ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Identity-Based Encryption Approach to Provide Confidentiality and Authentication in Publication / Subscription System without an Intermediary

Prerna V. Umalkar, Prof. N. D. Kale,

Department Of Computer Engineering, Padmabhushan Vasantdada Patil Institute of Technology, Pune, India

ABSTRACT: In a publication / subscription system based on content, authentication and confidentiality are very demanding. Due to the free coupling of publishers and subscribers to obtain the authentication of publishers and subscribers, it is very difficult, for example, the identification / authentication of the user and the confidentiality of the transmitted data are the main challenges that most systems faces in distributed. The existing subscription system uses intermediaries, but there are still some problems with message delivery. This document uses the identity-based encryption approach to provide confidentiality and authentication in a content-based publication / subscription system without an intermediary. There are three main objectives for the secure publication / subsystem system that must be compatible with authentication, privacy and scalability. Our system stores only unique events by using hash mechanism. To achieve security, the event is dividing into multiple fragments and instead of storing on single node, fragments stores on multiple nodes.

KEYWORDS*:* Content-based, publish/subscribe, broker-less, security, identity-based encryption, authentication, confidentiality, scalability, hash, fragments.

I. INTRODUCTION

The Internet has changed the scale of distributed systems and now these distributed systems all over the world involve thousands of users whose behavior and position can quickly change. Nowadays, Internet applications need to access information through different platforms, organizational limits and a large number of data producers and consumers. These restrictions require more flexible systems and models that reflect the decoupled and dynamic nature of applications. Today the publication / subscription system is receiving more attention, as it provides the freely coupled form of interaction needed in such large-scale applications.

A. Publish-Subscribe System:

The Publish-Subscribe system is a communication infrastructure that allows access to data through a large number of data editors and data subscribers, which are disseminated on the Internet. Here publishers publish information or data in the form of data events and subscribers show their interests in events by sending subscriptions to the network of the subscription system for the publication. In many publication subscription systems, publishers send messages to an intermediate intermediary and subscribers register their subscriptions with the broker and the broker executes the filter. Normally, the broker stores and forwards the function to send messages from publishers to subscribers. The publication / subscription system has gained a lot of attention due to the dissociation of publishers and subscribers.

The publication subscription system has two important characteristics

1. The first is the slow coupling: the communication of users in the publication subscription system is unique; it means that the editors do not need to know who the recipients of the information are and even the recipients do not need to know where they come from information.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

2. According to scalability, the publication subscription system allows a dynamic and flexible communication environment for a large number of users.

The Publish-subscribe system offers the opportunity for better scalability through parallel operations, network-based routing, etc.

B. Public Key Infrastructure:

In PKI, senders and receivers are closely connected means that if an issuer wishes to send a message to a recipient, the recipient must generate a public / private key pair and must obtain its public key signed by a certification authority and send it to the sender. . There is an overload to obtain the public key from the recipients of the certification authority. Then, a new mechanism is needed to overcome this drawback. One of these mechanisms is the encryption of messages through cryptography based on identity.

C. Identity based Encryption:

Identity-based encryption is a scheme in which a user's public key consists of unique user information.

D. Hash Mechanism:

System only allows unique events by using SHA-256 algorithm.

II. REVIEW OF LITERATURE

1. **M.Nabeel, N. Shang, and E. Bertino (2012) have represents Efficient Privacy Preserving Content Based Publish Subscribe Systems [1].**
   The author proposes a new approach to preserve the privacy of subscriptions made by subscribers and the confidentiality of data published by content publishers that use cryptographic techniques when third-party content agents are used to make routing decisions based on the content. The proposed protocols are expressive to support any type of subscription and are designed to function efficiently. The author distributes the work in such a way that the load on the Content Agents, where the bottleneck is in a CBPS system, is minimized. Expand a popular CBPS system using our protocols to implement a CBPS system that preserves privacy.

2. **W.C.Barker and E.B. Barker (2012) has represents SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher [2].**This publication specifies the triple data encryption algorithm (TDEA), which includes the cryptographic engine of the main component, the data encryption algorithm (DEA). When implemented in SP 800-38-compliant operating mode and a FIPS 140-2 compliant encryption module, federal organizations can use TDEA to protect sensitive, unclassified data. Data protection during transmission or during storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. This Recommendation defines the mathematical steps necessary to cryptographically protect data using TDEA and then processes the protected data. The TDEA is available for use by federal agencies in the context of a comprehensive security program consisting of physical security procedures, good information management practices and access controls to the computer system / network.

3. **M.A.Tariq, B. Koldehofe, G.G. Koch, I. Khan, and K. Rothermel (2011) has developed Meeting Subscriber-Defined QoS Constraints in Publish/Subscribe Systems [3].**The author proposes a peer-to-peer approach to meet individual subscriber delay requirements in the presence of bandwidth limits. This approach allows subscribers to dynamically adjust the granularity of their subscriptions based on their bandwidth restrictions and delay requirements. Subscribers maintain the overlay in a decentralized manner, establishing only connections that meet specific delay requirements and provide messages that exactly match the granularity of subscriptions.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

4. **M.Srivatsa, L. Liu, and A. Iyengar (2011) has represents EventGuard: A System Architecture for Securing Publish-Subscribe Networks [4].**
The author proposes a peer-to-peer approach to meet the individual delay requirements of the subscriber in the presence of bandwidth limits. This approach allows subscribers to dynamically adjust the granularity of their subscriptions based on their bandwidth restrictions and the delay requirements. Subscribers maintain the overlay in a decentralized manner, establishing only connections that meet the specific delay requirements and provide messages that exactly match the granularity of the subscriptions.

5. **A.Lewko, A. Sahai, and B. Waters (2010) has represents "Revocation Systems with Very Small Private Keys [5].**
The author designs a method for the creation of public key transmission cryptography systems. Our main technical innovation is based on a new technique of "two equations" to revoke users. This technique translates into two key contributions: first, our new schema is overloaded with an encrypted text size O (r), where r is the number of users revoked and the size of public and private keys is just a number \ emph {constant} of group elements of a group of first-order elliptic curves. In addition, the public key allows us to encrypt an unlimited number of users. Our system is the first to achieve these parameters.

6. **H.-A. Jacobsen, A.K.Y. Cheung, G. Li, B. Maniymaran, V. Muthusamy, and R.S. Kazemzadeh (2010) has represents The PADRES Publish/Subscribe System [6].**The author presents PADRES, the publication / subscription model with the ability to correlate events, access data produced in the past and in the future in a uniform manner, balance the traffic load between intermediaries and manage network failures. The new model can filter, aggregate, correlate and project any combination of historical and future data. A flexible architecture is proposed that consists of distributed and replicated data repositories that can be prepared based on the availability of exchange, storage overload, query overload, query delay, load distribution, parallelism, redundancy and location. This chapter provides a detailed description of the publication / subscription system based on the content of PADRES.

7. **M.Ion, G. Russello, and B. Crispo (2010) has developed "Supporting Publication and Subscription Confidentiality in Pub/Sub Networks [7].**The publication / subscription model offers a freely coupled communication paradigm in which applications interact indirectly and asynchronously. Publishing applications generate events that are sent to affected applications through an intermediary network. Subscription applications express interest in specifying the filters that intermediaries can use for event routing. Supporting the confidentiality of the messages exchanged remains a challenge. First, it is desirable that any scheme used to protect the confidentiality of events and filters does not require publishers and subscribers to share secret passwords. Actually, this restriction is against the free coupling of the model. In addition, this scheme should not limit the expressiveness of the filters and should allow the intermediary to filter events to direct events to interested parties. Existing solutions do not completely solve these problems. In this document, we provide a new scheme that admits (i) confidentiality for events and filters; (ii) filters can express very complex restrictions on events even if intermediaries can not access any information about events and filters; (iii) and finally does not require that publishers and subscribers share the keys.

8. **S.Choi, G. Ghinita, and E. Bertino (2010) has represents A Privacy-Enhancing Content-Based Publish/Subscribe System Using Scalar Product Preserving Transformations [8].**Users of content-based publication / subscription systems (CBPS) are interested in receiving data elements with values that meet certain conditions. Each user sends a list of subscription specifications to an intermediary, which routes the data elements of the editors to the users. When a broker receives a notification that contains a value from an editor, it forwards only to the subscribers whose requests match the value. However, in many applications, the published data is confidential and its content should not be disclosed to intermediaries. In addition, the subscription of a user may contain confidential information that must be protected by intermediaries.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Therefore, it poses a difficult challenge: how to direct publisher data to appropriate subscribers without intermediate intermediaries learning the plain text values of notifications and subscriptions. To this extent, intermediaries must be able to carry out operations in addition to the encrypted content of subscriptions and notifications. Such operations can be as simple as equality equalization, but often require more complex operations, such as determining the inclusion of data in a range of values. Previous work has attempted to solve this problem through the use of unidirectional data associations or specialized cryptographic functions that allow the evaluation of the conditions in the encrypted texts. However, these operations are computationally expensive and the resulting CBPS has no scalability. Since rapid diffusion is an important requirement in many applications, we focus on a new data transformation method called ASPE (Encryption of preservation of asymmetric scalar products).

9. **Y.Yu, B. Yang, Y. Sun, and S.-l. Zhu (2009) has represents Identity Based Signcryption Scheme without Random Oracles [9].** The author, motivated by the cryptography scheme based on the identity of Waters, proposes the first cryptography scheme based on identity without random oracles. We show that the proposed scheme is safe in the standard model. Specifically, we demonstrate its semantic security under the harshness of the Decisional BiliearDiffie-Hellman problem and its imperceptibility under the Computational Diffie-Hellman hypothesis.

10. **A.Shikfa, M. O ¨ nen, and R. Molva (2009) has represents "Privacy-Preserving Content- Based Publish/Subscribe Networks [10].** The author addresses the issue of privacy of end users in CBPS. This problem poses a demanding requirement for the management of encrypted data for routing based on secure content and encrypted subscription information. We suggest a solution based on multiple schemes of commutative encryption to allow intermediaries to perform network matching and content-based routing without having access to the contents of the package. This is the first solution that avoids the exchange of keys between end users and is aimed at an advanced model of CBPS where brokers can also subscribe at the same time.

III. EXISTING SYSTEM

In the existing publication / subscription system, authentication and confidentiality are a very challenging issue due to the free coupling of publishers and subscribers. Getting authentication between publishers and subscribers is very difficult. In the same way that there is an overload to obtain the public key of the recipients of the certification authority.

Disadvantages:

- Contain broker network.
- Issue regarding to Authentication.
- Less data Confidentiality and Scalability.
- Does not maintain system user friendly.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

IV. SYSTEM ARCHITECTURE

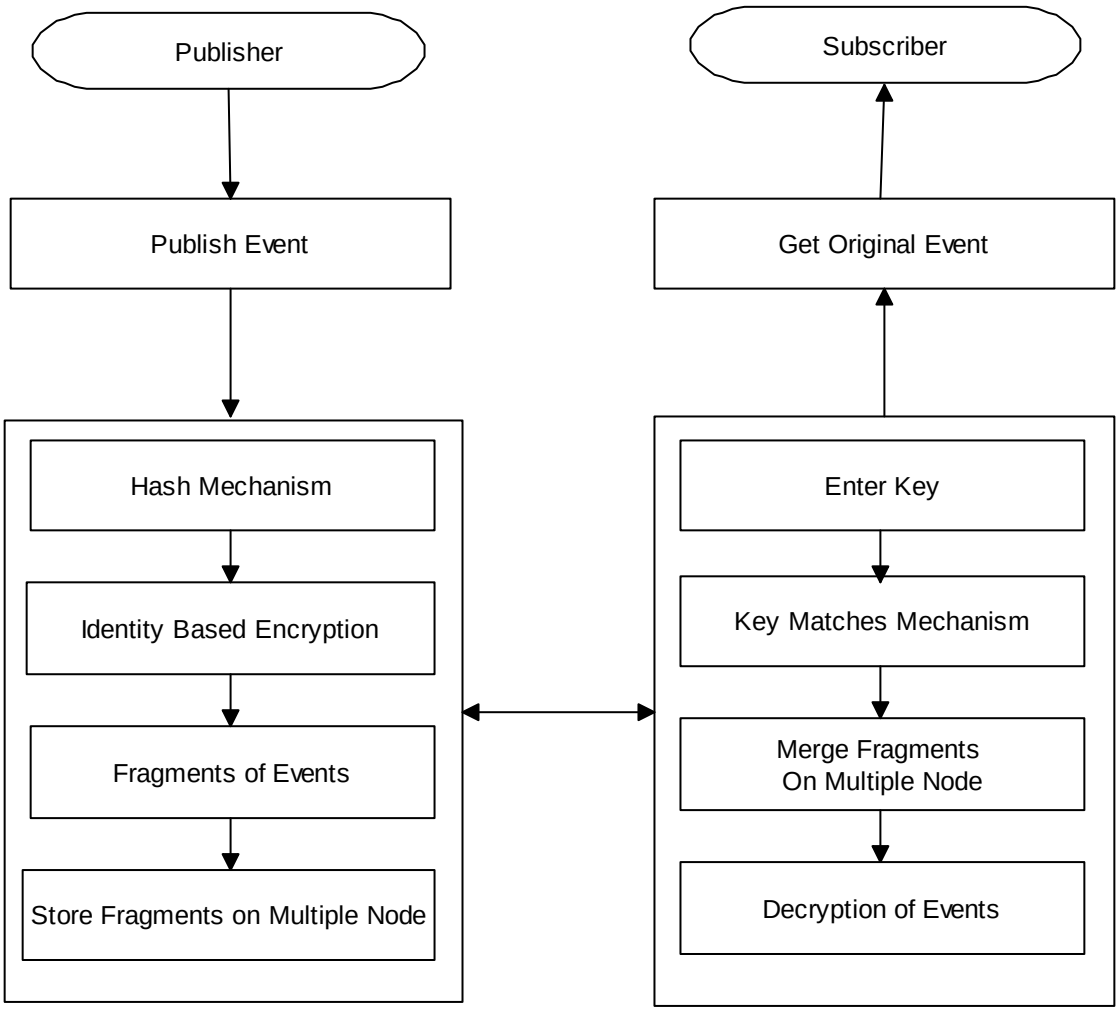


Figure. System architecture

System Overview:
The system contains two modules i.e. Publisher and Subscriber.

1. **Publisher:**

Publisher is responsible to publish the events. Only unique event is published for that purpose hash mechanism is used. To encrypt the event identity based encryption is used. The identity-based cryptographic scheme is a public-key cryptography scheme in which the public key can be a valid user string. In identity-based encryption, a key server generates and maintains a primary public key and a primary private key. When a sender wishes to encrypt a message and send it, it uses the primary public key with any unique identity of the recipient, such as an email address. If a recipient wants to read that message, it is necessary to obtain the private key from the key server. After that event is divided into number of fragments and fragments stores on multiple nodes for security mechanism.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

2. Subscriber:

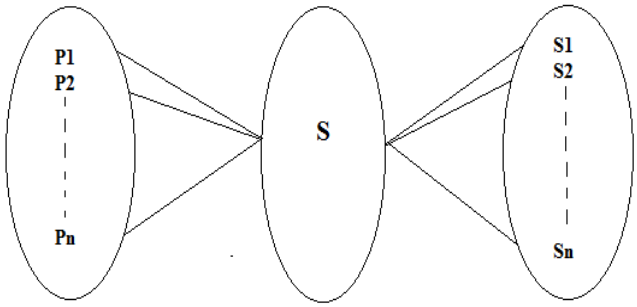
Whensubscriber wants to access the event, send the key request to Publisher. After granted permission or key matching, all fragments of events merge from multiple nodes and decrypt event successfully and return to Subscriber.

Advantages:

- 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.
- Proposed secure pub/ sub system which is to support authentication, confidentiality, and scalability.
- Support broker less network.
- Achieves security by dividing events into number of fragments and store on multiple nodes instead of single node.

V. MATHEMATICAL MODELING

A] Mapping Diagram



Where,

$P_1, P_2 \ldots P_n$= No. of Publisher.

S = System

$S_1, S_2, \ldots\ldots S_n$=No. of Subscriber

B] Set Theory

S={s, e, X, P, Y,Φ}

Where,

s = Start of the program.

1. Authentication.

Where,

R=Register

L = Login, UN = User name, PWD = Password

To access the facilities of system, Publisher and Subscriber has to Register and login to system.

X = Input of the program.

2. Identify Input as

Input should be Events.

$X = \{E_1, E_2, \ldots\ldots E_n\}$

Where,

$E_1, E_2, \ldots\ldots E_n$ =No. of Events uploaded by publisher.

P= Process of the program

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

3. **Identify Process P as**

- **Event Fragmentation:**
  Divide event into no. of Fragments(i.e. Converting event into no. of chinks)
  Fs = Size/Nof
  Where,
  Fs= Fragment Size.
  Size = Size of source event
  NoF = Number of fragments
- **Encryption:**
  By using Identity based encryption generate ciphertext of each fragment.
- **Node Creation:**
  for(int i= 1; i<=No Of Node; i++)
  {
  File(i).mkdirs();
  }

- **Fragment Placement:**
  E_r= {e_1,e_2,……e_n}
  S_f= {sizeOf(e_1), sizeOf(e_2)….. sizeOf(e_n)}
  Col={open_color,close_color}
  for(int i= 1; i<=No Of Node; i++)
  {
  //place fragments on nodes
  }

Y = Output of the program

4. **Identify Output Y as**

Y = {Dec(E_1)….Dec(En)}
Where,
Dec(E_1)….Dec(En) =Decryption of the Event..

- **Retrieve Fragments:**
  Retrieve all fragments of particular Events.
  E= {e_1,e_2,……e_n}

- **Merge Fragments:**
  for(int i= 1; i<=No Of Fragments; i++)
  {
  Merge(i);
  }

- **Decryption:** If key match then Subscriber can download the Event.

φ = Success or failure condition of system.

Failures:

1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 3, March 2018

Success:
1. Search the required information from available in Datasets.
2. User gets result very fast according to their needs.

Above mathematical model is NP-Complete.

VI. CONCLUSION

The System developed a broker-less publish-subscribe system and used an Identity based encryption scheme for publish-subscribe system. This Identity based encryption scheme made use of a string which uniquely identify a user as a public key of that user. Data confidentiality has been provided in this paper by encrypting the information or data using Identity based encryption scheme. It is ensured that a subscriber can decrypt data only if he has the valid key. To achieves security by dividing events into number of fragments and store on multiple nodes instead of single node.

REFERENCES

1. 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.
2. 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.
3. 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.
4. 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.
5. A.Lewko, A. Sahai, and B. Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, 2010.
6. 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.
7. 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.
8. 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.
9. 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.
10. A. Shikfa, M. O ¨ nen, and R. Molva, "Privacy-Preserving Content- Based Publish/Subscribe Networks," Proc. Emerging Challenges for Security, Privacy and Trust, 2009.