Secure Publish/Subscribe System using SK IBE

Approach
Onkar P. Kasarlewar

Department of Computer Engineering, AISSMS College of Engineering 1 Kennedy Road Pune - 411 001, Maharashtra, India

Abstract— Providing essential security mechanisms like authentication and confidentiality is very difficult in a publish/subscribe system. Many-to-many communications and loosely coupling of publishers and subscribers is the strength of Publish/Subscribe System. Authentication of publishers and subscribers is hard to accomplish because of the loosely coupling of publishers and subscribers. In the existing system, methodology to provide confidentiality and authentication in a broker less distribute/subscribe system is described. To handle the needs of Publish/Subscribe System, Pairing based cryptography is used. Also an algorithm is given to arrange subscribers according to their subscriptions. Existing system uses searchable encryption and also multicrodential routing used to disseminate the new event to subscribers. It strengthens the weak subscription confidentiality. In the proposed system, a SK IBE algorithm is used to improve the security of publish/subscribe system. In previous system, BF-IBE scheme is used. Proposed SK IBE is more secure than that of BF IBE. Particularly in encryption, SK IBE has better performance than BF IBE. As SK IBE uses hash function instead of maptopoint operation, it is faster than BF IBE.

Keywords— Publish/Subscribe ,Identity Based Encryption Broker-Less, Security

I. INTRODUCTION

Due to the decoupling of publishers from subscribers, the publish/subscribe (pub/sub) communication model has achieved high popularity. Publishers distribute/publish data into the pub/sub network, and subscribers provide subscriptions which describes their interest in events. Without publishers knowing the set of subscribers, published events are delivered to their appropriate subscribers. This decoupling is generally guaranteed by routing over a broker system [1]. In later systems, publishers and subscribers arrange themselves in a broker less routing framework, building an event forwarding overlay [2].

Content based pub/sub is the model that gives the most expressive subscription framework, where subscriptions provide limitations on the message content. It is helpful for large scale distributed applications because of its expressiveness and asynchronous nature, for example, environmental monitoring, traffic control, and news distribution. Of course, pub/sub needs to give supportive components to complete the essential security requirements of these applications, for example, confidentiality and access control.

In the setting of pub/sub system, access control implies that only authenticated publishers are permitted to distribute events in the system and only those events are delivered to authorized subscribers. In addition, the content of events ought not to be revealed to the routing framework and a subscriber ought to get all related events without exposing its subscription to the system. Solving these security issues in a publish/subscribe framework forces new difficulties. For example, end-to-end authentication utilizing a Public Key Infrastructure clashes with the loose coupling of publishers and subscribers, a key prerequisite for building scalable publish/subscribe system. For PKI, publishers must keep up the public keys of all intrigued subscribers to encrypt events. Subscribers must know the public keys of all related publishers to confirm the authenticity of the events.

Besides, conventional systems to give confidentiality by encrypting the entire event message clash with the content based routing standard. Henceforth, new methodologies are required to route encrypted events to subscribers without knowing their subscriptions and to permit subscribers and publishers authenticate one another without knowing one another. In the existing system, another methodology is provided to enable authentication and confidentiality in a broker less publish/subscribe system. This methodology permits subscribers to maintain credentials as per their subscriptions. Private keys allocated to the subscribers are labeled with the credentials. A publisher assigns each encrypted event with a set of credentials. Also, Identity Based Encryption (IBE) [3], [4] methodologies are implemented to guarantee that a specific subscriber can decrypt an event if there is a match between the credentials labeled with the event and the subscribers credentials.
the event and the key; and to permit subscribers to verify the authenticity of events.

II. RELATED WORK

The literature survey is divided into two categories which are: Approaches based on Broker Network, Approaches based on Semi-Trusted Broker Network.

A. Approaches based on Broker Network

In the study by C. Raiciu and D.S. Rosenblum [5], they had introduced an investigation of confidentiality in content-based publish/subscribe, attaining some of the security concerns specific to this interaction model. They had displayed a formal. Security model and analyzed the general C-CBPS issue, indicating out its limitations. They had provided provably secure procedures that permit content based routing for the huge amount of applications. They have depicted two conventions that support range matches in C-CBPS yet can likewise be applied in different areas.

J. Bacon et al [6] presented architecture which contains ad-ministration domains sharing a dedicated event-broker system. They had discovered this to be suitable for some applications. They likewise accepted a secure server per domain that handles credentials and activates parts as per policy. With access con-trol functionality located in the client-hosting brokers, they had the capacity to enforce RBAC on the publish/subscribe clients. Generally, separating event-management functionality into event service makes access control simpler to enforce than in a peer-to-peer methodology where the client and event service are co-located. The latter appears unsuitable for applications transmitting sensitive data. They have expected content based routing, for proficiency of communication, instead of broadcast routing. At the point when a few brokers are not trusted to see particular sensitive information this style of routing can be utilized, with the modifications they provided.

M. Ion et al [7] given a solution for providing confidentiality in pub/sub frameworks. Their solution is an encryption plan based on CP-ABE, KP-ABE and multi-client SDE. Their plan supports both the publication and the subscription confidentiality property while in the meantime does not oblige publishers and subscribers to share secret keys. In spite of the fact that events and filters are encrypted, brokers can perform event filtering without realizing any data.

At last, their plan permits subscribers of express filters that can characterize any monotonic and non-monotonic imperatives on events.

M. Srivatsa et al [8] have introduced EventGuard, reliable framework for ensuring publish/subscribe services from different attacks. Event Guard offers security features that are basic to publish-subscribe overlay services, for example, confidentiality, authenticity, integrity, and strength to flooding based DoS attacks. We have depicted the two key segments of Event Guard. The first segment is a suite of security guards that protects the essential publish and subscribe operations from DoS attacks and unauthorized reads and writes. The second segment is a flexible publish-subscribe system design that is equipped for giving secure yet adaptable message routing, counterering message dropping-based DoS attacks. A remark-able feature of Event Guard is its combined security structure that meets both security objectives for shielding the pub-sub overlay services from different susceptibility and threats and performance objectives for keeping up the adaptability and simplicity of the general framework while giving security guarantees.

S. Choi et al [9] presented a safe CBPS framework based on Asymmetric Scalar product Preserving Encryption to offer notification and subscription confidentiality and to diminish matching complexity. Their techniques help range filtering, equality filtering, covering, conjunction filtering, and inequality filtering, which are crucial in CBPS. Furthermore, their solution does not cause false positives, rather than existing work, for example, C- CBPS. Also, they proposed another technique for secure aggregation utilizing homomorphic functions and ASPE.

B. Approaches based on Semi-Trusted Broker Network:

Objective of P. Pietzuch [10] was to develop Hermes event-based middleware platform. They depicted its layered architecture and the two event routing algorithm supported by Hermes, type based routing, which supports subscriptions as per an event type, type-and-attribute-based routing, which gives content-based filtering with respect to event attributes also. Both routing algorithms utilize meeting nodes to develop adaptable event dissemination trees on top of a distributed hash table. Due to their prerequisite of programming language integration, they developed the routing algorithms with event type inheritance and support for super type subscriptions. They likewise presented the fault-tolerance mechanisms in the algorithms that are focused around soft-state approach and the replication of meeting nodes. A model implementation of Hermes was proposed in detail, as was an assessment of Hermes routing in a distributed frameworks simulator, contrasting it with the Siena routing algorithm, which is standard for content-based routing of events.

L. Opyrshal and A. Prakash [11] recognized the "safe end-point delivery” issue and investigated various
probable solutions. They were concerned about providing confidentiality when sending events from brokers to subscribers. The issue is that in content-based frameworks, each event can possibly have a different set of intrigued subscribers. There are $2N$ probable subsets, where $N$ is the number of subscribers. With a huge number of subscribers it is infeasible to setup static security groups for each probable subset. Various key management frameworks for group communication tackle a similar issue yet none of them was intended to handle the dy-namic nature of content based event delivery. They investigated various dynamic caching methodologies. A basic solution is to encrypt every event independently for each one interested subscriber; however this obliges a huge number of encryptions for substantial sets of subscribers. Their primary objective is to decrease the number of encryptions needed to deliver privacy while sending events to interested subscribers. The number of encryptions is essential as it makes an interpretation straightforwardly into message throughput.

H. Khurana [12] demonstrated a solution for providing confidentiality, integrity, and authentication of events as they are routed through a content based publish/subscribe network. Their solution supposes an untrusted broker network. In this context their solution allows brokers to do content based matching and routing with respect to clear text parts of events yet does not reveal sensitive event content to the brokers as they are encrypted. The solution utilizes Jakobsson’s proxy re-encryption methods to disseminate event encryption keys by means of a transformation methodology to authorized sub-subscribers without obliging any direct interactions of publishers and subscribers. Additionally, they provide verifiable usage-based accounting services by logging all transformations and giving publishers with the logs so they can charge subscribers.

### III. PROPOSED SYSTEM

In the proposed system, subscribers are allowed to maintain credentials as per their subscriptions. Every subscriber is assigned with the private keys which are labeled with the credentials. Every event is assigned with set of credentials by publisher. Also Identity Based Encryption is used to ensure that a subscriber can decrypt event only when the credentials associated with the event and the key are matched. It also allows subscriber to verify the authenticity of received events. Subscribers are arranged in tree according to containment relationship between their credentials. Searchable encryption is presented which is used to route of encrypted events efficiently. To improve the weak subscription confidentiality, Multicredential routing is provided. In the existing system, BF IBE scheme is used. Instead of that SK IBE is used which is more secure than BF IBE. Also SK IBE has better performance. No pairing computation is required for SK IBE.

#### A. Algorithm SK IBE Algorithm

SK-IBE is specified by four polynomial time algorithms: Setup: Given a security parameter $k$, the parameter generator follows the steps.

1. Generate three cyclic groups $G_1, G_2$ and $G_T$ of prime order $q$, an isomorphism from $G_1, G_2$, a bilinear pairing map $e : G_1 \times G_2 \rightarrow G_T$ pick a random generator $P_2 \in G_2$ and set $P_1 = (P_T)$.

2. Pick a random $S \in Z_q$ and compute $P_{pub} = SP_2$.

3. Pick four cryptographic hash functions $H_1 = 0$, $0, 1 \in Z_q, H_2 = G_T \in \{0, 1\}$, $H_3 : f \mapsto f$, $H_4 : f \mapsto g^n f; 0; 1g n n n n$ for some integer $n > 0$.

The message space is $M = f0; 1g^n$. The ciphertext space is $C = G_1 f0; 1g^n f0; 1g^n$. The master public key is $M_{pk} = (q, G_1, G_2, G_T : e^{\cdot n}; P_1, P_2, P_{pub}; H_1, H_2, H_3)$, and the master secret key is $M_{sk} = S$.

Extract: Given an identifier string $ID_A f0; 1g$ of entity $A$, $M_{sk}$ and $M_{pk}$.

The algorithm returns $d_A = s + H_1(ID_A)$

Encrypt: Given a plaintext $m$, $ID_A$ and $M_{pk}$, the following steps are performed.

1. Pick a random $f0; 1g^n$ and compute $r = H_4(m)$.

2. Compute $Q_A = H_2(ID_A)P_T + P_{pub}; g^r = e^{\cdot r} P_1 P_2$.

3. Set the ciphertext to $C = (rQ_A; H_2(g^r); m H_3(\cdot) )$.

Decrypt: Given a ciphertext $C = (U, V, W)$, $C, ID_A; d_A$ and $M_{pk}$, follow the steps:

1. Compute $g^r = e^{\cdot r}(U; d_A)$ and $0 = V H_3(g^r)$.
2) Compute \( m' = W H(0) \) and \( r_0 = H(x, m') \).

3) If \( U \neq r' (H(ID_A)p_1 + P_{pub}) \), output \( ? \), else return \( m' \) as the plaintext.

B. Mathematical Model

Set Theory

System \( S \) is represented as \( S = fR, I, Mg \)

Table captions appear centered above the table in upper and lower case letters. When referring to a table in the text, no abbreviation is used and "Table" is capitalized.

1) Registration Process

\( R = fP, Sg \)

Where, \( R \) is the set of publishers and subscribers

1) \( P = fP_1, p_2, p_3, ..., png \)

Where, \( P \) is represented as a set of publishers and \( p_1, p_2p_2n \) are the number of publishers.

2) \( S = fS_1, s_2, ..., sng \)

Where, \( S \) is the set of subscribers and \( s_1, s_2, s_n \) are the number of subscribers.

2) Identity based encryption

\( I = fi_1, i_2, ..., ing \)

Where, \( I \) is represent as a Identity and \( i_1, i_2, ..., in \) are number of identity.

1) Credentials

\( C = fc_1, c_2, ..., cng \) Where \( C \) is the set of credentials and \( c_1, c_2, ..., c_n \) represent as a number of credentials.

3) Formula:

1) Public key for a credential \( Cred_{ij} \) is given as

\[ Pu_{i,j}Cred_{ij}A_{ij}S_{ij}B_{ij}E_{ij} \]

Where \( SUB \) is used to differentiate the keys used for the verification of valid events from the ones used to provide event confidentiality and \( Ai \) is attributes.

2) For cyphertext:

\[ E = fe_1, e_2, ..., eng \]

Where, \( E \) is the set of cyphertext and \( e_1, e_2, ..., e_n \) are the number of cyphertext.

4) SK-IBE

\( M = fiD, EN, Deg \)

Where, \( M \) is the set of identity, encryption and decryption.

IV. CONCLUSION

In this paper, methodology is proposed to provide authentication and confidentiality in broker less publish/subscribe system. Specifically, mechanisms are developed to assign credentials to publishers and subscribers as per their subscriptions and advertisements. Publishers and subscribers assigned by private keys and cipher texts are labeled with credentials. An event can be decrypted only if credentials associated with the event and its private keys are matched. Proposed system allows subscribers to verify the authenticity of events. Additionally, to improve the security and time, SK IBE is implemented. In the broker less publish/subscribe system, organizing peers may cause higher message overhead as system leads to the forwarding the same messages

ACKNOWLEDGEMENTS

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We also thank the college authority for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

REFERENCES


