Privacy Enhancing In Broker-Less Publish/ Subscribe System

Ulka Vidhate[1], Sonali Pingale[2], Diksha Rajguru[3]

[1, 2, 3] Department of Computer Engineering

[1, 2, 3] AISSMS's Institute Of Information Technology, Pune-411001, Savitribai Phule Pune University, India

Abstract*- The provisioning of basic security mechanisms such as authentication and confidentiality is highly challenging in a content based publish/subscribe system. Authentication of publishers and subscribers is difficult to achieve due to the loose coupling of publishers and subscribers. Likewise, confidentiality of events and subscriptions conflicts with content-based routing. This paper presents a novel approach to provide confidentiality and authentication in a broker-less content-based publish/subscribe system. The authentication of publishers and subscribers as well as confidentiality of events is ensured, by adapting the pairing-based cryptography mechanisms, to the needs of a publish/subscribe system. Furthermore, an algorithm to cluster subscribers according to their subscriptions preserves a weak notion of subscription confidentiality. In addition to our previous work, this paper contributes*

1) *Use of searchable encryption to enable efficient routing of encrypted events,*
2) *Multicredential routing a new event dissemination strategy to strengthen the weak subscription confidentiality,*
3) *Thorough analysis of different attacks on subscription confidentiality. The overall approach provides fine-grained key management and the cost for encryption, decryption, and routing is in the order of subscribed attributes. Moreover, the evaluations show that providing security is affordable w.r.t.*
    1) *Throughput of the proposed cryptographic primitives,*
    2) *Delays incurred during the construction of the publish/subscribe overlay and the event dissemination.*

Keywords*-* Encryption, Decryption, Security, Content- Based, Identity-Based

I. INTRODUCTION

Marketing a product and selling it, is not a simple employment, so all fabricates are searching for a wide range of outsider item promoters like advertisement agencies, Dealers or third party brokers. publish/subscribe network contain two elements: 1) Publisher and 2) Subscriber. Publisher who is going to distribute occasion and subscribe who is demonstrated his enthusiasm for specific occasion and subscribe that occasion. Publish/Subscribe network is fundamentally approximately coupled. So the publishers and subscribers are obscure to one another. So for smooth working, already specialist is utilized as a go between. As it may, there are such a large number of impediments. So it requires more security methods to keep up authentication and confidentiality of data. So some broker-based frameworks are storing so as to keep up classification encoded design data in database. In any case, again there is a restriction and trust issue same as it may be. Really in business dealers are assuming a key part to put the offering record on the track. In any case, it is constantly million dollar query arrives on broker's dependability. In later case, publish/subscribe system is executed by without facilitate these framework is called as broker- less publish/subscribe network. Security require in publish/Subscribe system in numerous things first just confirmed publisher can distribute their occasion and just approved endorser can permitted to get to that occasion which they subscribe for the same. Besides other data couldn't open to whatever other supporter that is called as secrecy. For these security issues are make a test to the designer to make exceedingly secure publish/subscribe system.

To leave this issue, numerous broker less frameworks are been proposed for the publish/subscribe framework in appropriated worldview. However, the majority of them have neglected to accomplish the abundantly required security of the data over the exchanges. So our proposed framework puts advances a thought of creating irregular keys for each publish/subscribe exchanges which are haphazardly producing taking into account the occasion points of interest and supporter data in which scrambled occasions are steered to subscribers without knowing memberships and to permit supporters and publishers authenticate one another without knowing one another.

II. LITERATURE SURVEY

Punam V. Maitri, Dattatray S. Waghole and Vivek S. Deshpande had implemented "A Low latency for file encryption and decryption using BRA algorithm in network security" in which Results are taken for image ,text and audio file encryption and decryption process BRA and AES algorithm.

M. Bala Krishna, M. N. Doja investigate the Symmetric key management and distribution techniques in wireless adhoc networks which provides analysis of key management and symmetric key distribution techniques in wireless ad hoc network. For central coordination and sparse network, master key management is used. For large scale dense network, random key management is used. Analytical methods conclude that to save node energy self healing techniques are used in local area and distributed Diffie Hellman is used in wide area.

JunShu, Yiwen Wang, Wenchang Li, Zhiyong Gan [3] proposed an approach of Realization of a resource sharing fast encryption and decryption. By changing the traditional encrypting and decrypting s box of AES to realize the resource sharing, the area of hardware is reduced. Limitations in this paper is that System uses more number of characters for encryption. System capacity is measured using FPGA which is again non soft computing area.

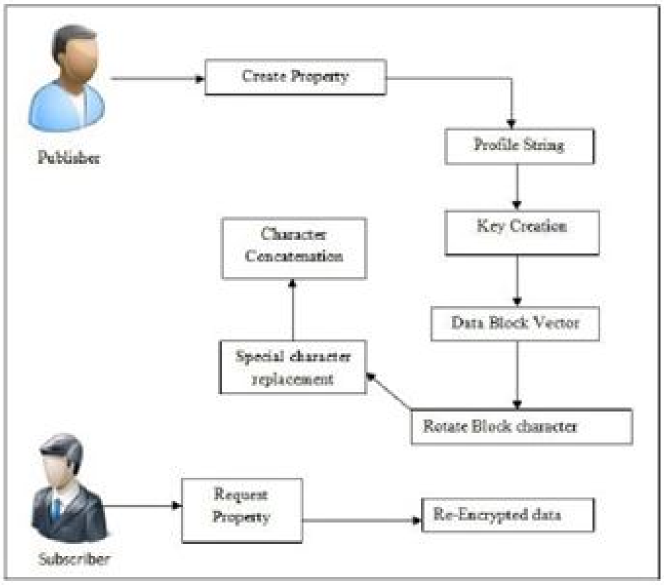
Montida Pattaranantakul1, Aroon Janthong2, Kittichai Sanguannam2,Paramin Sangwongngam1[4] presents new technique in quantum cryptography network-a new trend in secure communication to build trusted network. System has adapted various VPN technique to construct a private network. Key management and custom protocols is designed to support key distribution across multiple users
Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi [5] A cryptosystem is proposed that can be used for both personal and network security. It optimizes performance of data but also provides adequate level of security of the data. Limitations of this paper is System uses comparatively larger number of character for encryption thereby it leads to more space complexity.

CostinRaiciu and David S. Rosenblum [6] This paper presents a study of confidentiality in content-based publish/subscribe, addressing some of the security concerns particular to this interaction model and opening the road for real deployment. Focus on enabling confidentiality for commonly used applications and subscription languages in content-based publish/subscribe and propose a series of practical solutions.

III. PROPOSED SYSTEM

In this paper, we evaluate performance and scalability of the proposed publish/subscribe system only with respect to the security mechanisms. The idea of this proposed method is triggered by the fact that random keys can be maintained by the random request parameters done by the subscriber. Then to enhance the complex key structure system uses highly secured Reverse circle cipher for maintaining privacy. To enforce the system more vigorously system uses high level key management system in the network. In our proposed system, when publisher publishes the events using publishers credentials that events are encrypted and then store on the cloud. When any subscriber request the event, if the subscriber is authorized user key server generates private key using subscribers credentials. Using that private key subscriber now can decrypt the event.

Following architecture diagram shows the working of the proposed system.



3.1 METHODOLOGY

The proposed work in this paper deals mainly deals with the key generation using key server for publishers and subscribers relevant to their cradentials. When publishers publish their events, which are encrypted with their keys which are public and subscribers decrypt events of their interest using private keys which are generated by key server using subscribers relevant credintials.

IV. ALGORITHM

4.1 Key Generation based on Profile

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

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

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

4.2 Key Generation based on date and time

```
Step 0: Get the current date & time
Step 1: Concatenate all the characters to get a single String and hash it using md5
Step 2: Convert all the data to Integer type
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 xth character from the String
Step 7: Continue till 7 characters are selected
Step 8: concatenate all the 7 characters
Step 9: return key
```

4.3 Reverse circle cipher encryption 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 j=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
```

V. ADVANTAGES

1. Random keys are used to maintain the random request
2. parameters done by the subscriber.
3. Secure Reverse circle cipher for maintaining privacy.
4. Time based keys are enhancing the key generation process.

VI. LIMITATIONS

1. Loosely coupled distributed systems can cause transaction failures.

VII. RESULTS

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.

7.1 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.

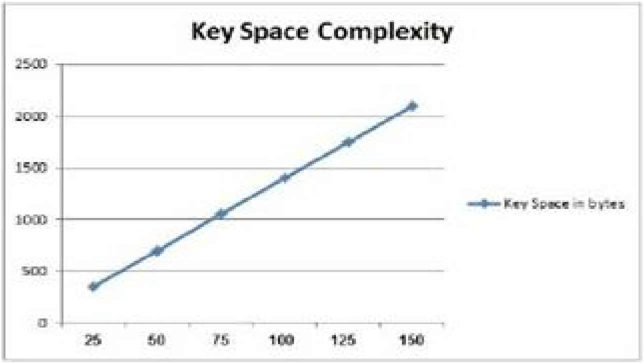


Fig: Key Space Complexity analysis

7.2 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.

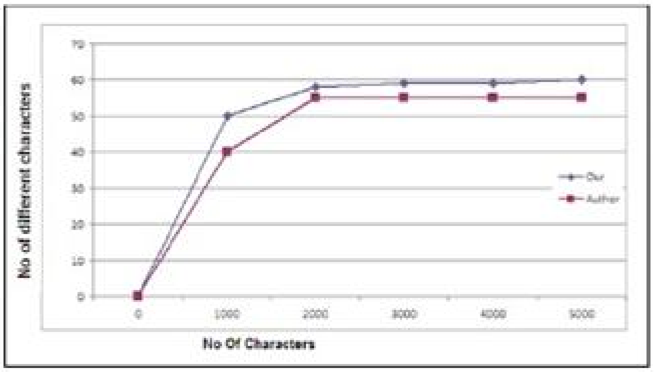


Fig : No of File character v/s No of Using different characters for the encryption and decryption

VIII. CONCLUSION

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.

IX. FUTURE SCOPE

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] M. A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel,“Providing Basic Security Mechanisms in Broker-Less Publish/Subscribe Systems,” Proc. ACM Fourth Int’l Conf. Distributed Event-Based Systems (DEBS), 2010.

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

[3] 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.

[4] E. Anceaume, M. Gradinariu, A.K. Datta, G. Simon, and A.Virgillito, “A Semantic Overlay for Self- Peer-to-Peer Publish/Subscribe,” Proc. 26th IEEE Int’l Conf. Distributed Computing Systems (ICDCS), 2006.

[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] H.-A. Jacobsen, 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.

[7] L.I.W. Pesonen, D.M. Eyers, and J. Bacon, “Encryption Enforced Access Control in Dynamic Multi-Domain 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. O ¨ nen, and R. Molva, “Privacy-Preserving Content- Based Publish/Subscribe Networks,” Proc. Emerging Challenges for Security, Privacy and Trust, 2009.

[10] 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.