ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 8, AUGUST 2015, PP 491-496

Augmenting Publish/Subscribe System by Identity Based Encryption (IBE) Technique

[1]Zunaira Begum,[2] M.Sri Lakshmi, [3]Dr S.Prem Kumar
[1](M.Tech), CSE, Assistant professor Department of Computer Science and Engineering
[2]Assistant Professor, Department of Computer Science and Engineering
[3]Professor & HOD, Department of computer science and engineering,
G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract: Security is one of the extensive and complicated requirements that need to be provided in order to achieve few issues like confidentiality, integrity and authentication. In a content-based publish/subscribe system, authentication is difficult to achieve since there exists no strong bonding between the end parties. Similarly, Integrity and confidentiality needs arise in published events and subscription conflicts with content-based routing. The basic tool to support confidentiality, integrity is encryption. In this paper for providing security mechanism in broker-less content-based publish/subscribe system we adapt pairing-based cryptography mechanism. In this mechanism, we use Identity Based Encryption (IBE) technique to achieve the needs of publish/subscribe system. This approach helps in providing fine-grained key management, effective encryption, decryption operations and routing is carried out in the order of subscribed attributes.

Keywords— Pairing-based cryptography, Key server, Credential, Publish/Subscribe.

1. INTRODUCTION

Common requirement for any system is security. The need for security must be extremely high. It is one of the major requirements to protect or control any sort of failures. There are number of mechanisms which are available to provide security. In that one of the most important mechanisms is encryption. In cryptography encryption is the process of converting plain text to cipher text which is unreadable from unauthorized users. The cryptography mechanism is required in publish/subscribe system. In publish/subscribe system publisher is one who publishes his content without specifying a particular destination to reach publisher will not program the documents to be delivered to a particular subscriber. Publisher will classify publishing documents based on different criteria and release it and subscriber will show interest on one or more documents and subscribe to that particular one in order to have access over it. This publish/subscribe system is traditionally carried out in broker-less [12] content based routing which forwards or routes the message based on the content of the message instead of clearly routing to a specified destination. Content based routing applies some set of rules to It's content to find the users who are interested in its content. Its different nature is helpful for huge-level scattered applications and also provides a high range of flexibility and adaptability to change. Authorized publisher have permission to publish events in the network and similarly subscribers who likes the content can gets subscribed to a particular published content and have access over it by which high level access control [7] can be achieved. Here published content should not be exposed to routing infrastructure and subscribers should receive content without leaking subscription identity to the system, which is a highly challenging task which needs to be carried out in content-based pub/sub system. Publisher and subscriber are the two entities and they do not trust each other. Even though authorized publisher publish events, nasty publisher pretend to be the real publisher and may spam the network with fake and duplicate contents similarly subscribers are very much eager to find other users and publishers which are challenging tasks. Finally, Transport Layer Security (TLS) or Secure Socket Layer (SSL) is secure channels for distributing keys from key server to the required. Existing security approach deals with traditional network and security is based on restricted manner which tells about key word matching [8]. Key management was the challenging task in the existing approach, so to overcome all these, we use new approach called pairing-based cryptography mechanism, which helps in mapping between to end parties so called cryptographic groups. Here, Identity Based Encryption Technique (IBE) [9] is used under this mechanism. New approach IBE provide greater concern towards authentication and confidentiality in the network. Our approach permit users to preserve credentials based on their subscriptions. Secret keys provided to the users are labeled with the credentials. In Identity-based encryption (IBE) mechanisms 1) key can be used to decrypt only if there is match between credentials with the content and the key; and 2) to permit subscribers to check the validity of received contents. Moreover, this approach helps in providing fine-grained key management, effective encryption, decryption operations and routing is carried out in the order of subscribed attributes.

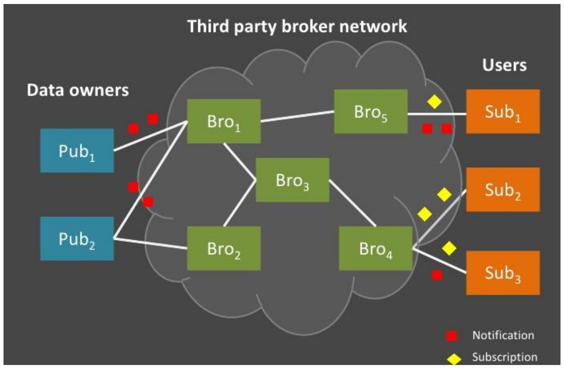

Fig 1. Subscriber/Publisher System

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 Identity (ID)-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 sub -state 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].

III. SYSTEM ARCHITECTURE

In this paper we come across Content-Based [10],[11] model for routing, that is published contents from the publishers to the appropriate subscriber we use content based model. Each event consists of a overall ordered set of attributes (A). For example attributes are of unique name, types of data, and its field. An event will have set of attributes and related standards. An event is matched next to a subscription, if the standards of attributes in the event suit the equivalent constraints required by the subscription. For the better and efficient confidentiality and authentication we use Identity Based Encryption (IBE) which is technique comes under pairing based cryptography mechanism which is the most efficient mechanism for provisioning of authentication and confidentiality.

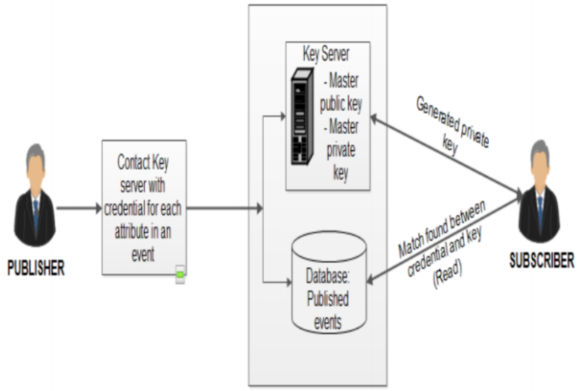
PUBLISHER
Contact Key server with credential for each attribute in an event
Key Server
- Master public key
- Master private key
Database: Published events
Generated private key
Match found between credential and key (Read)
SUBSCRIBER

Fig. 2. System Architecture.

Identity-Based Encryption (IBE) provides a good substitute method to decrease the amount of keys to be managed. In identity-based encryption, user's identity which is a valid string can be considered as the public key of the user.

A pair of master public key and master private key is maintained by the key server. Sender sends the encrypted message to a user with user's identity with the help of master public key. User in order to decrypt the message sent by the sender needs to obtain a private key for user identity Fig. 2. Shows the clear view of identity based encryption, whose properties are for extremely disseminated applications. For communication a sender needs to know about a single master public key with a unique identity likewise, to have the access over the message receiver needs to obtain private keys for its identity from the key server. In addition, a case of central key server can be simply fake inside the network. At last, a single pair of master keys maintained by the key server and hence which can be realized as a smart card provided to the user who are going to participate in the system. IBE comes under pairing-based cryptography which maps two cryptographic groups. For security mechanisms in publish/subscribe, we influence the ideology of identity-based encryption to carry more and more communications between subscribers and publishers. In IBE, publishers and subscribers act together with a key server Pub/sub give credentials to the key server to receive keys which fit for their suitable credentials. Then, for encrypt/decrypt those keys are used, and mark applicable contents in the content based pub/sub system, that is the credential becomes certified by the key server. Credential consists of binary string and a proof for its identity. Credential is used for verification against the key server and verifies the identity of the end user. The keys will be in cipher text format which are labeled with credentials assigned to publishers and subscribers.

The identitybased encryption tells that in order to decrypt a message using particular key there should be match between the credentials of the cipher text and the key. Separate private keys for each authorized credential are maintained by publisher and subscriber. By a string concatenation of a credential, an epoch for key revocation, a symbol € {SUB; PUB} distinguishing publishers from subscribers the public keys are generated. Without contacting the key server or other peers in the system the public keys can be simply generated by any peer. Similarly, encryption of events and their verification using public keys do not require any interaction which is done by their own. Since there is loose coupling between publishers and subscribers, a publisher does not know the set of appropriate subscribers in the system. Therefore, a published event is encrypted with the public key of all likely credentials, which authorizes a subscriber to effectively decrypt the event. The cipher texts of the encrypted event are then signed with the private key of the publisher. The whole network is maintained based on the subscriptions done by the subscribers and subscriptions with common events are placed close to the root in the hierarchy and events are forwarded to the subscribers with less common events. Every subscribers need to know about the subscriptions of the parent and child peers in the hierarchy. In this IBE approach subscriber's identity and the relationship between subscriptions are not leaked to the system and thus confidentiality can be achieved successfully

A. Publishing Events and Subscriber Event

In 1st part publisher publish the events and each them self by the advertising set of events that was intends to publish. This advertized is forward to any or all the subscribers within the system. The subscribers that have interested in that explicit event can send reply to the publisher. After receiving request from publisher, Subscriber maintains the credentials consistent with subscriber and personal key assigned to the subscriber labeled thereupon credentials. Identity based mostly cryptography is employed to confirm that specific subscriber decode the message only if there's match between credentials go together with the event and key.

B. Key Generation

Firstly, a publisher contact the key server with the credentials that ar appointed to every attribute gift in its advertisement by key server then it publish the event within the network. If the publisher is echt consistent with credential for all publish event, then the key server generate separate public keys for every credentials at the side of signature of that publisher. within the same manner, to receive events subscriber conjointly contact to key server for matching subscription to get the personal key on the digital signature for the credentials that are related to every attribute within the subscription.

C. Identity based encryption

Identity based mostly cryptography cut back the key management mechanism that was wiped out ancient PKI infrastructure to maintain identity of public/private key try that was noted solely to human action parties. Key server maintains a single try of master public key and master personal key. The master public key may be employed by publisher to write in code the message and send this message to the subscriber with identity, e.g. associate email address. Likewise to decode the message, subscriber has to get a non-public key from key server for its identity from the key server. Figure one shows the fundamental idea of victimization identity-based cryptography. during this key server alter to make on demand for load equalization and reliableness and act as revolving credit provided to any or all participant within the system. Identity based mostly cryptography seem like extremely centralized solution and its properties are ideal for extremely distributed applications.

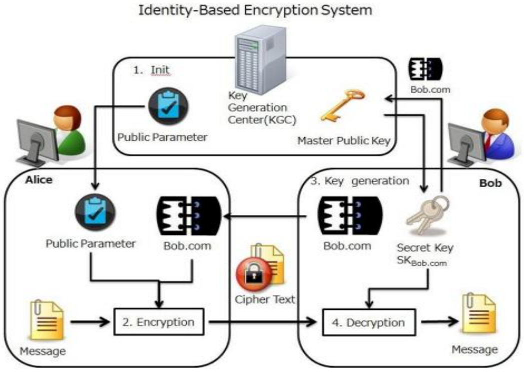

Fig 3. Proposed System Architecture

D. Certificate based encryption

Certificate-based cryptography (CBE) is formal security model; it concerned 2 entities that\'s certifier and a shopper. Definition of CBE somewhat almost like the powerfully key-insulated cryptography and in distinction

E. Advanced Encryption Standard (AES)

AES is regular block cipher that\'s supposed to switch DES because the approved customary for wide selection of application. In AES, Cipher takes a plaintext block size 128 bits or sixteen bytes. During this algorithmic rule key length is sixteen,24 or thirty two bytes. The input to the cryptography and coding algorithmic rule may be a single 128 bits block. AES have classic Feistel Structure, half the information block is employed to switch the opposite half the information block and so the halves are swapped. The structure is sort of easy for each cryptography and coding. The cipher begins with AN AddRoundKey Stage, followed by 9 rounds that every includes all four stages, followed by tenth spherical of 3 stages. Solely the AddRoundKey stages create use of the key. For this reason, the cipher begins and ends with AN AddRoundKey stages. Every stage during

IV. CONCLUSION

In this paper, we have presented broker-less approach in content based publish subscribe system for providing authentication and confidentiality. The approach is extremely good for number of subscribers and publishers in the system and the number of keys maintained by them. The keys will be in cipher text format which are labeled with credentials assigned to publishers and subscribers. We adapted techniques from Identity-based encryption (IBE) mechanisms 1) key can be used to decrypt only if there is match between credentials of cipher text and the key; and 2) to permit subscribers to check the validity of received contents.

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, February 2014.

[2] 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.

[3] 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.

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

[5] 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.

[6] A. Shikfa, M. O ¨ nen, and R. Molva, "PrivacyPreserving Content-Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.

[7] 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.

[8] 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.

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

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

[11] 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.

[12] M.A. Tariq, B. Koldehofe, A. Altaweel, and K. Rothermel, "Providing Basic Security Mechanisms in Broker-Less Publish/ Subscribe Systems," Proc. ACM Fourth Int'l Conf. Distributed Eventt- Based Systems (DEBS), 2010.