, "Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption," Proc IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.

[2] Fengjun Li, Bo Luo, Pang Liu, Dongwon Lee, and Chao-Hsien Chu, "Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing", June2013.

[3] Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi, "Reverse Circle Cipher for Personal and Network Security" .ebeisaac@gmail.com, 2013.

[4] 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.

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

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

[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), 2006.

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

[9] 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.

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

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

[12] W. C. Barker and E .B. Barker, "SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," technical report, Nat"l Inst. of Standards & Technology, 2012.

[13] Sasu Tarkoma, Publish / Subscribe Systems: Design and Principles, John Wiley & Sons, 18-Jun-2012.