ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
*A Peer Reviewed Open Access International Journal*

# Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption

**Karnewar Vijaya Laxmi**
M.Tech Student,
Department of CSE,
AMR Institute of Technology,
Mavala, T.S, India.

**Mr. A. Hanuman Prasad**
Associate Professor
Department of CSE,
AMR Institute of Technology,
Mavala, T.S, 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.***

## 1.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 endto-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.

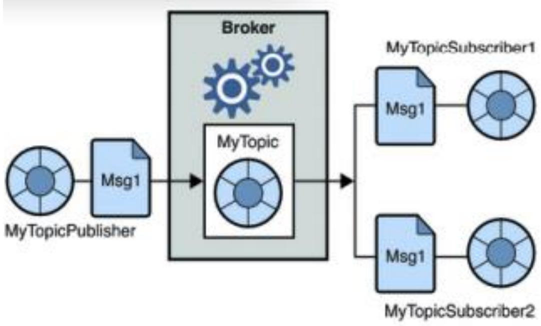


Fig 1 Public/Subscriber system

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.

## 2. RELATED WORK

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 coordinate 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 textPolicy 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 secretsharing 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.

## 3. 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.

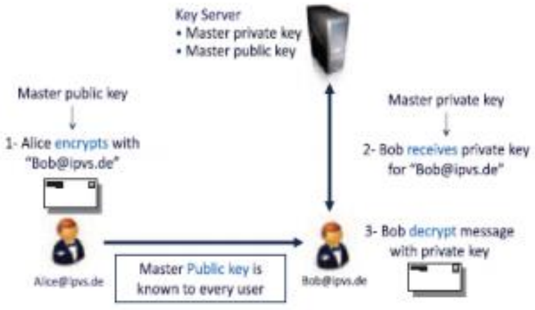

Key Server
• Master private key
• Master public key
Master public key
1- Alice encrypts with "Bob@ipvs.de"
Master private key
2- Bob receives private key for "Bob@ipvs.de"
3- Bob decrypt message with private key
Alice@ipvs.de
Master Public key is known to every user
Bob@ipvs.de

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

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

server maintains a pair of public and private master keys.

## 4. PROPOSED SCHEME

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

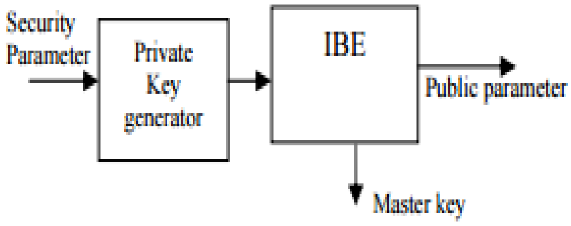


Fig 3 Setup

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.

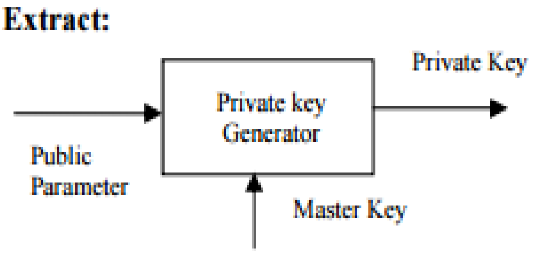


Fig 4 Extract

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.

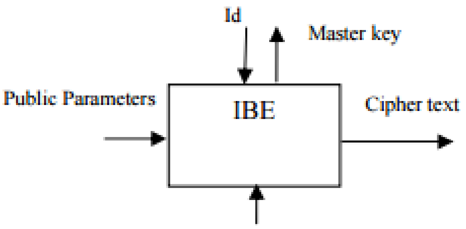


Fig 5. Encryption

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.

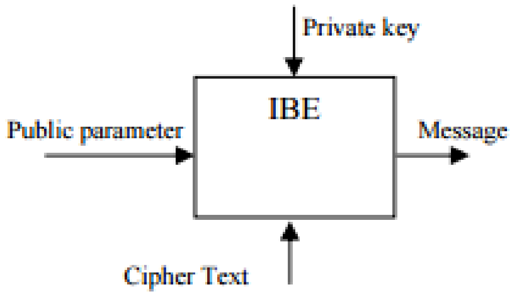


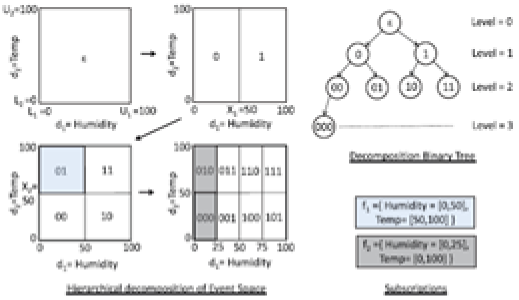
Fig 6 Decryption

## 5.CREATION OF CREDENTIALS

In the following, we will first describe the creation of credentials for numeric and string attributes. Further extensions to handle complex subscriptions are discussed subsequently.

### 5.1 Numeric Attributes

The event space, composed of d distinct numeric attributes, can be geometrically modeled as a d-dimensional space such that each attribute represents a dimension in the space. With the spatial indexing approach, the event space is hierarchically decomposed into regular subspaces, which serve as enclosing approximation for the subscriptions, advertisements, and events. The decomposition procedure divides the domain of one dimension after the other and recursively starts over in the created subspaces. Fig. 3 visualizes the advancing decomposition with the aid of a binary tree. Subspaces are identified by a bit string of “0” and “1”s. A subspace represented by $dz_1$ is covered by the subspace represented by $dz_2$, if $dz_2$ is a prefix of $dz_1$. Subscription or advertisement of a peer can be composed of several subspaces. A credential is assigned for each of the mapped subspace. For instance, in Fig. 3, $f_2$ is mapped to two subspaces and therefore possesses two credentials f000; 010g. An event can be approximated by the smallest



## 5.2 String Attributes

The above spatial indexing technique can work with any ordered data type with a known domain. String attributes usually have a maximum number of characters. This allows them to have known bounds. They can be linearized by hashing or other linearization mechanisms and, thus, can also be indexed [24].

Credentials for more expressive string operations such as prefix matching can be generated using a trie. Each node in the trie is labeled with a string, which serves as a common prefix to all its descendants, as shown in Fig. 4. Each peer is assigned a single credential, which is same as its subscrip-tion or advertisement.

## 6 Publisher / Subscriber Authentication And Event Confidentiality

The security methods describe in this section are built upon ciphertext-policy attribute-based encryption (in short CP-ABE) scheme proposed by Bethencourt et al. [4]. In particular, our modifications 1) allow publishers to sign and encrypt events at the same time by using the idea of the identity-based signcryption proposed by Yu et al. [25], 2) enable efficient routing of encrypted events (from publishers to subscribers) by using the idea of searchable encryption proposed by Boneh et al. [5], and 3) allow subscribers to verify the signatures associated with all the attributes (of an event) simultaneously. Our modifications do not change the basic structure of the CP-ABE scheme and preserves the same security strength, as discussed in the supplemental document available online.

### 6.1 Receiving Events

Decryption. On receiving the ciphertexts, a subscriber tries to decrypt them using its private keys. The ciphertexts for each attribute are strictly ordered according to the containment relation between their associated credentials; therefore, a subscriber only tries to decrypt the ciphertext whose position coincides with the position of its credential in the containment hierarchy of the corresponding attribute. The position of a credential can be easily determined by calculating its length. For example, for a numeric attribute, credential 0000 occupies fourth position in the containment hierarchy, i.e., after 0, 00, and 000. Subscribers decrypt the ciphertext in the following manner: Step 1. The symmetric key SK is retrieved from the ciphertext CT1 by performing the following pairing-based cryptographic operations:

$$DT = \frac{\left(\prod_{i=1}^{d} \frac{\hat{e}(Pr^{s}_{i,\tau_i}[1],CT_i)}{\hat{e}(Pr^{s}_{i,\tau_i}[2],CT_{i,\tau_i})}\right) CT_1}{\hat{e}(CT_2, Pr^{s}[4])} = SK,$$

## 7. SUBSCRIPTION CONFIDENTIALITY

In this section, we address to achieve subscription con-fidentiality in a broker-less pub/sub system.

### 7.1 Publish/Subscribe Overlay

The pub/sub overlay is a virtual forest of logical trees, where each tree is associated with an attribute (cf. Fig. 5).

TABLE 1
Cost of Security Methods

| | Public params | Private keys | Ciphertext Size | Encryption cost | Decryption cost | Sign cost | Verification cost |
|---|---|---|---|---|---|---|---|
| Numeric | $O(1)$ | $O\left(\sum_{i=1}^{d} \log_2 \mathcal{Z}_i\right)$ | $O\left(\sum_{i=1}^{d} \log_2 \mathcal{Z}_i\right)$ | $O\left(\sum_{i=1}^{d} \log_2 \mathcal{Z}_i\right)$ | $O(d)$ | $O(d)$ | $O(d)$ |
| String | $O(1)$ | $O\left(\sum_{i=1}^{d} \mathcal{L}_i\right)$ | $O\left(\sum_{i=1}^{d} \mathcal{L}_i\right)$ | $O\left(\sum_{i=1}^{d} \mathcal{L}_i\right)$ | $O(d)$ | $O(d)$ | $O(d)$ |

subscriber joins the trees corresponding to the attributes of its subscription. Similarly, a publisher sends an event on all the trees associated with the attributes in the event. Within each attribute tree, subscribers are connected according to the containment relationship between their credentials associated with the attribute. The subscribers with coarser credentials (e.g., the ones mapped to coarser subspaces in case of numeric attributes) are placed

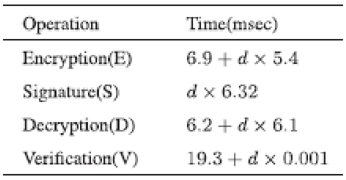
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

near the root of the tree and forward events to the subscribers with finer credentials.

## 8.PERFORMANCE EVALUATIONS

We evaluate three aspects of our system: 1) quantifying the overhead of our cryptographic primitives, 2) benchmarking the performance of our secure pub/sub system, and 3) analyzing attacks on subscription confidentiality. Here, we only discuss the first two aspects and the evaluations related to the analysis of subscription confidentiality are available in the supplemental document available online Experimental Setup. Simulations are performed using PeerSim [11]. Simulations are performed for up to N ¼ 2; 048 peers. Unless otherwise stated, out-degree constraints of the peers are chosen as log$_2$ðNÞ. The delays between the communication links are chosen in the range [24 and 134 ms]. The complex subscriptions used during the evaluations contain conjunction of predicates defined on up to d ¼ 16 different attributes. We evaluate the system performance under uniform (WL$_1$) and skewed (WL$_2$) subscription workloads, and with a uniform and skewed event distribution. Skew is simulated using the widely used 80-20 percent Zipfian distribution with three to five hot spots. The security mechanisms are implemented by the pairing-based cryptography library [14]. The implementa-tion uses a 160-bit elliptic curve group based on the supersingular curve y$^2$ ¼ x$^3$ þ x over a 512-bit finite field.

TABLE 3
Computation Times for Publishers and Subscribers



| Operation | Time(msec) |
|---|---|
| Encryption(E) | $6.9 + d \times 5.4$ |
| Signature(S) | $d \times 6.32$ |
| Decryption(D) | $6.2 + d \times 6.1$ |
| Verification(V) | $19.3 + d \times 0.001$ |

## 8.1Performance of Cryptographic Primitives

In this section, we measure the computational overhead of our security methods. All of our measurements were made on a 2-GHz Intel Centrino Duo with 2-GB RAM, running Ubuntu 9. Table 2 shows the throughput of the cryptographic primitives to perform encryption, decryp-tion, signature, and verification. All reporting values are averaged over 1,000 measurements. In our system, pairing-based encryption is used to encrypt a random key SK, which is later used to decrypt the actual event using symmetric encryption (cf. Section 5.3). Therefore, the an overhead of approximately 230-300 ms due to security mechanisms. Our evaluations with higher number of attributes indicate that the average connection delay experienced by a subscriber is independent to the number of attributes.

## 9. CONCLUSION

In this paper, we have presented a new approach to provide authentication and confidentiality in a broker-less content-based pub/sub system. The approach is highly scalable in terms of number of subscribers and publishers in the system and the number of keys maintained by them. In particular, 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 ciphertexts are labeled with credentials. We adapted techniques from identity-based encryption 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 its private keys and 2) to allow subscribers to verify the authenticity of received events. Furthermore, we developed a secure overlay maintenance protocol and proposed two event dissemination strategies to preserve the weak subscription confidentiality in the presence of semantic clustering of subscribers. The evaluations demonstrate the viability of the proposed security mechanisms and analyze attacks on subscription confidentiality.

## 10.ACKNOWLEDGEMENTS

I am **KARNEWAR VIJAYA LAXMI** and would like to thank the publishers, researchers for making their resources material available. I am greatly thankful to Associate Prof**: MR. A. HANUMAN PRASAD** for their guidance. We also thank the college authorities, PG coordinator and Principal for providing the required infrastructure and support. Finally, we would like to

extend a heartfelt gratitude to friends and family members.

## 11.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.

**Miss KARNEWAR VIJAYA LAXMI.** MTech student, in M.Tech Student, Dept of CSE in **Amr Institute of Technology**, mavala, T.S, India

**Mr.A. HANUMAN PRASAD** working as a Associate at **Amr Institute of Technology**, mavala, T.S, India, Graduate from JNTUH Hyderabad. He has 2 years of UG/PG Teaching Experience

‘