# Risk-Less Brokering System In Distributed Network Using Variable Key Technique

Gayatri P. Teke
Computer Engineering Department
SKN Sinhgad Institute of Technology and Science
Lonavala, Pune, India.
*Email: gayatri.teke@gmail.com*

Prof. Bhagyashree Patle
Computer Engineering Department
SKN Sinhgad Institute of Technology and Science
Lonavala, Pune, India
*Email: bhagyashreepatle@gmail.com*

***Abstract—*** Most of the business startups and established business sectors approach third party marketing agents to extend their businesses. In this scenario many times marketing agents or brokers can use the other business owner's crucial information for their illegal gains. So a big question arises for the trustworthiness of the brokers in these kind business arrangements. So a need of a strongly coupled business entity system is required in distributed paradigm to restrain the business relationship in between owners and brokers.Many systems are existed in the market where they deal with one or two aspects of the security issues in the system. So a proposed system put forwards an idea of providing $360^0$ security for the broker -less publisher and subscriber system using strong two tier key generation system which is powered by reverse circle cipher cryptographic technique. In addition to our previous work [1], this paper contributes 1) use of profile based key generation system 2) use of time based key generation system 3) use of two tier key generation combing 1 and 2 4) Powerful encryption technique using reverse circle cipher encryption 5) fine grained key management system 6 ) Enriched event distribution using Gaussian model.

***Keywords :-*** *Gaussian distribution model , event, publisher, subscriber, two tier key, Riverse cicrle cipher.*

*****

## I. Introduction

Now a days publish subscribe system also known as pub sub system starts gaining lots of attention as it completely isolates publishers from subscribers. In case of pub sub system publishers publishes the list of events to the system, and subscribers shows there interest by means of subscription. Once publishers issue the events, automatically it will send to the respected subscribers.

In such pub system publishers need not to know all the subscribers and vice versa. There are some systems which makes use of brokers as an intermediate between subscribers and publishers. But it lacks the security as broker may steal the data and used it in authorized manner. Also one point of failure will lead to complete fail of the system. So to avoid this scenario broker less system are emerged as one of the good system which insures the security and confidentiality of all the elements of the system. In broker less communication no broker involvement is there in any aspect of the system.

In pub sub systems access control is at heart. Access control means distributed events should be accessed by the valid subscribers. Access control also ensures that distributed events information should not get exposed to the routing infrastructures also. Because of secure nature of pub sub system it has been used in numbers of application such as environmental monitoring, news distribution, stock exchange and in event organization etc.

In order to ensure the security, public key encryption emerged as a solution. In public key encryption only authorized users of the systems have rights to access use the respected information. In this scenario owner of the events put the event information on the system, once he put all the information and save it, all the content of the events will get encrypted to ensure the privacy of the system. So only interested persons will get the information by requesting and having key of that particular event.

Since unique key is maintained across the complete operation of the system, it is important to use proper key generation algorithms. There are different ways to generate cryptographic keys such as time based, attribute based etc. The generated key is used as base for the encryption and decryption. The key which used for the encryption purpose should be used for the decryption else data will not get decrypted properly. Figure1 illustrates the normal functioning of reverse circle algorithm which is the core part of the proposed idea.

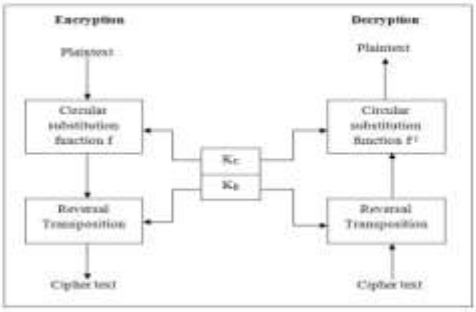

Figure 1: functions of reverse circle algorithm

Now a day's identity based encryption is one of the best options used by the pub sub system developers as it reduces the number of keys to be maintained. In identity based encryption any identity which uniquely identifies the person is used to generate the key, required for the encryption purpose. Although the attribute based encryption is widely used for the centralized applications, now a days it is best suited for the distributed applications also and this can be illustrate in the figure2.

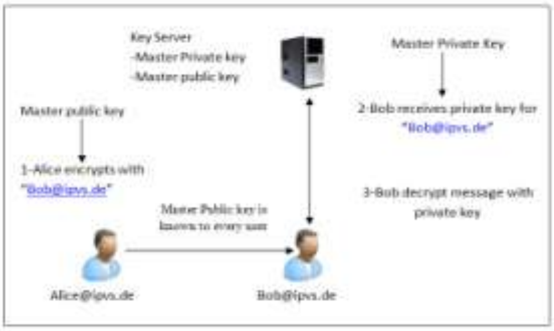
Key Server
-Master Private key
-Master public key
Master Private Key
Master public key
2-Bob receives private key for "Bob@ipvs.de"
1-Alice encrypts with "Bob@ipvs.de"
3-Bob decrypt message with private key
Master Public key is known to every user
Alice@ipvs.de
Bob@ipvs.de

Figure 2: Identity based encryption System

Gaussian distribution is a function used for restricting the probability distribution of the complex sums depending on the threshold value. It also named as normal distribution or bell shaped curve. In content based publish subscribe system it plays an important role as it helps in finding the trustworthy publishers. So it will get easier for the owner to find out the authorized and more trustworthy publishers. The more the value of the Gaussian functions the trustier will be the publishers.

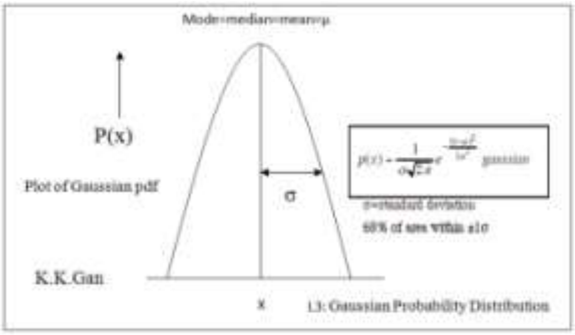

Figure 3: Gaussian distribution function

The rest of the paper is organized as follows. Section 2 discusses some related work and section 3 presents the design of our approach. The details of the results and some discussions we have conducted on this approach are presented in section 4 as Results and Discussions. Sections 5 provide hints of some extension of our approach as future work and conclusion.

## II. LITERATURE SURVEY

Here we are going to illustrates some of the previous works done by the researchers in same domain and also the supporting techniques used in our project.

[1] Elaborates the multi-rotational technique suitable for ensuring the security of the networks. Traditional encryption algorithms are facing the issues like encryption complication, cost of the encryption, and the difficulty in organizing the data. So here author comes with the different approach that can overcome the older issues. They make use of multi-rotational technique rather than linear rotational technique. In this paper writer provides the complete system architecture for the better understanding to the readers.

One of the drawback observed in encryption policies are encryption that done on coarse grain level. Coarse grain encryption refers to an encryption where private key is shared to another party. To overcome the problem of coarse grain encryption author proposed a new theory [2] named as key policy based attribute based encryption. In this policy an attribute and key labeling is done to the cipher texts. So that system can control which cipher text a user can decrypt. Author states an important difference between secret sharing schemes and his own scheme: Secret sharing scheme allow the coordination among the different parties while it is completely prohibited in his scenario.

Sahai and Waters proposed a theory of single authority attribute based encryption; in this work they kept multi authority based encryption as future work. [3] Tries to implement the future work of Sahai's contribution. Author developed a scheme in which any number of users can be able to monitor the attributes and thus to share the public keys. Before transferring the data owner sets a number N which is the number of set of attributes. After getting the encrypted message and number N, a receiver can decrypt the data only if it has at least N number of same attributes. If receiver doesn't have N number of attributes then it will not get the proper data as he is not authorized one.

[4] In case of attribute based encryption scheme, along with cipher text an access control policies are not sent, which highly increases the privacy of the encrypted data. As only the ciphered data is need to be send , the system will get lots of speed as it reduces the time required to transfer the access policies. Finally author concludes that the system is very expressive under the decisional Bilinear Diffie-Hellman assumption.

[5] Illustrates a deep survey on different attribute based encryption schemes. In this paper each of this policy is well explained along with the advantage and disadvantage of each policies with other policies.

Different attribute based encryption policies are

- Attribute based encryption (ABE)
- Key policy attribute based encryption (KP-ABE) scheme
- Cipher text policy attribute based (CP-ABE) scheme
- Attribute-based Encryption Scheme with Non-Monotonic Access Structures
- hierarchical attribute-based encryption scheme(HABE)
- multi-authorities attribute-based encryption scheme (MA-ABE)

Table 1 compares all the specified by considering the four factors: fine grained access control, efficiency, computational overhead and collusion resistant.

| Techniques | ABE | KP-ABE | CP-ABE | HABE | MA-ABE |
|---|---|---|---|---|---|
| **Fine grained access control** | Low | low | average | Good | better |
| **Efficiency** | Average | average | Average | Flexible | scalable |
| **Computational overhead** | High | average | Average | Average | average |
| **Collusion resistant.** | average | good | good | good | high |

Table 1: Attribute based policy comparison

[6] Explains a new system that can be widely used in pub sub system known as Event guard. Author proposed a Event guard mechanism in 3 steps. The design of architecture is done in such way that it maintains the security along with keeping simplicity and scalability of the system. Also author shows the efficiency of the system with numerous attacks.

[7] Here author focused on couple of problems that normally observed in content based pub sub system. The presented solution is based on commutative multiple encryption scheme which ensures that the intruders will not have access to the routing packets. Authors told that it is the first solution that avoids the key sharing with the end users. At some point of system brokers can be act as subscribers. The plus point of the paper is that it ensures the confidentiality of the publishers and privacy of the subscribers with respect to the interests of the subscribers.

[8] Here developer introduces PADRES, a pub sub system having capability to correlate the generated events , access all the events uniformly irrespective there creation time, balance the traffic of brokers and publishers over routing infra and failure of the network. While developing the system , simplicity is maintained to addressed all the problems like tradeoff availability, storage overhead, query overhead, query delay, load distribution, parallelism, redundancy and locality. The format of the message, language of the subscription and data models of content based pub sub models are well described in the format.

[9] provides a certificate based encryption scheme. In certificate based encryption identity based encryption and public key encryptions are combined to take advantage of both of the given schemes. Here signatures are generated and later signatures are used for the purpose of encryption and decryption. So in order to decrypt the message properly a person should have a public, private key and up to date certificates from the issuer.

## III. PROPOSED METHODOLOGY

In this section, we describe our framework for brokerless publisher / subscriber system using strong network cipher techniques with the below mentioned steps as shown in figure 4.

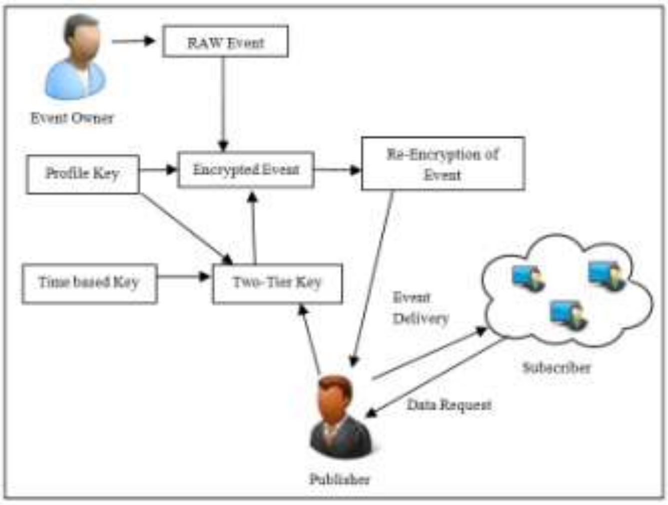

Fig 4: Overview of our approach

*Step 1*: Here in this step event owner first feed all the event parameter in to the system. Then by using the profile attributes and event data a key will be generated with mentioned algorithm 1.Which is having 7 character length and the uniqueness is maintained for all the new events created by the owner.

```
ALGORITHM 1: RANDOM KEY GENERATION
Input: Set U = {$u_1$, $u_2$, $u_3$……$u_n$}
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
```

### (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 event data
$P_{k\,=}$ P (f(x)) ………………………………..(2)
$P_{k=}$ private key
P (f(x))= random key generation function

*Step 2*: Here in this step the event data provided by the event owner will be encrypted by the strong cipher algorithm called reverse circle cipher technique. Where the data is 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 strong encryption technique over the network and this can be shown in the below algorithm no 2.

ALGORITHM 2: REVERSE CIRCLE CIPHER

```
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
```

*Step 3:* Here in this step event data is been distributed to different publisher based on the Gaussian distribution model (GDM). Where it considers the distribution parameter as the number of the published events by the publisher. Where GDM is a continuous function which approximate the exact binomial distribution of the events by the publisher to give him the right weight.

### (B) Gaussian Distribution Equation

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

Where
μ= mean of distribution
$\sigma^{2\,=}$ variance of distribution
y= continuous variable
P(y)= probability of y

*Step 4:* Here in this step publisher for whom the event is been assigned by the event owner is access the event data. And create a two tier key which is empowered with time based key along with owner key. This random key generation is been powered with MD5 one way hashing algorithm.

By using this new key encrypted data is been re-encrypted again, which is been controlled by the both owner and publisher.

*Step5:* Here the published data by the publisher can be view by the subscribers and then request for the same to the publisher. Then this data with the new two tier key is been served to the subscriber, which eventually decrypt using reverse circle cipher decryption technique to deliver plain text event data to the subscriber.
`

## 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. And a developed system is put under hammer in many scenarios to prove its authenticity as mentioned in below tests.

### 4.1 Key Space Complexity

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 figure 5

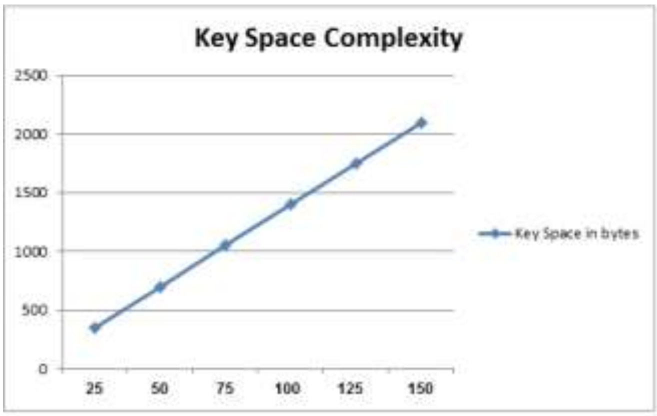

Figure 5: Key Space Complexity analysis

### 4.2 Character assignment for Encryption

The graph in figure 6 is drawn between the number of file character that are being used for the encryption and decryption v/s number of different characters that are using by the algorithm. Here in the above graph proposed system of brokering system in web uses the character to encrypt while each rotation is being happened, this takes more characters to replace than the system that is been proposed by the author[10] . As the author [10] uses the characters on completion of the rotation this makes the algorithms to take little less character than of our proposed method in web.

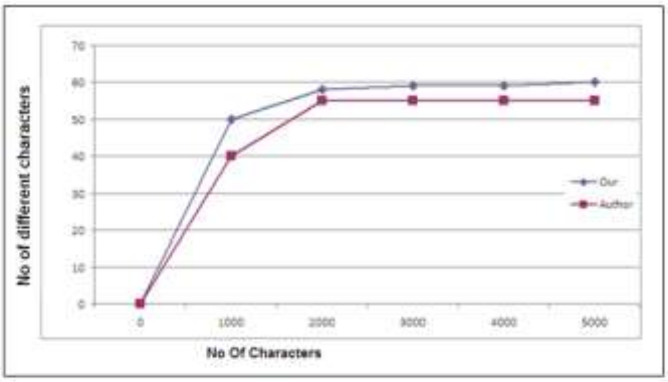

Fig 6: No of File character v/s No of Using different characters for the encryption and decryption

## V. CONCLUSION AND FEATURE SCOPE

Proposed method is efficiently shows the broker less subscriber / publisher relationship without adding much hazards of trustworthiness. Here keys are been generating by permutation of the characters in run time based on the event owner data generation scenario and publisher access scenario with different keys. In the system owner is efficiently generate the key based on his profile data and event data. Whereas the publisher manages to re-encrypt the data by generating two tier key using owner key and time based key for the reverse circle cipher encryption cipher base. Again System successfully maintains the Event distribution scenario by using Gaussian distribution model for the publisher. And in the end the whole system is tightly coupled to handle many subscriber requests in run time with proper event publishing schemes.

The proposed system can be enhancing to implement in heterogeneous network of internet of things using cluster based hierarchy. This makes the system to access completely in all possible types of network.

Cluster based hierarchy in distributed paradigm is the scenario where many clustered node in the systems are assigned for the different work in the distributed network. So we can enhance our model by assigning clusters for handling publisher work and event owner work. This actually greatly reduces the task completion time.

## REFERENCES

[1] “Enforcing Reverse Circle Cipher for Network Security Using Multirotational Technique” , Sajjade Zeba S. International Journal of Advanced Research in Computer Science and Software Engineering Volume 3 Issue 7, July 2014

[2] “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data” Vipul Goyal¤ Omkant Pandey Amit Sahai Brent Waters https://eprint.iacr.org/2006/309

[3] “Multi-Authority Attribute Based Encryption” Melissa Chase Computer Science Department Brown University Providence, RI 02912 https://eprint.iacr.org/2009/083

[4] “Ciphertext policy Attribute based Encryption with anonymous access policy” A.Balu1, K.Kuppusamy2 Research Associate, 2 Associate Professor Department of Computer Science & Engg.,Alagappa University, Karaikudi, Tamil Nadu, India. by A Balu - 2010

[5] “A Survey on Attribute Based Encryption Scheme in Cloud Computing ” Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3 *International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013*

[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 ContentBased Publish/Subscribe Networks,” Proc. Emerging Challenges for Security, Privacy and Trust, 2009.

[8] H.-A . J acobsen, A.K.Y. Cheung, G . Li, B. Ma niymaran, V . Muthusa my, and R.S. Ka zemzadeh, “The PADRES Publi sh/ Subscribe System,” Principl es and Applications of Distributed Event-Based Systems. IGI Global, 2010.

[9] “Certificate Based Encryption for Securing Broker-Less Publish/Subscribe System in Wireless Network” International Journal of Innovative Research in Computer and Communication Engineering , Vol. 3, Issue 4, April 2015

[10] Reverse Circle Cipher for Personal and Network Security ,Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi Jeppiaar Engineering College Chennai, Tamil Nadu, India ebeisaac@gmail.com