ISSN:0975-9646

Securing Broker-less Publish/Subscribe System using Fuzzy Identity-Based Encryption

Maithily B
M.TECH in Computer Science
CMR Institute of Technology
Bangalore, India

Swathi Y
Associate Professor & HOD
CMR Institute of Technology
Bangalore, India

***Abstract*— In broker-less publish/subscribe system, achieving security is a challenging issue. Security here mainly includes confidentiality and authentication, confidentiality is difficult to achieve due to content-based routing and authentication due to loose-coupling between the publisher and subscriber. In publish/subscribe system the publisher will inject information and events of interest is specified by the subscribers by means of subscriptions. Publishers publish the event without knowing the relevant set of subscribers. Supportive mechanism should be provided by the pub/sub to fulfill basic security demands such as access control and confidentiality. Authentication is difficult to achieve due to loose coupling of publishers and subscribers and confidentiality of event and subscription conflicts with content-based routing. So In this paper we propose a fuzzy logic technique which works on setup, extract, encryption and decryption. We shown in graph this fuzzy algorithm works better than traditional.**

Keywords— Security, Publisher, Subscriber, Fuzzy logic, Encryption, Decryption.

I. INTRODUCTION

High popularity is gained by the publish/subscribe communication because of inherent decoupling of publishers from the subscribers. In publish/subscribe system the publisher will inject information and events of interest is specified by the subscribers by means of subscriptions. Publishers publish the event without knowing the relevant set of subscribers. The most expressive subscription model is provided by the content based pub/sub, the restriction on the message content is defined by the subscriptions. The content based pub/ sub is very expressive and asynchronous in nature, it is due to this feature this method is widely used in distributed applications such as news distribution, stock exchange, public sensing, traffic control and environmental monitoring. Supportive mechanism should be provided by the pub/sub to fulfill basic security demands such as access control and confidentiality.

In pub/sub system as shown in fig 1, access control means allowing only authorized publisher to disseminate events in the network and only that events are forwarded to the authorized subscribers. Moreover while disseminating the event content should not be exposed to the routing infrastructure and all relevant information should reach the particular subscriber where the subscription is not revealed to the system. Solving basic security mechanism like end-to-end authentication is achieved through public key infrastructure, where publisher should maintain all interested subscribers public key to encrypt the event. Subscriber should contain all the public key of publisher to verify the received event. So a new mechanism to route the encrypted event to subscriber without revealing the subscription and authenticate each other without knowing each other.

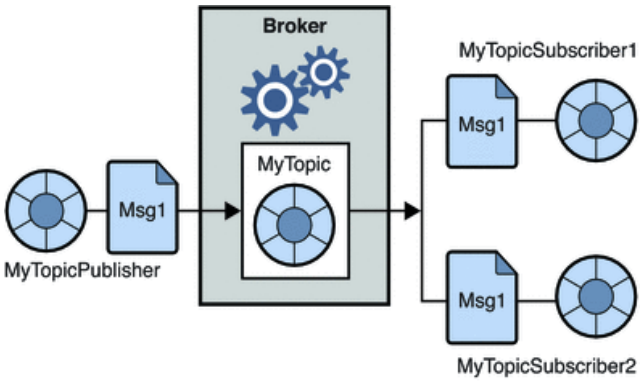

Fig 1 Public/Subscriber system

A new approach is presented to provide authentication and confidentiality in broker-less pub/sub system. The problem is solved using identity based encryption mechanism .This mechanism ensures that the credential of event match with credential of key so that subscriber can decrypt the event and verifies the authenticity of received event by subscriber. In the presence of clustering of subscribers, the confidentiality in the subscription is defined. The confidentiality in the subscription is preserved using secure overlay maintain protocol. To provide efficient routing of encrypted events, searchable encryption is used. To strengthen the confidentiality in the subscription, multi credential routing is used.

II. RELATED WORK

1. Anceaume.E, Gradinariu.M, Simon.G, and Virgillito.A, "A Semantic Overlay for Self- Peer-to-Peer Publish/ Subscribe," Proc. 26th IEEE Int'l Conf. Distributed Computing Systems (ICDCS).

A Semantic overlay is a novel design principle for reliable publish/subscribe architecture. Distributed Publish/Subscribe (DPS) is generic content based publish/subscribe system and is not based on a network of the broker. Without human intervention subscriber's co-

ordinate among themselves on peer- to- peer basis to construct an optimized event diffusion path. A subscription-driven semantic overlay is proposed where subscribers self-organize according to the similarity relationships based among their subscriptions. When two subscribers share a common attribute they are considered similar and are connected into same group. Groups of subscribers self-configure to form tree structures such that only one tree is built per attribute. Subscription is maintained only at the corresponding subscriber, as subscriptions are not replicated. Regardless of size of the system, each subscriber has to keep track of a limited number of neighbors and effect of node failure is confined within a bounded number of neighboring groups.

DPS achieves scalable events delivery in spite of failures and changes in the system. DSP includes variety of fault tolerant deterministic and probabilistic content-based publication/subscription schemes that target towards scalability.

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

In distributed system user can only access the data if a user possess a certain set of credential or attributes. The trusted server here stores the data and mediates access control. The confidentiality of the data will be compromised if the server storing the data is compromised.

Cipher Policy Attribute-Based Conversion (CP-ABC), provides the construction of a cipher text, where a user's private key will be associated with an arbitrary number of attributes expressed as strings. Here when the data is encrypted by user, they specify an associated access structure over the attribute, the message can be decrypted by the other user only if the attribute pass through the cipher text access structure. It uses monotonic access trees with the help of gates to perform the complex operations. Using CP-ABC, the encrypt data can be kept confidential even if the storage server is untrusted and secure against collision attacks. The collusion resistance is insured by using a private key randomization technique and secret-sharing schema.

3. Ion.M, Crispo.B, Rusello.P (2010) "Supporting Publication and Subscription Confidentiality in Publish/Subscribe Networks in Cloud," Proc. SixthInt'l ICST Conf. Security and Privacy in Comm. Networks (Secure Comm.), vol.32.

In publish/subscribe model, application interact indirectly and asynchronously. The publisher application generates message called event interesting application, where subscriber application express their interest by specifying filters. The publisher sends the event through the network of brokers and filters specified by subscriber is used of routing for events by the brokers. Due to loose-coupling exchange of message, achieving confidentiality is a challenge. To achieve confidentiality of event and filter, publisher and subscriber should not share the secret key.

Here confidentiality of publish/subscribe system by encrypting the content of the event by attribute-based encryption schema specifying the characteristic. For the subscriber to obtain the clear text should satisfy that characteristics specified with the encrypted data. The access control structured which is supported by attribute based encryption schema with encrypted search. The only information that broker can access is which filter are matched with the event. By this encryption schema for publish/subscribe system, confidentiality of events and filters and a simplified key management that does not require publisher or subscriber to share the secret key is supported.

III. EXISTING SYSTEM

A. *System model*

Content-Based Publish/Subscribe

The content based data model is used to route the events from the publishers to the relevant subscribers. The event space, denoted by Ω, is composed of a global ordered set of distinct attributes (Ai): Ω = {A1,A2,……Ad}.Each attribute Ai is characterized by a unique name, data type and domain. The data type can be either an integer or a floating point or a string. The range of the attribute value is defined by the domain. An event consists of attributes and associated values. If the values of the attributes satisfy the constraints of the subscriber, an event is said to be matched.

To maintain a self organizing overlay structure the publishers and subscribers act as peers. The concept of advertisements is used to authenticate the publishers, in which the publishers announce the set of events which it intends to publish.

Attacker Model

This model consists of two entities: publishers and subscribers. Both these entities are bounded computationally and they do not trust each other .The peers which are a part of the pub/sub overlay network are honest and they do not deviate from the protocol designed. The authorized publishers in the system can only send the valid events .Unauthorized publishers attack the authorized publishers with fake and duplicate events, take the control of the overlay network.

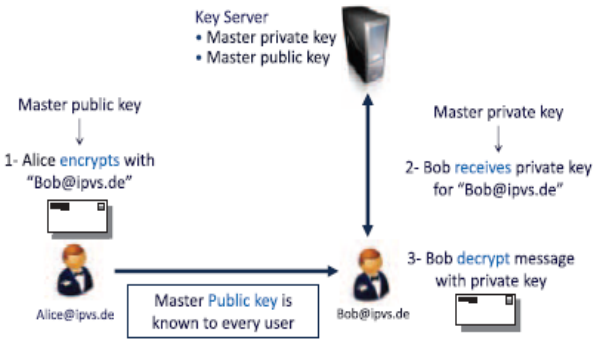

Fig 2 Identity based encryption

Security Goals and Requirements

The proposed secure pub/sub system consists of three main goals .They are:

- Authentication

- Confidentiality
- Scalability

Authentication: Only the authorized publisher can publish events in the system, to avoid no eligible publications. Only the authorized subscribers can receive those messages.

Confidentiality: There are two aspects of confidentiality in broker-less environment.

- To protect from the illegal modifications, the events are made visible only to the authorized subscriber.
- The subscriptions of the subscriber are confidential and unforgeable.

Scalability: There are three aspects to preserve scalability.

- The number of keys and the cost of subscription should be independent of the number of subscribers in the system.
- Constant number of keys per subscription should be maintained by the key server and subscribers.
- Without affecting the fine-grained access control, the overhead due to rekeying should be minimized.

Identity Based Encryption

For each publisher or subscriber a private /public key pair has to be known between the communicating entities to encrypt and decrypt the messages. Identity based encryption reduces the amount of keys to be managed. In identity based encryption, a string used to identify the user can be the public key of that user .The key server maintains a pair of public and private master keys.

IV. PROPOSED SCHEME

In this paper we proposed a fuzzy which uses setup, extract, encryption and decryption.

Setup:

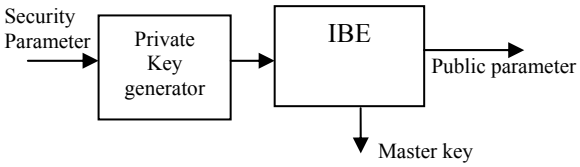

Fig 3 Setup

Give some security parameter as input to private key generator and run IBE the algorithm to generate master key and public parameter. Where this public parameter is given to interested parties and master key is kept secret.

Extract:

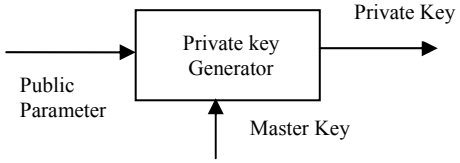

Fig 4 Extract

Provide master key and an identity ID as input, run the IBE algorithm to generate private key.

Encryption:

Providing the public parameters, identity ID' and plain text(message) as input and run IBE algorithm and generate a cipher text C.

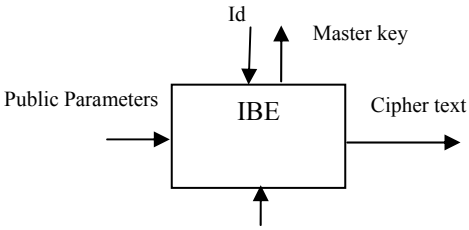

Fig 5. Encryption

Decryption:

Provide the public parameter, private key and cipher text C as input for decryption algorithm (IBE). It outputs message if $| ID \cap ID' | \geq d$ otherwise error message is displayed**.**

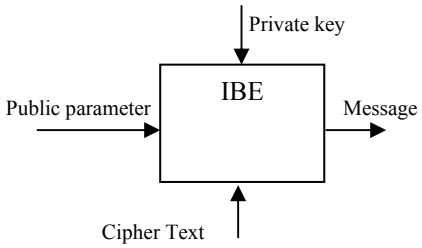

Fig 6 Decryption

V. SIMULATION RESULTS

Scenario 1:

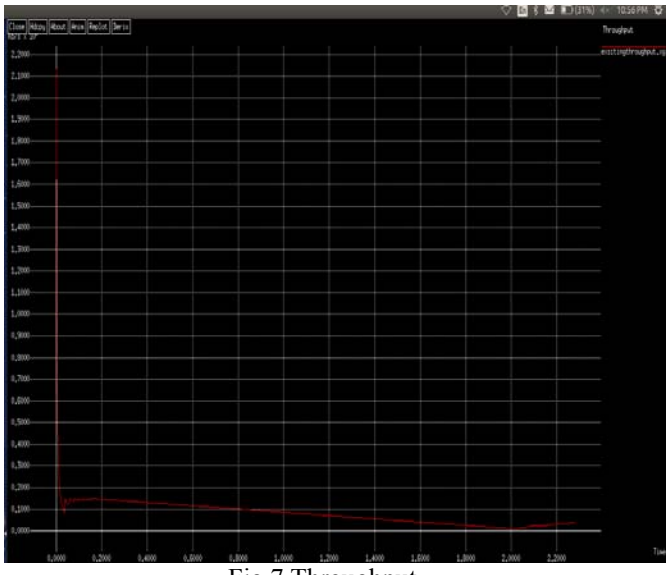

Fig 7 Throughput

In Above scenario we shown that fuzzy logic has more throughput than existing technique

Scenario 2:

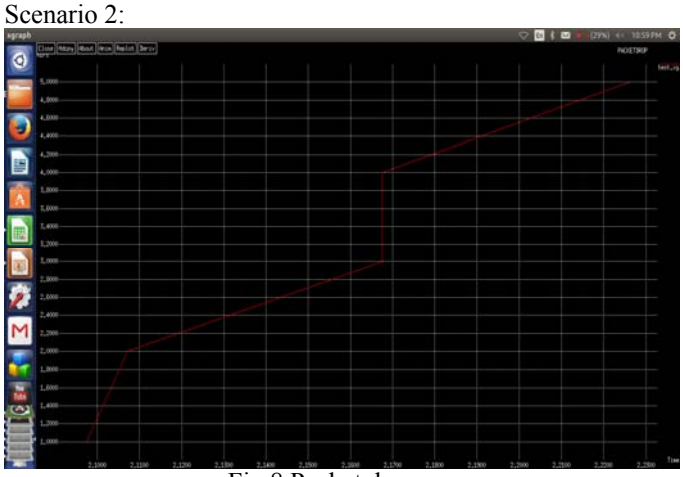

Fig 8 Packet drop

In Above scenario packet drop is less in fuzzy than existing.

VI. Conclusion and Future Work

In publish/subscribe system the publisher will inject information and events of interest is specified by the subscribers by means of subscriptions. Publishers publish the event without knowing the relevant set of subscribers. Supportive mechanism should be provided by the pub/sub to fulfill basic security demands such as access control and confidentiality. Authentication and confidentiality is difficult to achieve in content-based publish/subscribe system. Authentication is difficult to achieve due to loose coupling of publishers and subscribers and confidentiality of event and subscription conflicts with content-based routing. So using Fuzzy logic which has four algorithm such as setup, extract, encryption and decryption we can have confidentiality and authentication.

Acknowledgment

Maithily B, thanks to Mrs. Swathi Y, who is always encouraging and motivating me to do research activities. I am also very thankful my family and friends.

References

[1] 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.

[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] 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.

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

[5] 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.

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

[7] S. Choi, G. Ghinita, and E. Bertino, "A Privacy-Enhancing Content-Based Publish/Subscribe System Using Scalar Product Preserving Transformations," Proc. 21st Int'l Conf. Database and Expert Systems Applications: Part I, 2010.

[8] 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.

[9] 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.

[10] 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.

[11] M. Jelasity, A. Montresor, G.P. Jesi, and S. Voulgaris, "PeerSim: A Peer-to-Peer Simulator," http://peersim.sourceforge.net/, 2013.

[12] H. Khurana, "Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems," Proc. ACM Symp. Applied Computing, 2005.

[13] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, 2010. B. Lynn, "The Pairing-Based Cryptography (PBC) Library, http://crypto.stanford.edu/pbc/, 2010.