ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Certificate Based Encryption for Securing Broker-Less Publish/Subscribe System in Wireless Network

Priyanka Bubna, Parul Bhanarkar Jha

Dept. of I.T., TGPCET, RTM Nagpur University, Nagpur, India

Assistant Professor, Dept. of I.T., TGPCET, RTM Nagpur University, Nagpur, India

ABSTRACT: The security mechanisms such as authentication and confidentiality is highly challenging in a content-based publish/subscribe system and due to the loose coupling of publishers and subscribers, authentication and confidentiality of publishers and subscribers is difficult to achieve. In particular content-based approaches in broker-less environments do not address confidentiality at all. This paper presents to provide confidentiality and authentication in a broker-less content-based publish-subscribe system. The authentication and confidentiality and other security approach of publishers and subscribers ensured, by adapting the certificate based encryption mechanism. In certificate based encryption signature not only acts as certificate but also as encrypt and decrypt key. To encrypt or to decrypt a message, a key holder needs both its public key and private key and an up-to-date certificate from an authorizer. Certificate-based encryption combines the best aspects of identity-based encryption and public key encryption. This mechanism describes how certificate-based encryption can be used to construct an efficient PKI requiring fewer infrastructures than any previous method.

KEYWORDS: Certificate Based Encryption, Identity Based Encryption, Public Key Encryption, Publisher/Subscriber

I. Introduction

The publish/subscribe communication paradigm have more popularity because of its inherent decoupling of publishers from subscribers in terms of time, space, synchronization etc. As publishers inject information into the publish/subscribe system, subscribers specify its interest by means of subscriptions. Published events are routed to their relevant subscribers, without the knowing the relevant set of subscribers, or vice versa. This decoupling is traditionally ensured by intermediate routing over a broker network. In more recent systems, publishers and subscribers organize themselves in a broker-less routing infrastructure, forming an event forwarding overlay.

Content-based pub/sub is useful for provides the most expressive subscription model, in which subscriptions define restrictions on the message content and this expressiveness and asynchronous nature is useful for large-scale distributed applications such as news distribution, stock exchange ect. Publisher and subscriber needs to provide supportive mechanisms which fulfil the basic security need of these applications such as access control and confidentiality. Access controls in the pub/sub system allow only to authenticated publisher to disseminated events and this events are delivered to authorized subscriber.

For PKI, publishers must maintain the public keys of all interested subscribers to encrypt events. Subscribers must know the public keys of all relevant publishers to verify the authenticity of the received events, again there is traditional mechanisms to provide confidentiality by encrypting the whole event message conflict with the content-based routing paradigm. Therefore this paper provide some mechanism that are needed to route encrypted events to subscribers without knowing their subscriptions and to allow subscribers and publishers authenticate each other without knowing each other. To provide a new confidentiality authentication in broker-less pub/sub system, certificate based encryption has been used to encrypt and decrypt the files. Here, every user has unique public and private key.

Alice and Bob encrypts and decrypt the file by using master public and private key which was provided by key server on demand of Alice and bob. Key Server maintains both public and private keys. For this, identity based encryption and certificate based encryption concepts are used. Certificate based encryption performs the function of both digital signature and encryption. A secure encryption mechanism scheme should provide confidentiality, authentication, scalability, non-repudiation and should provide insider security too.

A certificate contain signature of trusted certificate authority (CA) which have several quantities. Typically, these quantities include at least the name of a user *U* and its public key *PK*. The CA includes a serial number *SN along with* certificate's issue date *D*1 and expiration date *D*2 to simplify its management. By issuing *SigCA*(*U; PK; SN;D*1*;D*2), after this CA basically attests to its belief that *PK* is user *U*'s authentic public key from the current date *D*1 to the future date *D*2. Since CAs cannot tell the future circumstances may require a certificate to be revoked before its intended expiration date. For example, suppose user accidentally reveals its secret key or an attacker compromises it, then user itself may request revocation of its certificate. Alternatively, the user's company may request revocation if the user leaves the company or changes position and is no longer entitled to use the key.

If a certificate is revocable, then third parties rely on certificate status provided by CA that told whether certificate is valid or not but cannot rely on certificate. This certificate status information can be fresh within a day. It widely distributed to all relying parties. If large amounts of fresh certification information is distributed then it create the "certificate revocation problem", to solve this problem lot of infrastructure is required and the apparent need for this infrastructure is often cited as a reason against widespread implementation of public-key cryptography.

II. RELATED WORK

Muhammad Adnan Tariq et all proposed "Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption" in 2014.In this paper, a new approach is provide for 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. They 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.

Yonglin Ren et al have proposed "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks" in 2011. In this paper, Selective encryption is one of the most promising solutions to reduce the cost of data protection in wireless and mobile networks. Again they proposed that a novel solution for selective encryption to achieve data protection effectively while with reasonably costs. The probabilistic and stochastic techniques in our proposed solution guarantee the security for data communications between the messages' sender and receiver.

Amar Rsheed et all proposed "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks" in the 2012. In this paper they proposed a general three-tier security framework for authentication and pair wise key establishment between mobile sinks and sensor nodes. The proposed scheme, based on the polynomial pool-based key predistribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key predistribution approach. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink.

Minakshi B. Shingan et all proposed "Securing Broker-Less Public/Subscribe Systems Using Identity-Based Encryption" in 2012.In this paper, they proposed new approach like pairing based cryptography to provide authentication and confidentiality in broker-less content based publisher/subscriber system. In addition to this an algorithm to cluster subscribers according to their subscriptions preserves a weak notion of subscription confidentiality .To enable efficient routing searchable encryption is provided for encrypted events. A new event distribution method is provided to support weak subscription confidentiality, multi credential routing. 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.

K. Sriswathika et all proposed “Securing Pub/Sub System Using Signcryption with Enhanced Energy Efficiency” in 2014.In this paper signcryption is used to provide authentication and confidentiality to important message. This mechanism performs both digital signature and encryption. Signcryption help to provide authentication in loose coupling publisher and subscriber system.

III. PROPOSED ALGORITHM

In proposed system, to provide the confidentiality, authentication, scalability and all security approach in the broker-less content based publisher/subscriber system, certificate based encryption used along with the identity based encryption. In the identity based encryption to identify a user uniquely the public key of that particular user is used. In this mechanism key management is required and no sharing of key was done. The proposed system contains publishers, subscribers and a key server along with master public and master private keys. The master public key is unique to publisher identity, by using this master public key publisher encrypt the message and send to respective subscriber. To decrypt the message subscriber get the private key from the key server and decrypt the message.

In this system subscribers to have credentials according to their subscriptions and all master private keys are assigned to the subscribers are also labelled with a same credentials. Certificate based encryption and Identity based encryption ensures that a subscriber can decrypt an event only if there is a match between the credentials associated with the event and the key to avoid the unauthorized publications. It also ensures that only the authorized publishers should be able to publish events in the system and similarly subscribers should only receive those events to which they have subscribed. To provide confidentiality, it ensures that the events are visible to only authorized subscribers and are protected from unauthorized Modifications.

A. *Publishing Events and Subscriber Event*

In first phase publisher publish the events and authenticated them self by the advertising set of events that was intends to publish. This advertized is forward to all the subscribers in the system. The subscribers which have interested in that particular event will send respond to the publisher.

After receiving request from publisher, Subscriber maintains the credential according to subscriber and private key assigned to the subscriber labeled with that credential. Identity based encryption is used to ensure that particular subscriber decrypt the message only when there is match between credential associate with the event and key.

B. *Key Generation*

Firstly, a publisher contact the key server with the credentials that are assigned to each attribute present in its advertisement by key server after that it publish the event in the network. If the publisher is authenticated according to credential for all publish event, then the key server generate separate public keys for each credential along with signature of that publisher. In the same way, to receive events subscriber also contact to key server for matching subscription to generate the private key along the digital signature for the credentials that are associated with each attribute in the subscription.

C. *Identity Based Encryption*

Identity based encryption reduce the key management mechanism which was done in traditional PKI infrastructure to maintain identity of public/private key pair that was known only to communicating parties. Key server maintains a single pair of master public key and master private key. The master public key can be used by publisher to encrypt the message and send this message to the subscriber with identity, e.g. an email address. Likewise to decrypt the message, subscriber needs to obtain a private key from key server for its identity from the key server. Figure 1 shows the basic idea of using identity-based encryption. In this key server enable to create on demand for load balancing and reliability and act as smart card provided to all participant in the system. Identity based encryption appear like highly centralized solution and its properties are ideal for highly distributed applications.

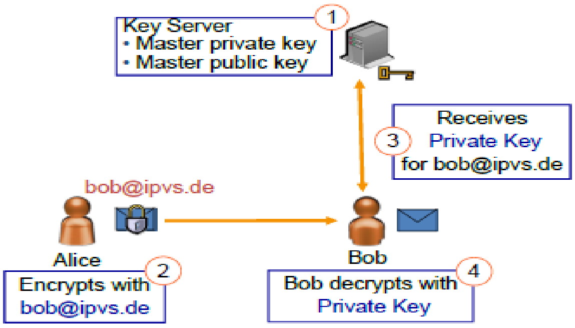

Key Server
• Master private key
• Master public key
1
3
Receives Private Key for bob@ipvs.de
bob@ipvs.de
Alice
2
Encrypts with bob@ipvs.de
Bob
4
Bob decrypts with Private Key

Figure 1: Identity Based Encryption

D. *Certificate Based Encryption*

Certificate-based encryption (CBE) is formal security model,it involved two entities that is certifier and a client. Definition of CBE somewhat similar to the strongly key-insulated encryption and in difference this model does not require a secure channel between the two entities. CBE does not necessarily have to be “certificate updating,” and it can be useful for applications other than certificate management. CBE is useful in other situation where authorization or access control is an issue. A publisher can use CBE to encrypt its message so that the key holder can decrypt only after it has obtained certain signatures from one or more authorized on more messages.

It may be seem strange that certificate or signature used as decryption key. This certificate / decryption key can be verified like a signature as explicit proof of certification (even of signature keys), or it can be used as a means for enabling implicit certification in the encryption context, as described in the Introduction. Certificate cased encryption is clear combination of PKE and IBE, where the client needs both its personal secret key and a certificate / decryption key from the CA to decrypt. The string s may include a message that the certifier “signs” – e.g., the certifier may sign clientinfo = hclientname, Depending on the scheme, pub/sub may include other information, such as the client’s signature on its public key.

E. *Advanced Encryption Standard (AES)*

AES is symmetric block cipher that is intended to replace DES as the approved standard for wide range of application. In AES, Cipher takes a plaintext block size 128 bits or 16 bytes. In this algorithm key length can be 16,24 or 32 bytes. The input to the encryption and decryption algorithm is a single 128 bits block. AES have classic Feistel Structure, half of the data block is used to modify the other half of the data block and then the halves are swapped. The structure is quite simple for both encryption and decryption.

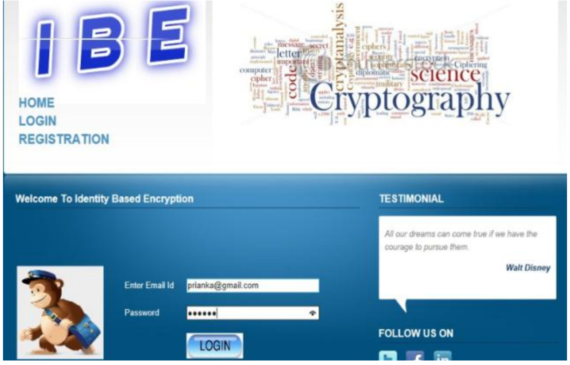
The cipher begins with an AddRoundKey Stage, followed by nine rounds that each includes all four stages, followed by tenth round of three stages. Only the AddRoundKey stages make use of the key. For this reason, the cipher begins and ends with an AddRoundKey stages. Each stage in this algorithm is reversible because of this reason it help to provide security.

F. *Vernam Cipher*

The vernam cipher, also called as One-Time Pad, is implemented using random set of non- repeating character as the input cipher text. The most significant point here is that once an input cipher text for transposition is used, it is never used again for any other message. The length of the input cipher text is equal to the length of the original plain text.

IV. RESULT

In this paper, firstly user has to register as publisher or subscriber, for this user have to fill all the detail regarding to registration as email-id, name of user, password etc. and after that user get registration successful messages. User was successfully registered as publisher or subscriber. Publisher and subscriber get credential according to its event. As user get credential for its event, user is able to do login.

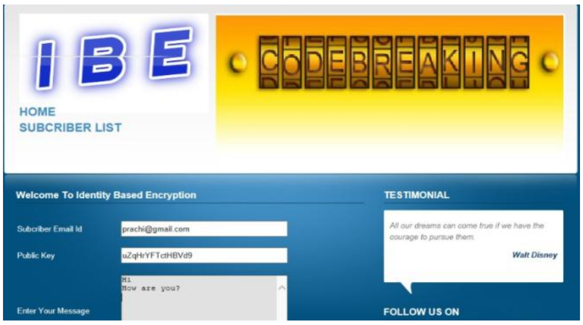


Enter Email Id: prianka@gmail.com
Password: ••••••

All our dreams can come true if we have the courage to pursue them.
Walt Disney

Figure 2. Showing Registration phase for Pub/Sub along with login phase

In login phase Publisher has to enter the detail of login, as publisher email-id and password. After this phase user is able to get the public key from server to encrypt the event for its credential. Key Server generate key only for credential of publisher. After that publisher has to select subscriber from list of subscriber and encrypt the event by using public key provided by key server. When publisher encrypt the event by using public key, advanced encryption algorithm is used for encryption the event. Publisher again generate certificate for subscriber during encryption of event.

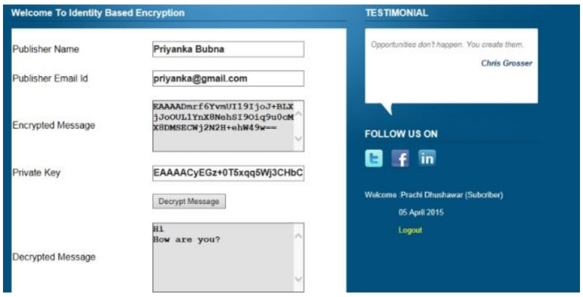


Subcriber Email Id: prachi@gmail.com
Public Key: uZqHrYFTctHBVd9
Enter Your Message:
```
Hi
How are you?
```

All our dreams can come true if we have the courage to pursue them.
Walt Disney

Figure 3. Showing Encryption Phase

Subscriber give respond to publisher, if credential associated with subscriber match with credential of event and key of publisher. After that subscriber has to login for decryption of event. Subscriber request to key server for private key to decrypt the event. Private Key that was generated by key server for subscriber is nothing but encrypted data of encrypted event of publisher and encrypted form of public key that was generated for publisher to encrypt the message, for this vernam cipher algorithm is used. Subscriber upload the certificate that was generated by publisher for subscriber and then subscriber decrypt the event by using private key if digital signature were match.



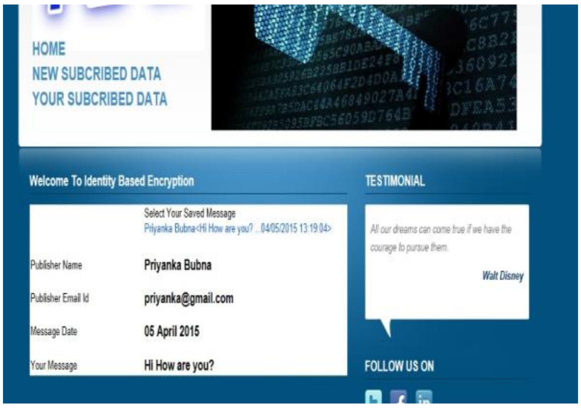
Publisher Name: Priyanka Bubna
Publisher Email Id: priyanka@gmail.com
Encrypted Message:
```
EAAAADmrf6YvmUI19IjoJ+BLX
jJoOULlYnX8NehSI9Oiq9u0cM
X8DMSECWj2N2H+ehW49w==
```
Private Key: EAAAACyEGz+0T5xqq5Wj3CHbC
Decrypted Message:
```
Hi
How are you?
```

Opportunities don't happen. You create them.
Chris Grosser

Welcome Prachi Dhushawar (Subcriber)
05 April 2015

Figure 4. Showing Decrypted Data

Subscriber is able to see all the detail related to event. Subscriber knows who send the event and at what time and date event was sended by publisher. Subscriber can decrypt new data or decrypt previous data. In this paper, Certificate based encryption is used that was secure all event from all type of attack and add digital signature into the generated key. Certificate based encryption used for providing all type of security mechanism. Certificate Based Encryption save event from man in middle attack that was rare in wireless network.



Select Your Saved Message
Priyanka Bubna<Hi How are you? ...04/05/2015 13:19:04>

Publisher Name Priyanka Bubna

Publisher Email Id priyanka@gmail.com

Message Date 05 April 2015

Your Message Hi How are you?

All our dreams can come true if we have the courage to pursue them.

Walt Disney

Figure 5. Window Showing detail of Decrypted Data

V. Conclusion

In this paper, to provide authentication and confidentiality and all security mechanism in a broker-less content based pub/sub system new approach is used and this approach is scalable in terms of number of publisher and subscriber and the number of keys maintained. Identity based encryption is used to assign credentials to publishers and subscribers according to subscriptions and advertisements. Certificate based encryption is used 1) to eliminate third party queries on certificate status and 2) to reduce infrastructure requirement. The key ideas behind this encryption enabled the implicit certification without the problem of IBM and demonstrate how it streamlines PKI. This mechanism prevents all attack and secures all events in the system.

References

1. 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.
2. R. Agrawal, A. V. Evfimievski, and R. Srikant. Information sharing across private databases. In A. Y. Halevy, Z. G. Ives, and A. Doan, editors, SIGMOD Conference, pages 86–97. ACM, 2003.
3. Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel, "Securing Broker-Less Publish/Subscribe Systems Using Identity- Based Encryption," IEEE Transactions on parallel and distri buted systems, vol. 25, no. 2, Februar y 2014
4. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, 2007.
5. 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.
6. 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.
7. 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.
8. A. Shikfa, M. O¨ nen, and R. Molva, "Privacy-Preserving Content-Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.
9. M. Srivatsa and L. Liu. Vulnerabilities and security issues in structured overlay networks: A quantitative analysis. In *Proceedings of the Annual Computer Security. Applications Conference (ACSAC)*, 2004.
10. M. Srivatsa and L. Liu. Eventguard: Securing publishsubscribe networks. Technical report, Georgia Institute of Technology, 2005.
11. M. Srivatsa, L. Xiong, and L. Liu. Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks. In *Proceedings of the World Wide Web Conference (WWW)*, 2005.
12. C. Wang, A. Carzaniga, D. Evans, and A. L. Wolf. Security issues and requirements for internet-scale publish subscribe systems. In *Proceedings of the 35th Hawaii International Conference on System Sciences*, 2002.

13. L. Xiong and L. Liu. Peertrust: Supporting reputationbased trust for peer-to-peer electronic communities. In *Proceedings of IEEE TKDE, Vol. 16, No. 7*, 2004.
14. E. W. Zegura, K. Calvert, and S. Bhattacharjee. How to model an internetwork. In *Proceedings of IEEE Infocom*, 1996.

BIOGRAPHY

Priyanka Bubna is a Student of Master of Engineering (Wireless Communication and Computing) of Information Technology department, College of Tulsiramji Gaikwad Patil College of Engineering, Nagpur, India. She received Bachelor of Engineering degree in 2011 from RTMNU, Nagpur, MS, India. Her research interests are Computer Networking etc.

Parul Bhanarkar Jha received master of engineering degree from Bhopal (MP) and assistant professor in Nagpur University. Her research interests are Computer Networking etc.