IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 11, November 2015.
www.ijiset.com
ISSN 2348 – 7968

Enhancement of Security in Content Based Publish/Subscribe System by Access Control and IBE

Sunitha R L[1], Yedukondalu N[2]
PG Student, Dept. of CSE, Shree Institute of Technical Education, Tirupati, A.P, India1
Assistant Proffessor, Dept. of CSE, Shree Institute of Technical Education, Tirupati, A.P, India2

Abstract : In recent trends the subscription of information and providing same to the subscribed user is the continuous process in present information system, with this reason publish/subscribe network is high attention for loosely coupled form of interaction in large scale. Generally the subscriber specifies their interest in events and the publisher stores the information which subscriber needs in the pub/subscriber system, later the subscriber asynchronously receives the events matching their interest. Authentication of publishers and also subscribers is difficult to achieve because of its loose coupling and in the same way confidentiality of events conflicts with the content based routing. So we are presenting the novel approach to provide the basic security by adapting identity based encryption mechanism and access control by providing the encryption of the events.

We specify user to get access control by the publisher in order to get the data or information, thus fine grain key management and the cost for encryption, decryption and routing in order of subscribed attributes are the key points we are presenting.

Keywords : Content-based, publish/subscribe, peer-to-peer, broker-less, security, identity-based encryption.

I. INTRODUCTION:

The scale of distributed system has considerably changed the internet, increasing demand for high flexible communication model systems. Each unique point-to-point and synchronous communications, that tends to lead to hard and static applications. The publish/subscribe (pub/sub) network has became high focus as because of its inherent decoupling of publishers from subscribers with respect to time, synchronization also with respect to space. In this network publishers fills the data into the pub/sub network for the subscribers specified request, the published information is routed to the interested subscribers while not publisher knowing the relevant set of subscribers.

1.1 Methods of pub/sub system:

We mainly have two categories in distributing information. Two types are 1.system which mainly based on subject, 2.system mainly based on content. The system with subject is the one in which event involves to one particular set of which variously said to as groups. The subscription mainly focuses on a group or topic. And the user receives the events which are joining with the particular group or channel. On the other hand in content based system it is not mandatory that the information or event strictly to be in particular group instead the decision to which the message is directed is taken based on the message-by-message by query or predicate issued by the subscriber.

1.2 Security Concerns in PUB/SUB system:

In content based publish/subscribe system providing security causes main challenge; following are the security concerns we need to focus on achieving them are Authentication, Confidentiality, Accountability, Integrity.

1.3 Motivation:

Traditional methods to provide confidentiality and authentication by encrypting the data conflict with the content based mechanism and thus we require new mechanism to route the encrypted event in the route infrastructure without knowing the subscription confidentiality.

1.4 Problem statement:

In this we have two entities: publisher and subscriber, both parties do not trust each other and they are computationally bounded. In this system many publisher system and subscriber system participate and they do not deviate from the designed protocol. With all data provider may mask and chance of overhearing of data and thus accredited publishers and spam the overlay fabric.

ISSN 2348 – 7968

1.5 Goals:

1. To encrypt the events and also route the encrypted events in the pub/sub network.. 2.To provide access control at the publisher side in order to access the information at the subscriber side by providing the expiry date for the secret key.

II. EXISTING SYSTEM:

In previouse work, most of the work focused only on giving expressive and scalable pub/sub systems, but rare attention has given for the need of security. Existing methods towards secure pub/sub systems mostly lie an the existence of traditional broker network. This wont address security under restrictive expressiveness. For example, by using only keyword matching for routing events or lie on a network of believable brokers. Further available approaches mainly coarse-grain period based key management and cannot provide fine-grain gain mechanism in a salable sort. Still, instrument in broker-less pub/sub systems, where the subscribers are clustered according to their subscriptions.

2.1 Disadvantages of Existing System

1) Present methods won't address security under restricted expressiveness, for a matching for routing events or rely on a network of (semi-trusted) brokers.
2) Using of PKI system for the giving security causes more burden to underlying system to maintain the all the keys.
3) Data users based on groups and its security concerns are not yet described in the literature.

III.PROPOSED SYSTEM:

Proposed System presents a new approach to provide authentication and confidentiality in a broker-less pub/sub system. Our approach allows subscribers to Maintain credentials according to their subscriptions. Private keys assigned to the subscribers are labeled with the credentials. A publisher associates each encrypted event with a set of credentials. We adapted identity-based encryption (IBE) mechanisms 1) To ensure that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event and the key; and 2) To allow subscribers to verify the authenticity of received events. A credential consists of two parts:

1. A binary string which describes the capability of a peer in publishing and receiving events.
2. A proof of its identity. The latter is used for authentication against the key Server and verification whether the capabilities match the identity of the peer.

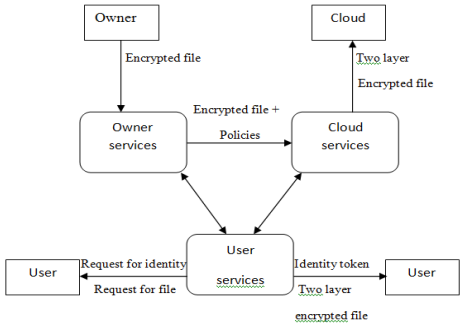
In particular, the identity-based encryption ensures that a particular key can decrypt a particular cipher text only if there is a match between the credentials of the cipher text and the key. Publishers and subscribers maintain separate private keys for each authorized credential. Due to the loose coupling between publishers and subscribers, Therefore, a published event is encrypted with the public key of all possible credentials, which authorizes a subscriber to successfully decrypt the event.

3.1 Advantages of proposed system:

1) Proposed system gives authorization, confidentiality, and scalability.
2) Extensions of the cryptographic methods to provide efficient routing of encrypted events by using the idea of searchable encryption.
3) "Multi credential routing" data distribution which strengthens the weak subscriber confidentiality.

IV. SYSTEM ARCHITECTURE:

Illustrates the system architecture of the proposed system. in this the various operations carried out in order to distribute the information or data which is generated at the publisher(owner)side. When the user(subscriber request for the data, the key server or proxy server asks for the identity and once the identity token got verified from the server the file and the key for the data decryption will be provided.



System Architecture

ISSN 2348 – 7968

V. IMPLEMENTATION:

Goal of this section is s to convert the designed system in design phase to make it work in implementation phase in the form of code by using some specific programming language. That can compute in the system. the development of any software or any application is mainly depends on requirements and tools that we have chosen to build and those things should be platform independent.

5.1 Module Description

This section defines the number of modules and various function carried out by the system modules which are developed.

5. 1.1 Admin Module

Proxy server(Add, Edit, Delete)

- Data Owner (Add, Edit, Delete)

➢ Add – Key Generation and send it through email

- Domain (View Only)
- Sub-Domain (View Only)
- Change Password

5.1.2 Subscriber Module

Subscriber are the data access users, suppose publisher is a college Liberian then subscriber are like students, lectures and admin staff in a college. Subscriber can able to register themselves and he will receive the Identity Token through email.

Algorithm 1. Secure overlay maintenance protocol at peer sq.

1. upon event Receive(CR of snew from sp) do
2. if decrypt requestðCRÞ ¼¼ SUCCESS then
3. f degree(sq) == available then //can have child peers
4 connect to the snew
5. else
6. forward CR to fchild peers and parentg _ sp
7. if decrypt requestðCRÞ ¼¼ FAIL then
8. if sp ¼¼ parent then
9. Try to swap by sending its own CR to the snew.
10. else
11. forward to parent

5.1.3 Publisher Module

Data publisher is the one who has the various collections of data, whenever the publisher interested in publishing the data events he/she will upload the data to the proxy server by encrypting the data.

When the data is uploaded to the proxy server the data will be encrypted using the publisher encryption key. And also the data owner will specifies the access policies for the uploaded file in order to provide the authentication and confidentiality of the uploaded file in the proxy server. Once the publisher has logged in to upload the file, he/she has the following functions:

- User details(view, delete)
- View subscriber request & send secret file
  -view all request
  -verify identity Token
  -send secrete key to requested subscriber

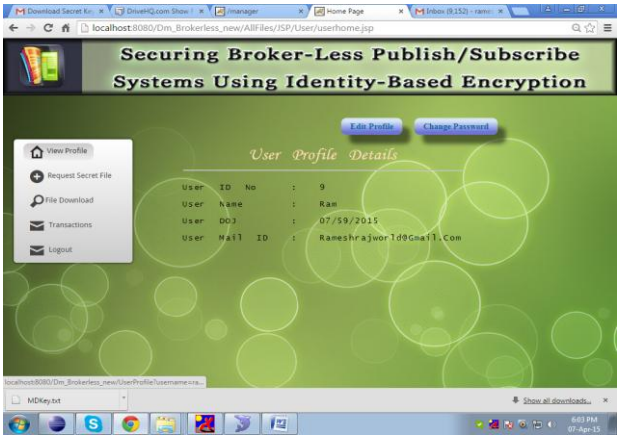
✓ Get RNS key
✓ RNS keys + Domain details + Expiry Date
✓ Encrypt the above string using DES
✓ Send secret file to requested user Email ID

- File Upload
  -File selection
  -Encrypting using RNS
  - Proxy server selection
  -Transfer the Encrypted file to selected proxy
- Uploaded file details(view, delete)
- File access control setting
- File access control details(view, delete)
- Transaction Details
- Change password

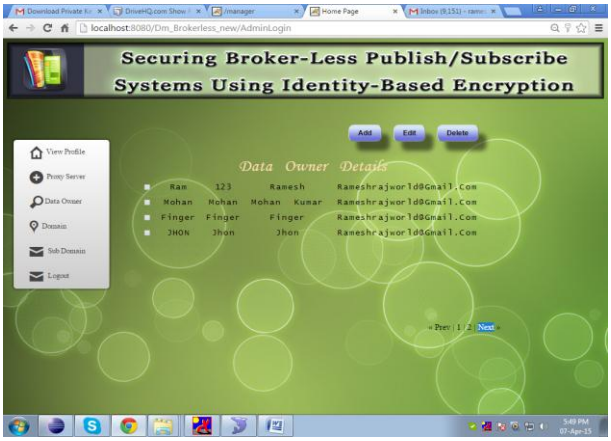
VI.RESULTS:

Snapshot1: Admin Login Page

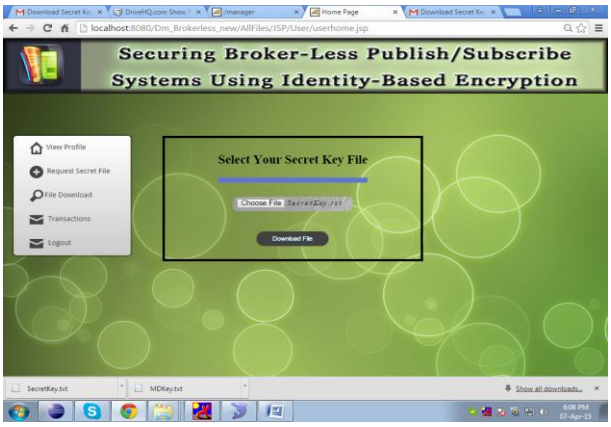
ISSN 2348 – 7968



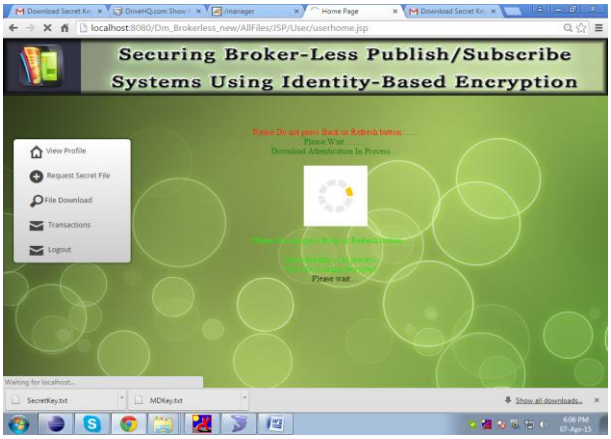
Snapshot2:view user profile



Snapsot3: Added Data Owner



Snapshot 4:File Download



VII. CONCLUSION:

This work presents a new approach to provide confidentiality of data and authentication by using the cryptographic methods such as IBE,DES and RNS algorithms. In addition to previous works. We have designing the double layer encryption in order to provide the strong security to the pub/subscribe system. Thus the introduced methods are extendable as the numbers data consumer's increases, publishers and also the number of to secret keys maintained by them.

In future enhancements, publisher has the different private key with their id for example publisher has to publish the Indian express, magazines, etc for each publish obtain the separate private key with id of the publisher or credential and also video and image encryption can carried out .

REFERENCES

[1] 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.

[2] 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.

ISSN 2348 – 7968

[3] 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.

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

[5] C. Raiciu and D.S. Rosenblum, "Enabling Confidentiality in Content-Based Publish/Subscribe Infrastructures," Proc.
IEEESecond CreatNet In Int'l Conf. Security and Privacy in Comm. Networks (SecureComm), 2006.

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

[7] 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.

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

[9] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public Key Encryption with Keyword Search," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques on Advances in Cryptology (EUROCRYPT), 2004.

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

[11] S. Choi, G. Ghinita, and E. Bertino, "A Privacy-Enhancing Content-Based Publish/Subscribe System Using Scalar Product Preserving Transformations," Proc. 21st Int'l, 2010.

[12] 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.

[13] 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.

[14] M.A. Tariq, B. Koldehofe, G.G. Koch, I. Khan, and K. Rothermel,"Meeting Subscriber-Defined QoS Constraints in Publish/SubscribeSystems," Concurrency and Computation: Practice and Experience, vol. 23, pp. 2140-2153, 2011.

[15] 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.

.