International Journal of Technical Innovation in Morden Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 3, Issue 4, April-2017

Implements Brokerless Security System for Publisher/Subscriber Interrelation in Distributed Network

Rupali Arun Jairange[1], Prof. A. K. Gupta[2]

[1] Student, M.E. Computer Engineering, Jayawantrao Sawant College of Engineering, Pune
[2] Professor, M.E. Computer Engineering, Jayawantrao Sawant College of Engineering, Pune

Abstract*— Security is one of the wide ranging and problematic requirement that use to be maintaining in order to manage few problems like confidentiality, integrity and authentication. In a content-based publish/subscribe system; authentication is challenging to manage since there are no secure connections between the end parties. Similarly, an Integrity and confidentiality need occurs in published events and subscription conflicts with content-based routing. In this paper based for implement security system in Brokerless content based publish/subscribe system we modify pairing based cryptography system. In this system, we use Identity Based Encryption (IBE) technique to manage the needs of publish/subscribe system. This helps in maintain fine-grained key management encryption, decryption operation and routing is carried out in the order of subscribed attributes.

Keywords*— Publisher, Subscriber, Identity Based Encryption, Gaussian distribution and Reverse Circle Cipher.

I. INTRODUCTION

Many of the event publishing system are not over perform due to lack of market holding. So these types of system even though on having higher technical assets are unable to deliver their best in the business. So they need to relay on third party brokers. Brokers are the inter mediators who are having the greater assets on the subscriber side as well as on the publisher side in the business. But the main issue in the whole scenario is trust; it is always difficult to trust brokers in the business. As broker can take advantage of the past data in the future, this may cause in losing of clients for the business and also may spoil the reputation. So it is always a challenging job to maintain a strict broker less publish / subscribe system with greater privacy for the data. To achieve this secure key generation techniques is required to maintain the data distribution system with secured cipher technique in the distributed paradigm.

There are several application used to provide basic security mechanisms access control and confidentiality of the system also used Brokerless publish/subscribe system. These applications are as follows 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.

Risk less brokering, secure bond between owner and broker, secure data delivery to end user, data privacy and secure key generation techniques are few advantages of publish/subscribe system.

Topic based and Content based is two subscription models to provide the subscription. In topic based subscription model messages are published by their name logical channel and subscriber acquired those messages published to the topic which they are subscribed. In content based subscription model messages are deliver to the subscriber only when the messages are similar to constrains.

Identity based encryption is technique used in publish/subscribe system which requires to maintain private/public key pair and it has been known between communicating entities to encrypt and decrypt messages. Identity based encryption [1] provides to reduced the amount of keys to be managed. In this technique any valid string which uniquely identifies a user can be the public key of the user and key server is maintains a single pair of public and private master keys. The master public key used by the sender to encrypt and send the messages to user with any identity, for example e-mail address. Successfully decrypt the message, to receiver needs to obtain a private key for its identity from the key server. Fig. 1 shows Identity Based Encryption.

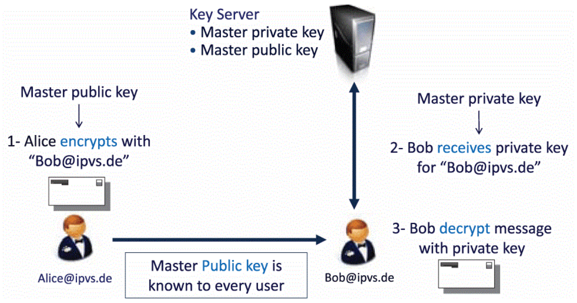
Key Server
• Master private key
• Master public key
Master public key
1- Alice encrypts with "Bob@ipvs.de"
Master private key
2- Bob receives private key for "Bob@ipvs.de"
3- Bob decrypt message with private key
Alice@ipvs.de
Master Public key is known to every user
Bob@ipvs.de

Fig. 1 Identity Based Encryption

Reverse circle cipher is one of the most important techniques used in proposed system. In this technique we can use encrypt and decrypt messages. Many different ways to find cryptographic key such as time based key and attribute based. That generated key is use for encryption and decryption messages. Fig. 2 shows Reverse Circle Cipher.

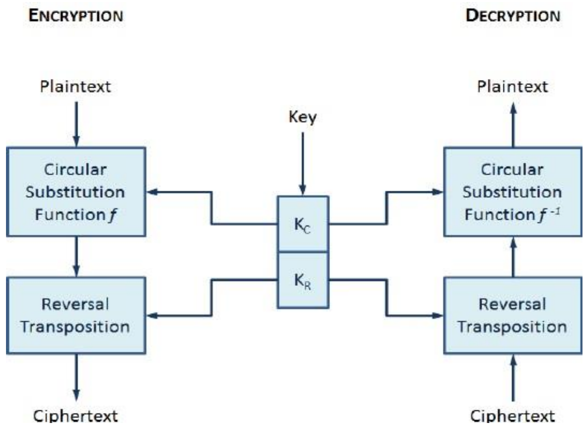

Fig. 2 Reverse Circle Cipher

Proposed system use Gaussian distribution technique. In this technique data is shared by convenient publisher with high probability distribution of complex value depending on the threshold value. It is also called as normal distribution and that technique is used easy to find out authorized and trustworthy publisher. Fig. 3 illustrates Gaussian distribution.

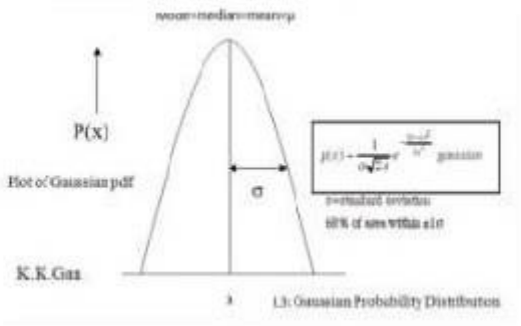

Fig. 3 Gaussian distribution

The rest of the paper is organized as follows. Introduction is discussed in Section I. Literature survey related to this system are discusses in Section II. Proposed system is discusses in Section III. Result and discussion are discusses in Section IV. Conclusion is discusses in Section V.

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 narrates identity based encryption and it used access key. This system also implemented Brokerless system. They can evaluate different attacks and developed a fine grained key management system. Identity based encryption entire the communication is based on identity of the party. If anyone can stole the identity then system data can organized. For example if anyone can be swiped the debit card and user also know the pin number then the user can debit some amount also. So this is the withdrawal of identity-based encryption. Solve this encryption in some condition by using attribute-based encryption. The major drawback of this model 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 describes the general solution of the privacy preserving information sharing problem in XML information brokering. It uses coordination for brokering systems. The major drawback of this system is that no inter coordinator communication is to protect system from malfunctioning.

Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi [3], they explain the block cipher technique used in own security such as data encryption standard (DES) and advance encryption standard (AES) both of them authority in helpful for real time data transfer. The purposes of reverse circle cipher algorithm are encryption and decryption. The performance of the algorithm across the size of the plaintext and frequency distribution within the cipher-text and it also replacement of character is applied on end of each rotation. Benefits of reverse circle cipher algorithm are as follows: key length is variable and set of bits used in AES and DES.

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

J. Bethencourt, A. Sahai, and B. Waters [5], this system elaborates complex access control techniques on encrypted data and it is called as cipher-text policy attributed based encryption. In this system the encrypted data is fully private even if the storage server is untrusted and it also support secure against collision attacks. This system based on Role Based Access Control. Performance and reliability that means duplicated data can be stored on different locations are the advantages of this system. The disadvantage 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 explains fully functional Identity Based Encryption (IBE). System is based on the weil pairing and that system has chosen cipher text security in random oracle model assuming.

Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters [7], this system narrates a new cryptosystem for fine-grained sharing of encrypted data it is called as key policy attribute based encryption (KP-ABP). 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 these techniques manage 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 explains broker based system. System communicate inter domain and it called as a multi-domain system. Multi-domain means contributes a network in multiple organization or single organization.

Costin Raiciu and David S. Rosenblum [9], this system describes the Content Based publish/subscribe networks. It manages the notification and subscriber confidentiality. In this system 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 explain 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. PROPOSED SYSTEM

Proposed system presents a new technique to implement authentication and confidentiality in Brokerless publish/subscribe system. Our system to grant subscribers to manage credentials allows giving their subscriptions. Private Key authorize subscriber are identify with the credentials. Publisher associates each encrypted event with a set of credentials. Proposed system uses Identity Based Encryption (IBE) mechanisms.

To establish that an appropriate subscriber can decrypt an event only if there is match between the credentials associated with the event and the key. To identify the subscribers to verify the authenticity of received events.

Additionally we address the problem of subscription confidentiality in the existence of semantic clustering of subscribers. A weaker notation of subscription confidentiality is defined and secure overlay maintenance protocol is designed to preserve the weak subscription confidentiality.

A. *System Overview*

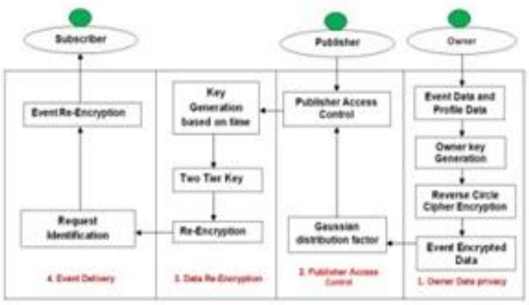

Fig. 4 System Architecture

System Architecture is the block diagram of the project. System architecture 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, describes 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.

B. *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 Ciphe2r
5. S = {R, E, Kg, Gd, Ka, Rcc}

The union of all subset of S gives the final proposed system.

(a)Random Key Generation

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

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

$$Pk=P\ (f(x)) \quad \text{..} \; (2)$$

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

(b)Gaussian distribution Equation

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

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

C. 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 maintain 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. RESULTS AND DISCUSSIONS

To show the effectiveness of the proposed system some experiments are conducted on java based windows machine using netbeans as IDE. To measure the performance of the system we set the bench mark by considering the system with more number of operating nodes (i.e. users).

To determine the performance of the system, we examined how many relevant keys are been generated on the rise of the number of users in the scenario. So the available result is shown in the Fig. 5.

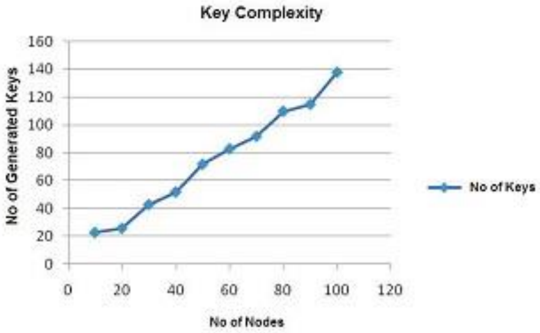

Fig. 5 Key Complexity

The plot in fig.5 clearly indicates that number of the keys are generated are always directly proportional to the number of the active users in the distributed system. This actually shows a good behavior of our model in distributed system.

Again key space is playing a vital role in the complete scenario as space required for the keys are always needed to be linearly dependent on the number of generated keys, which is successfully achieved by our system as shown in the Fig. 6.

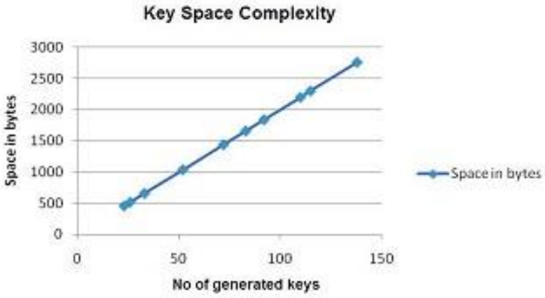

Fig. 6 Key Space Complexity

V. Conclusions

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] 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.

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

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

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

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