Improving Security of Publish/Subscribe System Using HASBE

Gokula Nath G[1], Syamamol T[2]

Abstract— **Publish/subscribe system is a wide-area communication infrastructure which allows data distribution across potentially unlimited number of publishers and subscribers. Published events are routed to their corresponding subscribers without knowing the relevant set of subscribers or vice-versa. Publishers and subscribers are organized in a broker-less routing infrastructure. Achieving basic security mechanisms such as authentication and confidentiality is highly challenging in pub/sub system, due to the loose coupling of publishers and subscribers. The proposed scheme, Hierarchical Attribute Set Based Encryption improves security of the data that based on a set of attributes. In addition to the previous work, this paper contributes 1) more flexibility and scalable with growth of data sharers, 2) cost of achieve, change and update access policy is relatively lower and 3) provide file addition, file deletion and user revocation. Moreover, the evaluations show that providing security is affordable w.r.t the event publication and dissemination delay.**

Index Terms— **Broker-less, DES, DSA, Hierarchical Attribute Set Based Encryption, Identity Based Encryption, Pub/Sub.**

I. Introduction

Publishers/subscribe system [2] is a highly-decoupled system in which there is no direct contact between publishers and subscribers. In such a system, publishers publish the events and subscribers have the ability to express their interest in form of events, or a pattern of events by sending the subscription to the publish/subscribe network. Pub/sub system gained high popularity because of this decoupling, enabling a many-to-many communication paradigm and which separates resource management from access control and ownership. Publishers inject information into the system and which is routed towards the relevant subscribers. In the traditional case, it is ensured by the intermediate routing over a broker network [6]. In more recent systems, publishers and subscribers are organized in a broker-less routing infrastructure. Publishers own the content of published event and responsible for denying access control over the event.

Fig.1. Pub/Sub System Network

.

Content based pub/sub is a variant in which subscriptions define based on the message content. Its expressiveness is particularly useful for large-scale distributed applications. Pub/sub system needs to provide basic security mechanisms such as access control and confidentiality. Access control in the sense means that only authenticated publishers are allowed to publish events into the network and only those events are delivered to authorized subscribers. Authentication of publishers and subscribers are difficult to achieve because of the loose-coupling between both of them.

Contents of events are not exposed to the infrastructure and a subscriber should receive all relevant events without revealing its subscription to the system. For instance, end-to-end authentication using a Public Key Infrastructure (PKI) conflicts with the loose-coupling between publishers and subscribers. But there is a problem that the subscribers must know the public key of all relevant publishers to verify the authenticity of received events.

Identity Based Encryption (IBE) [1], an approach to the problem of key management was introduced. IBE can use any arbitrary string as the public key and is generated based on a single identity of user such as email id or user id, which is not much secure. This paper presents a new approach to provide authentication and confidentiality in a broker-less publish/subscribe system, which is much more secure. HBASE, Hierarchical Attribute Set Based method also provides strong access control and user revocation in which keys are generated based on the set attributes.

Most of the existing approaches of publish/subscribe system done based on the presence of a traditional broker network [10], [2], [5], [13], [9]. These address security under limited expressiveness such as for example, by using matching of keywords for routing events [13], [11].

Manuscript received Feb, 2013.
***Gokula Nath G**, CSE, M G University*
***Syamamol T**, CSE, M G University*

Moreover, these cannot provide fine-grained access control in scalable manner [13], [10]. On the results of [12], this paper provides authentication and confidentiality in publish/subscribe system with much more security than Identity Based Encryption [1], [4], [7]. In IBE, the keys are generated based on a single identity, so that it is not much secure.

II. Related Work

There are two entities in the system: publishers and subscribers. Both the entities are bounded and do not trust each other [11], [13]. Moreover, all the publishers or subscribers participating in the network are honest and do not deviate from the specific protocol. There are two major goals for the proposed pub/sub system, such as authentication and confidentiality.

Authentication [5]: To avoid no eligible publications, only authorized publishers should be able to publish events in the system. Similarly, only authenticated subscribers should receive those messages.

Confidentiality [5]: In a broker-less environment, two aspects of confidentiality are: 1) events are only visible to authorized subscribers and are protected from illegal modifications, and 2) subscriptions of subscribers are confidential.

Two convincing paradigms have emerged for achieving scalability in widely distributed systems: publish/subscribe communication and role-based [2]. In the publish/subscribe paradigm, a principal takes the role of a publisher and/or a subscriber. Subscribers register their interest in receiving an event through a subscription. Publishers produce events without any dependence on subscribers. Principals connect to the publish/subscribe middleware to communicate. This occurs through an event broker, which routes events from publishers to subscribers.

The method enables efficient routing of events in the system, which is known as searchable encryption [3]. It deals with the problem of searching on data that is encrypted using a public key system. Here constructing a PEKS is related to Identity Based Encryption (IBE) [14]. Attribute Based Encryption is one of the encryption methods [4], which deals with the fine-grained sharing of encrypted data. PADRES [6], the publish/subscribe model with the capability to correlate events, uniformly access data produced in the past and future, balance the traffic load among brokers, and handle network failures.

Cipher text-Policy Attribute-Based Encryption [7], a system for realizing complex access control on encrypted data. Here, a user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message in our system, they specify an associated access structure over attributes. A user will only be able to decrypt a cipher text if that user's attributes pass through the cipher text's access structure. The main objective here attain is collusion-resistance: If multiple users collude, they should only be able to decrypt a cipher text if at least one of the users could decrypt it on their own.

In [8], introduce a method for creating public key broadcast encryption system. The main technical innovation is based on a new "two equation" technique for revoking users. Here create public key revocation encryption systems with small cryptographic private and public keys. The primary challenge in constructing broadcast encryption schemes is to achieve full collusion resilience.

Furthermore, existing approaches use coarse-grain epoch based key management and cannot provide fine-grain access control in a scalable manner [10], [13]. Content-Based Publish/Subscribe (CBPS) [10] is an interaction model where the interests of subscribers are stored in a content-based forwarding infrastructure to guide routing of notifications to interested parties

Identity-Based Encryption (IBE) [1], [12], [15] takes a breakthrough approach to the problem of encryption key management. IBE can use any arbitrary string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the dynamic generation of private decryption keys that correspond to public identities and the key servers base root key material. A key server provides credentials to the users and in turn receives 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.

III. Hierarchical Attribute Set Based Encryption

In this paper propose a hierarchical attribute-set-based encryption (HASBE) scheme for access control include computing. The contribution of the paper is multifold. First, ASBE algorithm with a hierarchical structure improves scalability and flexibility while at the same time inherits the feature of fine-grained access control of ASBE. Second, the scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in server computing. In IBE [1], the key generation is done based on a single id of user. Therefore the method is not much secure and the key is easily breakable. If the key is compromised, all the information related to that particular key is accessed by the malicious user.

To improve the security of the method, introduce an approach known as HASBE, in which the key is generated based on number of attributes. Attribute in the sense means file size, file name, customer name etc. For providing security mechanisms in pub/sub, leverage the principles of hierarchical attribute set based encryption to support many-to-many interactions between subscribers and publishers.

The HASBE algorithm consists of four operations:
1. Setup, which initializes a key server
2. Encrypt, which encrypts a message for a given user
3. Key Generation, which generates a private key for a given user based on a set of attributes
4. Decrypt, which given a public key, decrypts a message.

Here hierarchical in the sense means, there are a two level approach such as a key generator in the first level and the users such as publishers and subscribers in the next level to form a hierarchy.

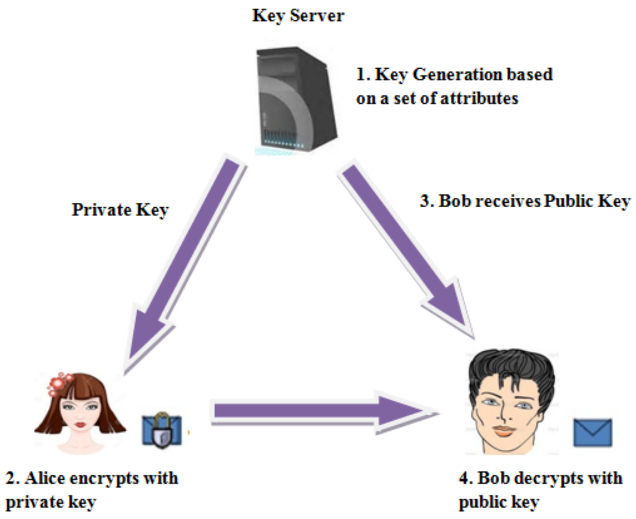
Key Server
1. Key Generation based on a set of attributes
Private Key
3. Bob receives Public Key
2. Alice encrypts with private key
4. Bob decrypts with public key

Fig. 2 System Architecture

In normal asymmetric key encryption, a public key is used for encryption and the corresponding private key is used for decrypting the data. But it doesn't create the digital signature. So to achieve this, here encrypts the message using its own private key instead of some ones public key. Then decryption is based on the corresponding public key so that the receiver can ensures that the message was originated from the authorized sender by signing the message with the sender. Thus it creates the digital signature.

Algorithm:

In HASBE algorithm, there are mainly three important phases: Key Generation, Encryption and Decryption. Here, the key generation is done based on a set of attributes by using Digital Signature Algorithm (DSA) [17]. Encryption is done using Data Encryption Standard algorithm (DES) [16].

1. Key Generation

1. Choose a set of attributes such as file size, user id etc.
2. Choose key size length as N.
3. If the file size is between 0 and n-1 for some n, then choose an N-bit prime number less than n as p.
4. If the user id is between 0 and m-1 for some m, then choose an N-bit prime number less than m as q.
5. Choose g such that it is a number and a primitive root of p.
6. Choose x, a prime number by some random method, 0< x< q.
7. Calculate y = gx mod p as like in DSA [17].
8. Private Key (Pr) is x and public Key (Pb) is y.

2. Encryption

1. Convert Pr and plain text into binary form.
2. Choose Pr and data as the inputs for DES algorithm [16].

3. Decryption

Decryption is also done using the inverse form of DES algorithm. Use the cipher text and Pb as the input to the DES algorithm but use the keys Ki in reverse order. That is, use K16 on the first iteration, K15 on the second until K1 which is used on the 16th and last iteration. Decryption is done only if the public key is match with the private key. Advantages of HASBE is that: (1) Member Organization and Member Deletion (2) Provides strong access control (3) Very flexible to operate and scalable with the growth of data sharers (4) The cost of achieve, change and update access policy is relatively lower (5) Avoid data replication/duplication (6) Provides file addition, file deletion and user revocation (7) and also the system is much more secure than IBE. So that the proposed method is better than IBE and at the same time inherits the feature of fine-grained access control of attribute based encryption. The subscriber can access the data only if the publisher activated them. Thus it also provides user revocation by deactivating the revoked user.

IV. Experimentation And Results

The performance and scalability of the proposed pub/sub system evaluate only with respect to the security mechanisms by omitting other aspects and also evaluate the performance with respect to the event dissemination delays.

Experimental setup Simulations are performed up to N = 1024 peers. Average event publication delay with publishers between the communication links are chosen in the range [0 and 8 sec]. Average event dissemination delays with subscribers are also chosen in this range.

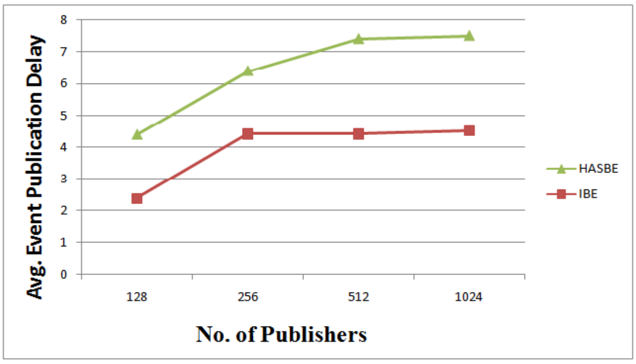

Fig: (a) measures the average time needed by the publisher to publish the events in the system. In this graph, the average time to publish the event increases with the number of publishers. For each publisher, the time is measured from the publication of the event till it is successfully encrypted and verified by the server. Fig: (b) shows that the average time to disseminate an event increases with the number of peers in the system because of the increase in number of the relevant subscribers.

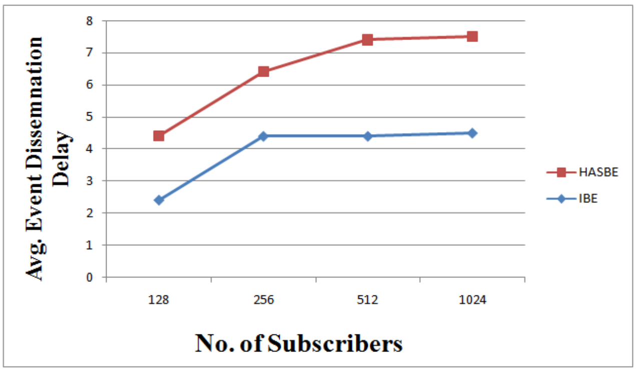

Fig: (b)

Fig. 3 Performance Evaluations

From the graph above, it should be clear that: (1) HASBE method is much more secure than IBE (2) Average time for publish/disseminate the events are increases with the number of publishers/subscribers. In IBE, the keys are generated based on a single identity of user. So that it is not much secure. To improve the security of the method by generating the keys based on the set of attributes, which is known as HASBE. These improvements in terms of publishers and subscribers are understood from the above graph.

V. CONCLUSION

Hierarchical Attribute Set Based Encryption provides authentication and confidentiality in broker-less pub/sub system. The method is highly scalable and flexible in terms of operation and number of data sharers. Main attraction is that it is more secure than Identity Based Encryption and avoids file duplication. The approach provides user revocation by deactivating the revoked user and ensures that a particular subscriber can decrypt an event only if there is a match between the credentials associated with the event. The method also provides strong access control and have low overhead due to the changes and updating in access policy. The scheme provides full support for hierarchical user grant, file creation and file deletion. The evaluations demonstrate the viability of the proposed security mechanisms in compared with Identity Based Encryption. Here the publisher has the ability to route the event to a selective user, so that no other users can access the data from the system.

ACKNOWLEDGMENT

The first author would like to thanks all those people, who guided and supported. Without their valuable guidance and support, this task was not possible and also likes to thank colleagues for their discussions and suggestions.

REFERENCES

[1] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel, “Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption”, *IEEE Transactions on parallel and distributed systems, vol. 25, NO.2, pp. 518-528, 2014.*

[2] J. Bacon, D.M. Eyers, J.Singh and P.R. Pietzuch, “Access control in Publish/Subscribe System,” *Proc.Second ACM Int’l Conf. Distributed Event-Based Systems (DEBS), 2008*

[3] 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, 2004.*

[4] 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.*

[5] M. Ion, G. Russello, and B. Crispo, “Supporting Publication and 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. Kazhemzadeh, “The PADRES Publish/Subscribe System,*” Principles and Applications Of Distributed Event-Based Systems.IGI Global,2010.*

[7] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” *Proc. IEEE Symp.Security andPrivacy, 2007.*

[8] A. Lewko, A Sahai, and B. Waters, “Revocation Systems with Very Small Private Keys,” *Proc. IEEE Symp Security and Privacy, 2010*

[9] 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.*

[10] 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.*

[11] A. Shikfa, M. Onen and R. Molva,”Privacy-Preserving Content-Based Publish/Subscribe Networks*” Proc. Emerging Challenges for Security, Privacy and Trust, 2009.*

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

[13] 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.*

[14] Y. Yu, B. Yang, Y. Sun, and S. I. zhu, “Identity Based Encryption with Random Oracles,” *Computer Standards and Interfaces, vol. 31, pp. 56-62, 2009*

[15] Handore Jayshree Shrikant, Prof. Shivaji R. Lahane, “A Review on a Highly Scalable Privacy Preserving Content-Based Publisher/Subscriber System using Event Based Encryption,” *International Journal for Computer Science and Information Technologies, vol. 5 (6), 2014*

[16] W. C. Barker and E.B. Barker, “Sp 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm Block Cipher,” *technical report, Nat’l Inst. of standards and Technology, 2012*

[17] P. Kitsos, N. Sklavos and O. Koufopavlou,”An efficient implementation of Digital Signature Algorithm,” *VLSI design laboratory, electrical and computer Engineering Department, University of Patras*

Gokula Nath G, Department of Computer Science & Engineering, Mangalam college of Engineering, Ettumanoor, Kerala, India.

Syamamol T, Assistant Professor, Department of Computer Science and Engineering, Mangalam college Of Engineering, Ettumanoor, Kerala, India.