www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13615-13617

Efficient Publish/Subscribe System Using Identity Based Encryption

[1]Prathyusha M. Kumar., [2]Mumthas T.K.

[1] M-Tech Student, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
prathyushamkumar@gmail.com

[2] Assistant Professor, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
mumthastk@gmail.com

Abstract: ***Publish/Subscribe (pub/sub) system is an emerging communication paradigm that offers efficient and decoupled information dissemination in distributed environments. Decoupling increases the privacy of each participants in the system . Publishers generate the flow of information as publications of interests expressed as subscriptions. The perfect decoupling is maintained by using the pairing based cryptographic mechanisms. The provisioning of basic security mechanisms such as authentication, confidentiality, access control are highly challenging in a content based publish/subscribe system. This work proposes a novel approach to provide confidentiality , authentication and access control in a brokerless content based publish/subscribe system using Hierarchical CP -ABE (Ciphertext Policy Attribute Based Encryption) scheme. So the new Publish/Subscribe system is very efficient with less computational time for cryptographic operations and also provide fine grained access control hierarchically.***

Keywords: **Content based, Brokerless, publish/subscribe, security.**

1. Introduction

The publish/subscribe (pub/sub) communication paradigm has gained high popularity because of its inherent decoupling of publishers from subscribers in terms of time, space, and synchronization. Publishers inject information into the pub/sub system, and subscribers specify the events of interest by means of subscriptions. Published events are routed to their relevant subscribers, without knowing the relevant set of subscribers. An important characteristic of the publish-subscribe system is the decoupling between publishers and subscribers in time, space, and flow. This decoupling improves the scalability and the effectiveness of the system.

1.1 Content Based Publish/Subscribe System

For the transfer of an event message from publishers to the relevant subscribers, we use the content-based data model. An event is matched against a subscription if the values of attributes in the event satisfy the corresponding constraints imposed by the subscription.

1.2 Security in Publish/Subscribe System

Authentication: To avoid non eligible publications, only authorized publishers should be able to publish events in the system. Similarly, subscribers should only receive those messages to which they are authorized to subscribe. To ensure authentication and integrity digital signature is used.

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

Key management: It is the creation, distribution and maintenance of a secret key

Access control: In access control systems, users must present credentials before they can be granted access.

2. Related works

Researchers are always been conducted to improve efficiency of publish subscribe systems. Here briefly presents different publish subscribe systems and encryption methods used in this area. M. Srivatsa et.al [1] introduced Event guard framework to provide confidentiality in publish/subscribe communication. Safeguarding the publisher subscriber overlay services from various vulnerabilities and threats. Tokenization technique is used here for event confidentiality with token, key and signature. Here token is created for each topic. Message is encrypted using secret encryption key. Encryption is done using symmetric key algorithm. Digital signatures concept is also used for signing. A subscriber subscribes for a topic and the matched topic is decrypted using symmetric key and digital signature is verified. It is having good publication Confidentiality but only supports topic based search. Khurana H. [2] introduced a scheme that does not require publishers and subscribers to share a key, but does not achieve full confidentiality of events. The secure pub/sub system requires the presence of trusted servers that will host a proxy security and accounting service (PSAS). Distribution of keys to

authorized subscribers is done using proxy encryption. Proxy re-encryption service changes the encryption of key, k to an encryption with the public key of the subscriber. Subscriber can easily decrypt using private key. But it does not achieve full confidentiality of events. Raiciu et.al [3] introduced an efficient publish subscribe system in which the data sharing is achieved by Equality Encrypted Matching technique. Here the publication attribute a and subscriber constraint c . Applying a K-keyed pseudo random function, F on a and c. FK(a) and FK(c) are used as keys to encrypt a common random value (using the same function F). If the cipher texts are similar then the matching can be successful. The matching is performed by intermediate Broker. Fast dissemination of events can be possible . Fast dissemination of events can be possible in this scheme. Scalable key management is also done here. Choi et.al [4] introduced a new publish subscribe system using data transformation method called Asymmetric Scalar-product Preserving Encryption (ASPE). The data confidentiality is achieved by using a new data transformation method called Asymmetric Scalar-product Preserving Encryption (ASPE). Encryption of publication in which publisher sends publication to the trusted authority . ASPE uses an invertible matrix. After Encryption publication send to broker and it stores data from Publishers and sends it when a subscription covers it. The advantage is identified by authors is fast dissemination of events but may not provide scalability. ASPE uses an invertible matrix. Trusted Authority (TA) generates Matrix every minute. Publisher sends publication to the trusted authority. The publication is encrypted with the matrix and sends to broker. The subscriber encrypts the request with inverse of the matrix. The matching of data occurs when the products of these ciphertexts are got one. ASPE is a secret-key algorithm, which naturally needs that the key information be distributed among participants. It is Vulnerable to attacks and it does not support scalable key management. Ion M. et.al [5] introduced a new publish subscribe system using data Attribute Base Encryption (ABE). In this scheme the main use of the paradigm is in encrypting the publication payload. The publications can be decrypted only if an access policy associated with the subscriber that receives them is satisfied. The access policy sets a specific structure for the subscription constraints.

3. Proposed work

In this section a new an efficient Publish subscribe system is introduced which is the modified the method of existing publish/ subscribe system. The modification is done to reduce the computational time and to provide access control hierarchically. With the recent adoption and diffusion of the data sharing paradigm in distributed systems there have been increasing demands and concerns for distributed data security. With the development of cryptography, the attribute based encryption (ABE) draws widespread attention of the researchers in recent years. Ciphertext policy attribute based encryption (CP-ABE) is a cryptographic solution to provide data confidentiality and expressive access control at the same time. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. In existing system CP-ABE scheme is used for data sharing in brokerless publish/subscribe system. Traditionally there is an intermediate broker between each publisher and subscriber. In this system there is no need of broker between the publisher and subscriber by the use of CP-ABE scheme. In this scheme publishers and subscribers interact with a key server. Key server is the key generation center for key storage . They provide credentials to the key server and in turn receive keys with respect to the credential. Data sharing is mainly based on the concept of Identity Based Encryption . The Ciphertext policy attribute-based encryption (CP-ABE) is based on Identity Based Encryption scheme. Pairing-based cryptography (PBC) has laid the foundation of practical implementation of Identity Based Encryption . PBC establishes a mapping between two cryptographic groups by means of bilinear maps. This allows the reduction of one problem in one group to a different usually easier problem in another group.

In existing system, publisher wants to publish an event message M , first step is generating a random key SK. The random key is encrypted using CP-ABE scheme. This is done for policy matching and key sharing. CP-ABE performed on SK for every attribute. Ciphertexts should be created for every credential with access policy. Subscriber can decrypt the SK only when the access policy matches. The message is encrypted using AES symmetric key algorithm with the key symmetric key SK . Finally the ciphertext is again secure with the help of digital signature(signing using sender's private key and verifying using sender's public key). Due to the loose coupling between publishers and subscribers, a publisher does not know the particular subscribers in the system and privacy is also maintained. Decoupling also increases scalability. The subscriber can decrypt the event only when the policy matches. But existing CP-ABE scheme have some problems., such as computation for cryptographic operations. Increasing the attributes in the policy will increase the computation time too. The other drawback of CP-ABE scheme is that it only support access control in single level. Hierarchical CP-ABE scheme is proposed to overcome all these issues and also provide fine grained access control.

When a publisher wants to publish an event the following steps are performed in this proposed scheme.

Step 1: Publisher generates a fixed length random key SK for each event.

Step 2: The File is encrypted with a symmetric encryption algorithm AES using key SK.

Step 3 : Sign the document using private key of the publisher.

Step 4: Hierarchical CP-ABE is performed on key, SK with respect the credential. For each credential a ciphertext should be created with the policy, so that a subscriber with any of these credentials should be able to decrypt the event.

Decryption: The subscriber can decrypt the data only if there is match between the policy and the key. The symmetric key , SK is retrieved from the ciphertext. Symmetric key SK is then used to file content from ciphertext.

Verification: A subscriber will only accept the message if it is from an authorized publisher. To check the authenticity of an event, subscribers use the public key.

Hierarchical CP-ABE Algorithm:

Setup: Public key , PK and Master key , MSK is generated in this phase.

Encryption : Encrypt the data using the public key and access policy. Here random key, SK is encrypted with access policy.

Key generation : Private key, TKS is generated with respect to this access policy from Master key.

Decryption : Administrator can decrypt all the files when the private key and policy matches. The Administrator first checks whether user is eligible for the data, which is administered by itself. If the user is eligible, it will forward the file. Users can decrypt the message only when it will get authorization from the Administrator.

So the new publish subscribe system is very efficient with less computational time for cryptographic operations and also provide good access control hierarchically, by this way fast dissemination of events can be possible and efficiency of the publish subscribe system is improved.

4. Results and Analysis

By evaluating these two systems based on the computational time provides the following result. Long computation time and average access control are the main drawbacks of existing scheme. Increasing the attributes in the policy will increase the computation time too. Also the existing CP-ABE scheme only support access control in single level. Once the modified scheme is implemented, introducing the proposed hierarchical scheme, it is found that the computation time for cryptographic operations is decreased and access control is improved. The following graph compare the computation time of the two systems . So fast dissemination of events can be possible and by this efficiency of the publish subscribe system is also increased.

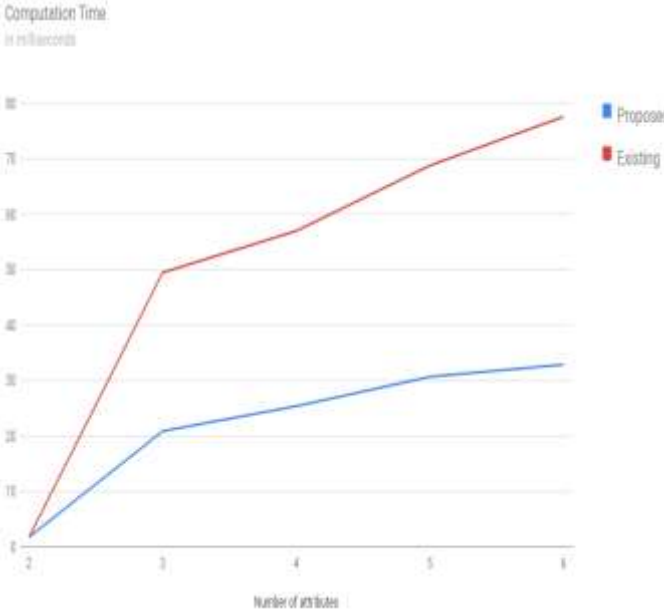

Figure 1: Computational time comparison

5. Conclusion

The existing Publish/Subscribe system provides authentication and confidentiality in a content based pub/sub systems. The approach is highly scalable in terms of number of subscribers and publishers. Long computation time and average access control are the main drawbacks of this publish subscribe system using CP-ABE scheme. Proposed method, which is the modified publish/subscribe system with Hierarchical CP-ABE scheme to overcome these problems effectively. The experimental results conclude that the proposed method reduces the computation time and also provide fine grained access control in hierarchical level.

References

[1] M. Srivatsa and L. Liu., "Securing publisher subscriber overlay services with event guard," ACM conf. on Computer and communications security, 2005

[2] Khurana H., "security and accounting services for content-based publish/subscribe systems," ACM symposium on Applied computing , Santa Fe,USA., 2005

[3] Raiciu C. and Rosenblum D. S., "Enabling Confidentiality in Content-Based Publish/Subscribe Infrastructures," IEEE Second CreatNet Intl Conf. Security and Privacy in Comm. Networks (SecureComm), 2006

[4] Choi S., Ghinita G., and Bertino E., "A privacy-enhancing content-based publish/subscribe system using scalar product preserving transformations, "Springer Berlin / Heidelberg, 2010

[5] Ion M.,Russello G., and Crispo B. , "Supporting publication and subscription confidentiality in pub/sub networks," IEEE in conference Security and Cryptography}, 2010

[6] M.A. Tariq, B. Koldehofe, and K. Rothermel , "Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption," IEEE Transactions on Parallel and Distributed systems,vol.25,no.2,February, 2014

[7] M.A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel , "Providing Basic Security Mechanisms in Broker-Less Publish/ Subscribe Systems," ACM Fourth Intl Conf. Distributed Event- Based Systems (DEBS), 2010

[8] J. Bethencourt ,A.Sahai and B.Waters, "Ciphertext-policy attribute based encryption," IEEE Symbosium on security and privacy,pp.321-334, 2007

[9] M.Nabeel ,N.Shang and E.Bertino, "Efficient privacy preserving content based publish subscribe systems," ACM symposium on access control Models and Technologies, 2012