ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 2 February 2015, Page No. 10478-10483

Identity-Based Encryption for Preserving Privacy In Cloud For Publish/Subscribe System

D.Devisri, J.Ramya, Mrs.T.Kalaichelvi
Department of Computer Science and Engineering,
Panimalar Engineering College, Chennai.
devisrimusic@gmail.com, ramyajayavel93@gmail.com.
Guide Name- Mrs.T.Kalaichelvi B.E., M.E., (PhD)

***ABSTRACT*—The provisioning of basic security mechanism such as authentication and confidentiality in the publish/subscribe system. Authentication in this system is difficult to achieve due to the loose coupling between publishers and subscribers. Likewise, Confidentiality of events and subscriptions conflicts with content-based routing. To ensure authentication and confidentiality in broker less publish/subscribe system we adopt pairing based cryptography mechanism. Furtherly, broadcasting encryption algorithm is adapted to provide subscription confidentiality by clustering subscribers according to their subscription by providing a private key with their credentials. Sowe adapt identity based encryption for providing private key to the subscribers with their credentials based on their identity (e.g. e-mail). This technique enables efficient routing of encrypted events, provides thorough analysis of various attacks on subscription confidentiality and a fine grained key management. Moreover, the evaluations show that providing security is affordable w.r.t. 1) throughput of the proposed cryptographic primitives, and 2) delays incurred during the construction of the publish/subscribe overlay and the event dissemination.**

Index Terms—Content-based, publish/subscribe, broker-less, security, identity-based encryption, pairing based cryptography, private key.

I.INTRODUCTION

In the current era of digital world, various organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. The publish/subscribe (pub/sub) communication paradigmhas gained high popularity in this organization. Because it inherent decoupling of publishers from subscribers interms of time, space, and synchronization. Publisher send information in to the pub/sub system and subscriber specify the events and then receive it. Published events are received to the relevant subscriber without the publishers 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 system is the variant that define restrictions on the message content for subscriber. Its expressivenessand asynchronous nature is particularly useful forlarge-scale distributed applications such as news distribution,stock exchange, environmental monitoring, trafficcontrol, and public sensing. Publish/subscribe needs to provide supportive mechanisms to fulfil the basicsecurity demands of these applications such as accesscontrol and confidentiality. Access control in the

publish/subscribe system is to allow only authenticated publisher to inject information and only those events are delivered to authorized subscribers. Moreover, a subscriber should receive all relevant events without revealing its subscription to the system. To solve this security issues new challenge i.e. "Public key infrastructure" that conflicts withthe loose coupling between publishers and subscribers, akey requirement for building scalable pub/sub systems.For PKI, publishers must maintain the public keys of allinterested subscribers to encrypt events. Subscribers mustknow the public keys of all relevant publishers to verify theauthenticity of the received events.In the past, most research has focused only on providingexpressive and scalable pub/sub systems, but little attentionhas been paid for the need of security. Existingapproaches toward secure pub/sub systems mostly relyon the presence of a traditional broker network and also it provides coarse grain key management in this system. In proposed work, a new approach to provide authentication and confidentiality in a broker-less publish/subscribe system. Private keys assigned to the subscribers are labelled with the credentials. We adapted identity based encryption mechanisms that simplifies the process of securing sensitive communications. Pairing based cryptography that establishes a mapping between two cryptographic groupsby means of bilinear maps. And also uses Broadcast Encryption Algorithm for generating keys that send to identity i.e. Email. By combining all these algorithms and techniques we can provide a safe, secured and efficient way of storing and processing message in the pub/sub system.

II.EXISTING WORK

In the past, most research has focused only on providing expressive and scalable pub/sub systems, but little attention has been paid for the need of security. Existing approaches toward secure pub/sub systems mostly rely on the presence of a traditional broker network. These either address security under restricted expressiveness, for example, by using only keyword matching for routing events or rely on a network of (semi-)trusted brokers. Furthermore, existing approaches use coarse-grain epoch based key management and cannot provide fine-grain access control in a scalable manner. Nevertheless, security in broker-less pub/sub systems, where the subscribers are clustered according to their subscriptions, has not been discussed yet in the literature. It includes some disadvantages such as It is very hard to provide subscription confidentiality in a broker-less publish/subscribe system, where the subscribers are arranged in an overlay network according to the containment relationship between their subscriptions. In this case, regardless of the cryptographic primitives used, the maximum level of attainable confidentiality is very limited. The limitation arises from the fact that a parent can decrypt every event it forwarded to its children. Therefore, mechanisms are needed to provide a weaker notion of confidentiality.

III.PROPOSED WORK

In this paper, we present a new approach to provide authentication and confidentiality in a broker-less publish/subscribe system. Our approach allows subscribers to maintain credentials according to their subscriptions. Private keys assigned to the subscribers are labelled with the credentials. A publisher associates each encrypted event with a set of credentials. We adapted identity based encryption mechanisms .Similarly, the content of events should not be exposed to the routing infrastructure and a subscriber should receive all relevant events without revealing its subscription to the system. These security issues are not trivial to solve in a content-based publish/subscribe system and pose new challenges. In Proposed system has some advantages follow as to ensure that a particular subscriber can decrypt an event only if there is match between the credentials associated with the event and the key. To allow subscribers to verify the authenticity of received events. Furthermore, we address the issue of subscription confidentiality in the presence of semantic clustering of subscribers. A weaker notion of subscription confidentiality is defined and a secure connection protocol is designed to preserve the weak subscription confidentiality. Finally, the evaluations demonstrate the viability of the proposed security mechanisms.

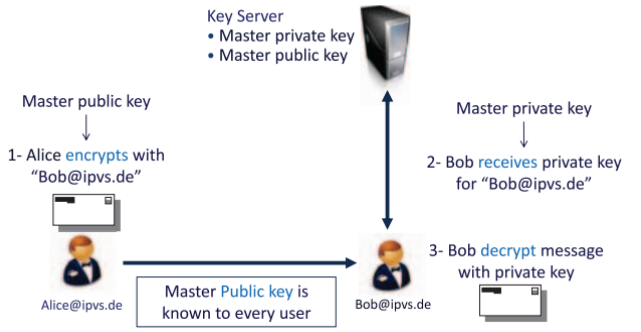
IV.METHODOLOGY DESCRIPTION

Identity Based Encryption:

While a traditional PKI infrastructure requires to maintain for each publisher or subscriber a private/public key pair which has to be known between communicating entities to encrypt and

decrypt messages, identity-based encryption [6] provides a promising alternative to reduce the amount of keys to be managed. In identity-based encryption, any valid string which uniquely identifies a user can be the public key of the user. A key server maintains a single pair of publicand private master keys. The master public key can be

Using identity based encryption.



Although identity-based encryption has been proposed some time ago, only recently pairing-based cryptography (PBC) has laid the foundation of practical implementation of identity-based encryption. Pairing-based cryptography 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. We utilize bilinear maps for establishing the basic security mechanisms in the pub/sub system and, therefore, introduce here the main properties. Let G_1, G_T be two cyclic groups of prime order q. A pairing is a map: $e: G_1 \times G_2 \rightarrow G_T$, which satisfies the following properties:

Bilinearity:

$$\forall a, b \in F_q^*,\ \forall P, Q \in G_1:\ e\left(P^a, Q^b\right) = e(P, Q)^{ab}$$

Non-degeneracy: $e(P, Q) \neq 1$

Computability: ^ e can be efficiently computed.

V.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

used by the sender to encrypt and send the messages to a user with any identity, for example, an e-mail address. To successfully decrypt the message, a receiver needs to obtain a private key for its identity from the key server. Fig. 1 shows the basic idea of

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.

Publishing Events Encryption

When a publisher wants to publish an event message M, it chooses bi 2 ZZq at random for each attribute Ai of the event, such that b ¼Pd i¼1 bi. These random valuesensure that only the subscribers who have matching credentials for each of the attributes should be able to decrypt the event. Furthermore, the publisher generates a fixed-length random key SK for each event. More precisely, the following steps are performed by the publisher to encrypt an event:

Step 1. Compute: CT1 ¼ ^ eog1;g2ÞbSK; CT2 ¼ hb and; CT3 ¼ BlockCipheroMsgk0ÞSK, where Msg¼oM;fPupi;jgÞ defines a record that includes 1) the actual event message M, and 2) the public keys of the credentials which authorize the publisher p to send the event. The cost of asymmetric encryption generally increases with the size of the plaintext. Therefore, only a fixed-length random key SK is encrypted using the private keys of publisher. The record Mgs is encrypted with a symmetric encryption algorithm such as AES [15] or Triple DES [3], using key SK.

Step 2. For each attribute Ai, compute CTi ¼ gbi. The CTi ciphertexts along with CT0i;j (created in Step 3) and Prsi;j½3are used for the routing of encrypted events (cf. Section 6.4).

Step 3. For each attribute of the event, a ciphertext should be created for every credential that matches the value associated with that attribute, so that a subscriber with any of these credentials should be able to decrypt the event.

Receiving Events

Decryption. On receiving the cipher texts, 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 thecontainment 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:

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 master public key (MPu).

VI.SUBSCRIPTION CONFIDENTIALITY

Secure Overlay Maintenance

In the following, we propose a secure protocol to maintain the desired pub/sub overlay topology without violating the weak subscription confidentiality. For simplicity and without loss of generality, here we discuss the overlay maintenancew.r.t.asingletreeassociatedwithanume ricattribute Ai and each of the subscribers owns a single credential.

Filling the security gaps. By looking at the number of ciphertexts in the connection request, a peer can detect the credential of the requesting subscriber s. For example, a subscriber with credential 00 can only connect to 0 or 00, and therefore, a connection request will have two ciphertexts, whereas the connection request for 000 will have three ciphertexts. In the worst case, a subscriber has a credential of the finest granularity. This can be covered by log2oZiÞ other credentials, and therefore, a connection request contains in the worst case that many ciphertexts. To avoid any information leak, ciphertexts in the connection request are always kept in Oolog2 ZiÞ (OoLiÞ for prefix matching) by adding random ciphertexts if needed. Furthermore, the ciphertexts are shuffled to avoid any information leak from their order.

Overall algorithm. The secure overlay maintenance protocol is shown in Algorithm 1. In the algorithm, the procedure decrypt request tries to decrypt one of the ciphertexts in the connection request message.

Algorithm 1. Secure overlay maintenance protocol at peer sq.

1: upon event Receive (CR of snew from sp) do

2: if decrypt requestoCRÞ¼¼SUCCESS then

3: if degree (sq) == available then //can have child peers

4: connect to the snew

5: else

6: forward CR to fchild peers and parentgsp

7: if decrypt requestoCRÞ¼¼FAIL then

8: if sp ¼¼ parent then

9: Try to swap by sending its own CR to the snew.

10: else

11: forward to parent

A child peer sq receives CR (of subscriber snew) from the parent sp only if the parent cannot accommodate more children. If sq cannot be the parent of snew, i.e., snew's credential is coarser than that of sq, and then it tries to swap its position with snew by sending its own connection request (cf. Algorithm 1, lines 7-9). However, if none of the children of parent sp can connect or swap with snew, then there is no containment relationship between the credentials of the children and snew. In this case, a parent should disconnect one of its children to ensure the new subscriber is connected to the tree.

VII.CONCLUSION

In this paper, we have presented a new approach to provide authentication and confidentiality in a broker-less contentbased 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 identitybased 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.

VIII.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.

[11] M. Jelasity, A. Montresor, G.P. Jesi, and S. Voulgaris, "PeerSim: A Peer-to-Peer Simulator," http://peersim.sourceforge.net/, 2013.

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

[13] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, 2010.

[14] B. Lynn, "The Pairing-Based Cryptography (PBC) Library," http://crypto.stanford.edu/pbc/, 2010.

[15] F.P. Miller, A.F. Vandome, and J. McBrewster, Advanced Encryption Standard. Alpha Press, 2009.

[16] M. Nabeel, N. Shang, and E. Bertino, "Efficient Privacy Preserving Content Based Publish Subscribe Systems," Proc. 17th ACM Symp. Access Control Models and Technologies, 2012.

[17] L. Opyrchal and A. Prakash, "Secure Distribution of Events in Content-Based Publish Subscribe Systems," Proc. 10th Conf. USENIX Security Symp., 2001.

[18] 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.

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

[20] 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.

[21] A. Shikfa, M. O ¨ nen, and R. Molva, "Privacy-Preserving ContentBased Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.

[22] M. Srivatsa, L. Liu, and A. Iyengar, "Event Guard: A System Architecture for Securing Publish-Subscribe Networks," ACM Trans. Computer Systems, vol. 29, article 10, 2011.

[23] 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 EventBased Systems (DEBS), 2010.

[24] M.A. Tariq, B. Koldehofe, G.G. Koch, I. Khan, and K. Rothermel, "Meeting Subscriber-Defined QoS Constraints in Publish/Subscribe Systems," Concurrency and Computation: Practice and Experience, vol. 23, pp. 2140-2153, 2011.

[25] Y. Yu, B. Yang, Y. Sun, and S.-l. Zhu, "Identity Based Signcryption Scheme without Random Oracles," Computer Standards & Interfaces, vol. 31, pp. 56-62, 2009.