ISSN (ONLINE): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 5, MAY 2015, PP 383-386

# A NOVEL APPROACH TO PROVIDE CONFIDENTIALITY AND AUTHENTICATION IN A BROKER-LESS CONTENT-BASED PUBLISH/SUBSCRIBE SYSTEM

[1]C.Ratna Prabha, [2]P.Ragha Vardhani

**Abstract:** Publish/subscribe systems has evolved as an striking communication model for building Internet-wide distributed systems by decoupling senders of messages from receivers. So far most of the research on publish/subscribe has focused on other areas such as efficient event routing, event filtering etc. Very trivial research has been published regarding securing publish/subscribe systems. In content based public subscribe systems authentication and confidentiality are basic security issues. In this paper we presents a new approach to provide confidentiality and authentication in a broker-less content-based publish/subscribe system. By using pairing based cryptography mechanism, authentication and confidentiality for public subscribe event is ensured. Additionally, an algorithm to cluster subscribers according to their subscriptions preserves a weak notion of subscription confidentiality .To enable efficient routing of encrypted events searchable encryption is provided. To support weak subscription confidentiality, multi credential routing a new event distribution method is provided. Also comprehensive analyses of different attacks on subscription confidentiality are provided. The overall methodology provides Key management for identity based encryption, cost for encryption decryption and routing based on subscription of attributes.

**Keywords:** Publish/subscribe, Identity-based encryption, PKG.

———————————— ◆ ————————————

## 1. INTRODUCTION

The publish/subscribe model evolved from last few years as an efficient tool for distributed applications in which information has to be dispersed from event producers to event consumers i.e. from publishers to subscribers. Users receive certain types of events by applying filters on event contents called subscription. For each new event published the Pub/sub system checks all events beside all present subscriptions and deliver it to all users for their matched subscription. Traditionally they were using broker networks for routing of events from publishers to subscribers. In more recent systems, broker-less routing infrastructure is used by making event forwarding overlay. [1] In content based public subscribe systems information concerning an event (i.e. content of message) determines where the message is delivered. Senders send messages without knowing the destination address, with only some message content visible to network. Receivers declare a query which is matched against published message content. Then the message is transmitted to all receivers whose query is matched by the content of the message. This method is useful for different distributed applications like stock exchange, traffic control, publish sensing.

Pub/Sub systems need to provide security to these applications such access control and confidentiality. In Pubs/sub system access control means only authenticated publishers are allowed to distribute events and only authorized subscribers are allowed to receive that events .Contents of events are kept as confidential and subscribers receive that events without informing their subscriptions for the system. Both publication and subscription confidentiality is required to reduce risk of leakage of events in systems. For that purpose publisher and subscriber need to share secret key, by using public key infrastructure, which is not desirable because it would weaken the decoupling property of the model.

In PKI, publishers maintain public keys of all subscribers for encryption of events. Similarly, subscribers must know the public keys of publishers to check authenticity of received events. Traditional methods of encrypting all message violates the approach of content based system. Hence new method is needed to route events to subscribers without knowing their subscriptions and authenticating them. Public subscribe systems are provided by most researchers but less consideration is given on security of public

- ***C.Ratna Prabha*** *is currently pursuing master's degree program in computer science & engineering in Ravindra College of Engineering for Women(JNTUA), India,E-mail: c.ratnagpcet09@gmail.com*
- ***P.Ragha Vardhani***,*.Currently she is working as Assistant Professor in Department of Computer Science Engineering in Ravindra College of Engineering for Women, Kurnool. India, E-mail: ragha.vardhani@gmail.com*

subscribe systems. Existing approach depends on conventional broker network. This either deal with security under limited perspicuity, for example, by using only keyword matching for routing events [2], [8] or depends on semi-trusted broker network. [7], [6], [5]. In keyword search method, events are routed based on keyword in the message contents. This approach provides key management but does not provide access control in scalable manner. Yet, in security issues of public subscribe systems how the subscribers are clustered is not mentioned. In this paper we present new approach to provide authentication and confidentiality in public subscribe systems. The credentials are maintained based on subscriptions of subscribers.

For encryption of events we requires keys, private keys allocated to the subscribers are labeled with credentials. A publisher is having set of credentials. In public key encryption a public key can be any arbitrary string. In such a scheme there are four phases. In first setup phase, global system parameters and a master-key are generated. In second, i.e. extraction, private keys are extracted from master keys. In third, encryption, events are encrypted using public keys. In fourth, decryption, messages are decrypted by using relative private keys. [4]

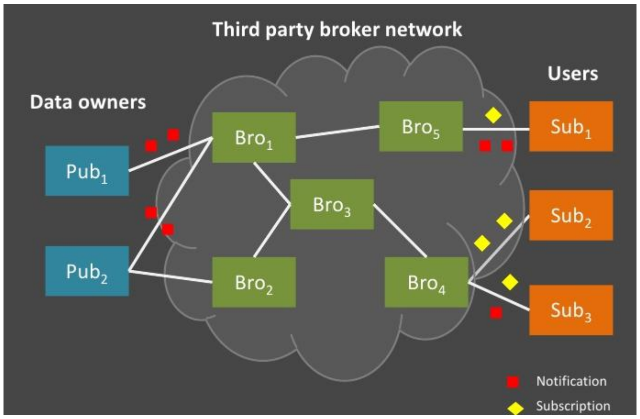

Fig 1. Subscriber/Publisher System

We develop an identity based encryption in which, relative subscribers can decrypt event only if there is match between credentials and key. Also it allows subscribers to check authenticity of received events. [3] In addition we tackle issues regarding subscription confidentiality for semantic clustering of events. A secure overlay maintenance protocol is designed to preserve the weak subscription confidentiality. Additionally, we propose a extended cryptographic methods for routing of events and “Multi credential Routing”, new event distribution method.

## II. RELATED WORK

There are two entities in the System publishers and subscribers. Both the entities are computationally bounded and do not trust each other. Moreover, all the peers (publishers or subscribers) participating in the pub/sub overlay network are honest and do not deviate from the designed protocol. Likewise, authorized publishers only allow valid events in the system. However, malicious publishers may masquerade the authorized publishers and spam the overlay network with fake and duplicate events. We do not intend to solve the digital copyright problem; therefore, authorized subscribers do not reveal the content of successfully decrypted events to other subscribers.

**A. PUBLISHER SUBSCRIBER TECHNIQUE** Publishers and subscribers interact with a key server. They provide credentials to the key server and in turn receive keys which fit the expressed capabilities in the credentials. Subsequently, those keys can be used to encrypt, decrypt, and sign relevant messages in the content based pub/sub system, i.e., the credential becomes authorized by the key server. A credential consists of two parts: 1) a binary string which describes the capability of a peer in publishing and receiving events, and 2) a proof of its identity [1].

**B. IDENTITY BASED ENCRYPTION (IBE)-**based public key cryptosystem, which enables any pair of users to communicate securely without exchanging public key certificates, without keeping a public key directory, and without using online service of a third party, as long as a trusted key generation center issues a private key to each user when he first joins the network [2].

**C. IDENTITY HANDLING:** Identification provides an essential building block for a large number of services and functionalities in distributed Information systems. In its simplest form, identification Is used to uniquely denote computers on the Internet By IP addresses in combination with the Domain Name System (DNS) as a mapping service between symbolic Names and IP addresses. Thus, computers can conveniently Be referred to by their symbolic names, whereas, in The routing process, their IP addresses must be used.[3] Higher-level directories, such as X.500/LDAP, consistently Map properties to objects which are uniquely identified by Their distinguished name (DN), i.e., their position in the X.500 tree [4].

**D. CONTENT BASED PUBLISH/SUBSCRIBE:** Content-based networking is a generalization of the content based publish/subscribe model. [4] In content-based networking, messages are no longer addressed to the communication end-points. Instead, they are published to a distributed information space and routed by the networking substrate to the “interested” communication end-points. In most cases, the same substrate is responsible for realizing naming, binding and the actual content delivery [5].

**E. SECURE KEY EXCHANGE:** A key-exchange (KE) protocol is run in a network of interconnected parties where each party can be activated to run an instance of the protocol called a session [6]. Within a session a party can be activated to initiate the session or to respond to an incoming message. As a result of these activations, and according to the specification of the protocol, the party creates and maintains a session state, generates outgoing messages, and eventually completes the session by outputting a session-key and erasing the session state [7].

## 3. SYSTEM WORKFLOW AND ALGORITHM

### 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 $\Omega$, 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.

**B.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.

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 [7].

**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.

## PROPOSED SYSTEM

The classical cryptosystems uses same keys for encryption and decryption. Both keys are kept are kept secret. The problems of this traditional cryptosystems were distribution of keys and key management. A paradigm is shifted towards public key cryptosystem [3]. In which different keys are used for encryption and decryption. One key being public and other as private. These schemes also possess some operational issues. For management of keys Public key infrastructure is maintained. But traditional PKI needs to maintain large number of keys. IBE provides alternative to reduce amount of keys to store. The private key generator is used as trusted third party. It is also called as key server. At the start first PKG generates pair of keys, public keys and private key. The public key is available users. These keys are called master public keys and master private keys[3].

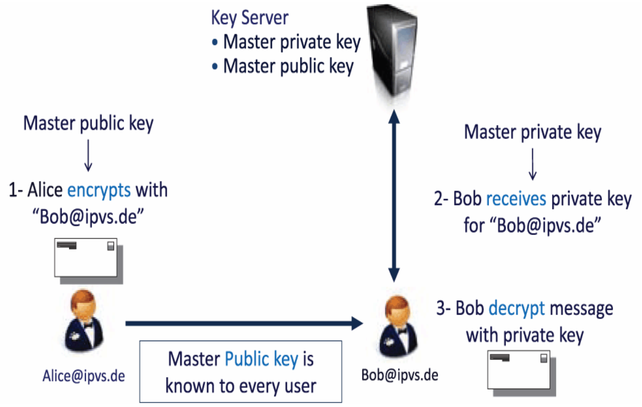

Figure 2: System Workflow

1) Sender, Alice in this case, creates plaintext message for receiver, bob. The message is sent from sender to receiver[6]. Alice uses some credentials for encrypting message that includes Bob's identity, public key of PKG, and cipher text is encrypted.

2) Bob receives cipher text from Alice. While transmitting cipher text some plaintext information is also sent with that. This information is used for receiving private key from PKG to decrypt message. Bob also required authenticating with PKG by sending credentials such as Identity of Bob. After that PKG transmits Bob's private key over a secure channel.

3) For ex. E-mail address can be used as public key.

4) Bob decrypts cipher text using his private key to recover plaintext message.

5) As PKG maintains single Master public keys and Master Private Keys, so it can be used as smart card. A pairing based cryptography is used for implementation of IBE. A mapping is established between to cryptographic groups by means of bilinear maps. Let G1 and G2 be cyclic group of order q, where q is some large prime

G2->E: G1 x G1 this bilinear graph satisfies Bilinearity, No degeneracy and Computability properties [9].

## 4. CONCLUSION

We have proposed a new approach to provide authentication and confidentiality in a broker-less content based pub/sub system. We have developed mechanisms to assign credentials to publishers and subscribers according to their subscriptions and advertisements. Private keys assigned to publishers and subscribers, and the cipher texts are labeled with credentials. The paper demonstrates the feasibility of the proposed security mechanisms and analyzes attacks on subscription confidentiality.

## REFERENCES

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

[2] Antonio Carzaniga, Michele Papalini, Alexander L. Wolf “Content-Based Publish/Subscribe Networking and Information-Centric Networking”.

[3] J. Bethencourt, A. Sahai, and B. Waters, “CiphertextPolicy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy, 2007.

[4] D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology, 2001.

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

[6] L. Opyrchal and A. Prakash, “Secure Distribution of Events in Content-Based Publish Subscribe Systems,” Proc. 10th Conf. USENIX Security Symp., 2001.

[7] L.I.W. Pesonen, D.M. Eyers, and J. Bacon, “EncryptionEnforced Access Control in Dynamic Multi-Domain Publish/Subscribe Networks,” Proc. ACM Int’l Conf. Distributed Event-Based Systems (DEBS), 2007.

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

[9] A. Shikfa, M. O ¨ nen, and R. Molva, “PrivacyPreserving 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.

## ABOUT AUTHORS

**C.RATNA PRABHA** received B,Tech degree in Computer Science and Engineering from G.Pullaiah College of Engineering and Technology (JNTUA)and now pursuing M.Tech (CSE) from Ravindra College of Engineering for Women(JNTUA). Research interest includes Secure Computing.

**Mrs. P.RAGHA VARDHANI,** received B.Tech (CSE) degree from Vaagdevi Institute of Technology & Science and M.Tech (CSE) from Vaagdevi Institute of Technology & Science. Currently she is working as Assistant Professor in Department of Computer Science and Engineering in Ravindra college of Engineering for Women, Kurnool. She has lifetime membership in Indian Institute of Technical Education (ISTE).