International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Survey on Encryption Methods for Providing Security in Pub/Sub System

Onkar P. Kasarlewar[1], P. S. Desai[2]

[1]PG Student, Pune University, STES's, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

[2]Professor, Pune University, STES's, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Abstract: ***Internet has changed the world of distributed computing significantly. Peer-to-peer communication mechanism making system more rigid and static applications in distributed system, making a way to loosely coupled infrastructure. This can be achieved by Publish/Subscribe system. As it has group of large unpredictable subscribers, developing a reliable Publish/Subscribe System is challenging task to perform. Many-to-many communications and loosely coupling of publishers, subscribers is strength of Publish/Subscribe. It has huge demand. Because of this, security issue arises. For that, mechanisms like The cost for encryption-decryption, fine grained key management and the pairing-based cryptography mechanisms, and routing is in the order of subscribed attributes are already implemented. Broker-less content-based publish/subscribe system do not tackle the problem of confidentiality at all. So to that, there is scope for providing confidentiality and authenticities in a broker-less content-based publish/subscribe system. By using Identity based encryption, confidentiality and authentication of publisher and subscriber can be ensured.***

Keywords: Publish/Subscribe, confidentiality, broker-less, multi-credential routing, Identity - Based Encryption.

1. Introduction

Distributed Systems are largely being used. As traditional point to point communication mechanisms making system more complex and difficult to understand, there is way opened up for loosely coupled communication system. The Publish/Subscribe system has gained popularity because of loose coupling of Publishers and Subscribers. Publishers are unknown of Subscribers who are accessing their data or retrieving it. Same as of Subscribers are also unknown of Publishers, of whom data they are retrieving. Publishers publish their data in Publish/Subscribe System and Subscribers show their interest by subscribing data. This system is traditionally has been implemented by using intermediate broker network [7]. Loose coupling and broker network are used to implement Publish/Subscribe system traditionally hence publishers will not know the recipients and subscribers will not know the publishers. In case of sensitive data, its visibility must be controlled carefully for security reasons. Due to the loose coupling of publishers and subscribers it is very difficult to provide authentication mechanism for Publishers and Subscribers.

In recent years, publishers and subscribers are organizing themselves in broker less infrastructure forming event forwarding overlay [15]. Publish/subscribe system is responsible for forwarding events to subscribers which have subscribed to that event, when new event is published. Software updates, stock exchange, location services in wifi network, multiplayer online games, traffic control are good example of Content based publish/subscribe system [8].

In publish/subscribe system; achieving security in large, heterogeneous network is most challenging task because it's loosely coupled nature of scalable communication paradigm. That is why Access control gained importance in publish/subscribe system. Fine grained and dynamic information dissemination, group communication makes it harder to guarantee that knowing precise identities of receiver will provide confidentiality without sacrificing scalability [2]. In past researches, little attention is given to need of security and largely focused on expressiveness and scalability of publish/subscribe system. Approach of security in existing system relied on traditional broker network [11] [9]. This is mostly achieved by restricted expressiveness [12] [13] or rely on semi trusted broker network [5] [10].

There is need of mechanism which will provide searchable encryption by which efficient routing of encrypted events will be achieved and multi-credential routing a new event dissemination strategy for strengthening weak subscription confidentiality. There is also need of maintaining credentials according to subscription.

2. Literature Review

This paper focuses on a general pub/sub architectural model and solutions proposed in the literature for event routing and their relations with overlay network level solutions and possible network deployment.

1) Content-Based Model

In content based model, subscribers apply constraints on event to be sent to them. According those constraints events will be routed to subscribers. An event is matched against subscriptions when attributes and its values in an event satisfy requirements of subscriptions [3]. The complexity of matching operation is influenced by complexity of subscription language. In concept based model, events are not matched by name but they are matched against attributes of event.

2) Semantic Overlay

A generic content-based publish/subscribe system which is dynamic and reliable also perform a comparative analysis of its probabilistic and deterministic implementations called as Dynamic Publish/Subscribe (DPS). Subscription driven clustering is obtained in Dynamic Publish/Subscribe (DPS). DPS has ability to achieve scalable event delivery even if failures and changes occur in the system [1]. DPS is targeted towards scalability and reliability for that it has schemes like fault tolerant deterministic and probabilistic content based publish/subscribe system [1].

3) Access Control

In publish/subscribe system which has loosely-coupled nature, achieving security is challenging task. Access control mainly deals with security of events and its routing to appropriate subscriber. Confidentiality is also important issue in Access control mechanism. Publish/Subscribe has large and heterogeneous groups publishers and subscribers which increases difficulty in achieving confidentiality and authenticity. Asynchronous publish/subscribe communication and role based access control will be helpful for making distributed system scalable [2].

4) Identity-Based Encryption

Identity Based Encryption is a cryptographic scheme where two nodes can communicate and verify their signatures without exchanging Public or Private Key [16]. An identity-based encryption scheme is specified by four randomized algorithms: Setup, Extract, Encrypt, and Decrypt [6].
Setup: Master Key and system parameters are generated.
Extract: Private Key corresponding to a Public Key is generated using Master Key.
Encrypt: Using Public Key, message is encrypted.
Decrypt: Using Private Key, message is decrypted.

3. Methods for Security

In system parameters, security mechanism is based on Ciphertext-Policy Attribute-Based Encryption proposed by J. Bethencourt [4]. Authentication of Publishers and Subscribers and confidentiality of events can be achieved by following steps:

A.Security Parameters and Initialization
There are mainly two keys:
1) Master Public Key.
2) Master Private Key.

The master public key is known to every peer in the system. It is used to for encryption and signature verification. The master private key is only known to key server. It is used to generate private key for publishers and subscribers [14].

B.Key Generation for Publishers/Subscribers
When a publisher tends to publish an event, publisher contacts key server with all needed attributes. The key server generates a private key for each credential when publisher is allowed to publish an event [14].

Table 1: Comparison of Existing Systems

Paper Name	*Details*	*Advantages*	*Disadvantages*
A Semantic Overlay for Self-Peer-to-Peer Publish/ Subscribe	DPS is presented which is a distributed reliable and scalable content-based publish/subscribe system that exhibits self-* characteristics.	Proposed system is very versatile, so it can be deployed in many applications.	Should have been evaluated in context where real-world subscriptions and publications are injected.
Access Control in Publish/Subscribe Systems	An alternative is proposed to whole-message encryption, appropriate for highly sensitive and long-lived data destined for specific domains with varied requirements	It is appropriate for many applications as it comprises multiple administration domains sharing a dedicated event-broker network.	For sensitive data that persists long term this may not be a sufficient guarantee.
A Privacy-Enhancing Content-Based Publish/ Subscribe System Using Scalar Product Preserving Transformations	A secure CBPS system is presented based on Asymmetric Scalar product Preserving Encryption in order to provide notification and subscription confidential-lity and to reduce matching complexity	These methods support equality filtering, inequality filtering, range filtering, covering, and conjunction filtering.	Not suitable in types of subscriptions with more complex conditions.
Ciphertext-Policy Attribute-Based Encryption	A system is proposed for realizing complex access control on encrypted data.	This system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys.	Limitation of this system is that it is proved secure under the generic group heuristic.
Privacy-Preserving Content-Based Publish/Subscribe Networks	A solution to the problem of privacy issues in content-based publish/ subscribe networks is presented which is based on multiple layer commutative encryption.	Privacy is guaranteed among all nodes, including subscribers and eavesdropping outsiders.	Needs to improve flexibility regarding the network topo-logy and the subscription filter format

C. Publishing Events

Publisher chooses an event message a key to encrypt that event such that it ensure that only subscribe having matching credentials should be able to decrypt the event. Publisher also generates fixed length random key for each event [14].

D. Secure Event Dissemination

In Secure Event Dissemination, there are mainly two challenges are present those are:

1) **Scalable key management:** Most existing system manages group based on their subscription by using group key management schemes. There is also another method given as subscription filter based authorization model but in this event can go to different group of subset, making it infeasible to setup static groups. Optimizations like key caching and the worst case key management have been suggested [10].
2) **Secure content based event routing:** Many existing system have used secure multicast network between publishers and subscribers. Secure content based event routing can be achieved by routing publisher to subscribers using multiple independent paths. In this frequency of all routing labels on an event appears not distinguishable [10].

E. Drawbacks of traditional security mechanisms

In Public Key Infrastructure (PKI), data can be encrypted for particular user. Receiver has to generate public/private keys and verify its public key to certificate authority after that sender can encrypt data. When dealing with large numbers of users, by using subscriber's every event to be encrypted. This is where Public Key Infrastructure (PKI) turning inefficient [14].

Subscribers are clustered according to their subscriptions. In this situation subscription confidentiality is very hard to provide. Events of children can be decrypted by parents. So to strengthen the weak notion of confidentiality, mechanism should be provided.

4. Proposed Methodology

D. Boneh and M.K. Franklin projected Identity Base Algorithm (IBE) is used for encryption[6]. In our methodology a SK-IBE (Sakai and Kasahar) encryption algorithm is used. It has better performance than BF-IBE algorithm. Especially, SK-IBE is also very practical in multiple PKG environments. Unlike the BF-IBE, this one provides an explicit redundancy-based rejection mechanism for mal-formed cipher texts.

5. Conclusion

We have prepared a report for different topics of Publish/Subscribe System. This report includes confidentiality and authentication in broker-less content based publish/subscribe system, semantic overlay, access control, identity-based encryption, security parameters and initialization, key generation for publishers/subscribers, publishing events, secure event dissemination, drawbacks of traditional security mechanisms. Based on such report, we surveyed dynamic publish/subscribe, security issues, methods of security, secure content based event routing, scalable key management.

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] 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.
[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext- Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, 2007.
[5] P. Pietzuch, "Hermes: A Scalable Event-Based Middleware," PhD dissertation, Univ. of Cambridge, Feb. 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] 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.
[8] H. Khurana, "Scalable Security and Accounting Services for Content-Based Publish/Subscribe Systems," Proc. ACM Symp. Applied Computing, 2005.
[9] 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.
[10] Prakash, "Secure Distribution of Events in Content-Based Publish Subscribe Systems," Proc. 10th Conf. USENIX Security Symp., 2001.
[11] 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.
[12] A. Shikfa, M. O ¨ nen, and R. Molva, "Privacy Preserving Content-Based Publish/Subscribe Networks," Proc. Emerging Challenges forSecurity, Privacy and Trust, 2009.
[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] 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 Event-Based Systems (DEBS), 2010.
[15] 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.
[16] A. Shamir, "Identity-based cryptosystems and signature schemes", in Advances in Cryptology – Crypto '84, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, pp. 47-53, 1984.