IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 7, Issue 6, June 2018

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

Ms. Prerna Umalkar[1], Prof. N.D.Kale[2]

PG Student, Comp. Engg , PVPIT, Pune, India [1]

Assistant Professor, Comp. Engg , PVPIT, Pune, India [2]

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 subscriptionsystem 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.

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.

DOI 10.17148/IJARCCE.2018.7625

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. LITERATURE SURVEY

1. M.Nabeel, N. Shang, and E. Bertino (2012) have represents Efficient Privacy Preserving Content Based Publish Subscribe Systems [1]. The creator proposes another way to deal with save the security of memberships made by supporters and the secrecy of information distributed by content distributers that utilization cryptographic systems when outsider substance specialists are utilized to settle on steering choices in view of the substance. The proposed conventions are expressive to help any kind of membership and are intended to work effectively. The creator disseminates the work such that the heap on the Content Agents, where the bottleneck is in a CBPS framework, is limited. Extend a mainstream CBPS framework utilizing our conventions to execute a CBPS framework that jelly protection.

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 production determines the triple information encryption calculation (TDEA), which incorporates the cryptographic motor of the fundamental segment, the information encryption calculation (DEA). At the point when executed in SP 800-38-consistent working mode and a FIPS 140-2 agreeable encryption module, government associations can utilize TDEA to secure delicate, unclassified information. Information insurance amid transmission or amid capacity might be important to keep up the classification and trustworthiness of the data spoke to by the information. This Recommendation characterizes the scientific advances important to cryptographically ensure information utilizing TDEA and afterward forms the secured information. The TDEA is accessible for use by government offices with regards to a far reaching security program comprising of physical security techniques, great data administration practices and access controls to the PC framework/organize.

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 creator proposes a distributed way to deal with meet individual endorser defer necessities within the sight of transfer speed limits. This approach enables endorsers of progressively change the granularity of their memberships in view of their data transmission limitations and defer prerequisites. Endorsers keep up the overlay in a decentralized way, setting up just associations that meet particular defer prerequisites and give messages that precisely coordinate the granularity of memberships.

4. M.Srivatsa, L. Liu, and A. Iyengar (2011) has represents Event Guard: A System Architecture for Securing Publish- Subscribe Networks [4]. The creator proposes a shared way to deal with meet the individual defer necessities of the supporter within the sight of data transfer capacity limits.
This approach enables supporters of progressively alter the granularity of their memberships in view of their data transfer capacity limitations and the postpone prerequisites. Supporters keep up the overlay in a decentralized way, setting up just associations that meet the particular defer prerequisites and give messages that precisely coordinate the granularity of the memberships.

5. A.Lewko, A. Sahai, and B. Waters (2010) has represents Revocation Systems with Very Small Private Keys [5]. The creator plans a strategy for the formation of open key transmission cryptography frameworks. Our fundamental specialized advancement depends on another procedure of ”two conditions” to renounce clients. This strategy converts into two key commitments: initially, our new composition is over-burden with a scrambled content size O (r), where r is the quantity of clients repudiated and the measure of open and private keys is only a number emph constant of gathering components of a gathering of first-arrange elliptic bends. Moreover, people in general key enables us to scramble a boundless number of clients. Our framework is the first to accomplish these parameters.

6. H.-A. Jacobsen, A.K.Y. Cheung, G. Li, B. Maniymaran, Muthusamy, and R.S. Kazemzadeh (2010) have represents The PADRES Publish/Subscribe System [6]. The creator presents PADRES, the production/membership display with the capacity to relate occasions, get to information delivered before and later on in a uniform way, adjust the activity stack amongst mediators and oversee arrange disappointments. The new model can channel, total, correspond and venture any mix of verifiable and future information. An adaptable engineering is suggested that comprises of circulated and imitated information storehouses that can be readied in light of the accessibility of trade, stockpiling over-burden, question over-burden, inquiry delay, stack appropriation, parallelism, repetition and area. This part gives a definite portrayal of the production/membership framework in view of the substance of PADRES.

7. M.Ion, G. Russello, and B. Crispo (2010) has developed Supporting Publicatioand Subscription Confidentiality in Pub/Sub Networks [7]. The distribution/membership display offers a uninhibitedly coupled correspondence

DOI 10.17148/IJARCCE.2018.7625

worldview in which applications connect by implication and no concurrently. Distributing applications create occasions that are sent to influenced applications through a go-between arrange. Membership applications express enthusiasm for determining the channels that mediators can use for occasion directing. Supporting the classification of the messages traded remains a test. To begin with, it is attractive that any plan used to ensure the privacy of occasions and channels does not require distributers and endorsers of offer mystery passwords. All things considered, this confinement is against the free coupling of the model. Furthermore, this plan ought not to restrict the expressiveness of the channels and ought to enable
the go-between to channel occasions to guide occasions to invested individuals. Existing arrangements don't totally take care of these issues. In this report, we give another plan that concedes (I) privacy for occasions and channels; (ii) channels can express extremely complex confinements on occasions regardless of whether mediators cannot get to any data about occasions and channels; (iii) lastly does not require that distributers and endorsers 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]. Clients of substance based production/membership frameworks (CBPS) are occupied with accepting information components with values that meet certain conditions. Every client sends a rundown of membership particulars to a mediator, which courses the information components of the editors to the clients. At the point when an agent gets a notice that contains an incentive from a manager, it advances just to the supporters whose solicitations coordinate the esteem. Be that as it may, in numerous applications, the distributed information is private and its substance ought not to be unveiled to middle people. Likewise, the membership of a client may contain classified data that must be secured by middle people. In this way, it represents a troublesome test: how to guide distributer information to fitting supporters without middle of the road go-betweens taking in the plain content estimations of warnings and memberships. To this degree, middle people must have the capacity to complete activities notwithstanding the scrambled substance of memberships and notices. Such activities can be as straightforward as fairness evening out, yet regularly require more perplexing tasks, for example, deciding the incorporation of information in a scope of qualities. Past work has endeavoured to take care of this issue using unidirectional information affiliations or specific cryptographic capacities that permit the assessment of the conditions in the scrambled writings. In any case, these activities are computationally costly and the subsequent CBPS has no versatility. Since fast dispersion is an essential necessity in numerous applications, we centre on another information change strategy called ASPE (Encryption of protection of uneven scalar items).

99. Y.Yu, B. Yang, Y. Sun, and S.-l. Zhu (2009) has represents Identity Based Signcryption Scheme without Random Oracles [9]. The creator, persuaded by the cryptography conspire in view of the personality of Waters, proposes the primary cryptography plot in light of character without arbitrary prophets. We demonstrate that the proposed plot is protected in the standard model. In particular, we show its semantic security under the brutality of the Decisional Biliear Diffie- Hellman issue and its subtlety under the Computational Diffie-Hellman theory.

110. A.Shikfa, M. O nen, and R. Molva (2009) has rep resents Privacy-Preserving Content- Based Publish/Subscribe Networks [10]. The creator tends to the issue of security of end clients in CBPS. This issue represents a requesting necessity for the administration of encoded information for directing in view of secure substance and scrambled membership data. We recommend an answer in view of various plans of commutative encryption to enable middle people to perform organize coordinating and content-based directing without approaching the substance of the bundle. This is the main arrangement that maintains a strategic distance from the trading of keys between end clients and is gone for a propelled model of CBPS where representatives can likewise buy in the meantime.

III.SYSTEM ARCHITECTURE OR SYSTEM OVERVIEW

A. 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.

B. Subscriber:

When subscriber 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.

C. Advantages:

1) The approach is highly scalable in terms of the number of subscribers and publishers in the system and the number of keys they manage. In particular, we have developed mechanisms to assign credentials to publish- ers and subscribers based on their subscriptions and advertisements.

DOI 10.17148/IJARCCE.2018.7625

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

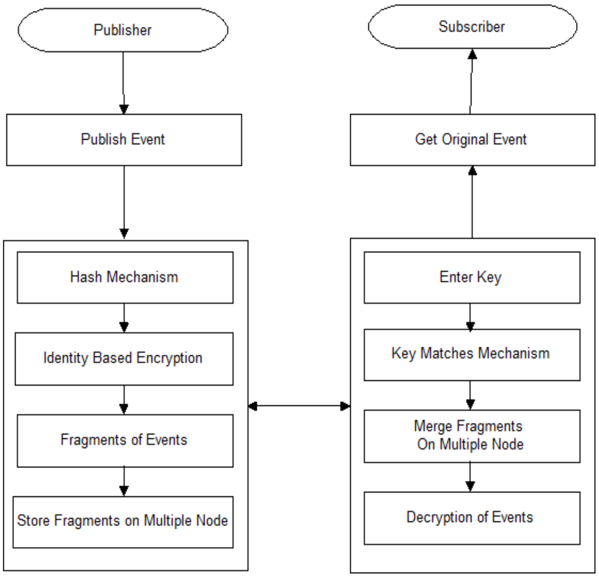

Fig.1. Proposed System Architecture

D. Algorithms Used:
1) SHA-256 Algorithm is used to calculate hash value.
2) Event fragmentation- Event is divided into no of fragments.
3) Encryption and Decryption- Identity based encryption generate cipher text of each fragment.
4) Event placement- Event fragment is place on different node.

E. Mathematical Model:

Set Theory

$S = \{ s, e, X, Y, \varphi\}\{ s, e, X, Y, t, F \varphi\}$

S = Set of system.

s = Start of the program.

- Register to system: Publisher/Subscriber provides own details.

- Authentication: $A= a_1,a_2..a_n$ Where,

A= No. of user attributes.(e.g username, password, emailed etc.)

Auth={Active/Inactive}

- Login to system. To perform functionality Publisher/Subscriber Login to system.

- Upload Data(File)

X = Input of the program

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

Where,

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

P=Process of the program

- Event Fragmentation: Divide Event(File) into no. of Fragments(i.e. Converting Event into no. of chunks)

$F_s = Size/N_f$

- Encryption: By using AES algorithm generate ciphertext of each fragment.

- Node Creation:

```
for(int i= 1; i<=No Of Node; i++)
{
 File(i).mkdirs();
}
```

- Fragment Placement: Col=open_color; close_color for(int i= 1; i<=No Of fragments; i++)

```
{
 //place fragments on nodes
}
```

- Download Event(File)

Y = Output of the program

- Retrieve Fragments: Retrieve all fragments of particular Event.

E= {f_1,f_2,f_n}

- Decryption: Generate plaintext of each fragment using AES algorithm.

- Merge Fragments:

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

e = End of the program

φ = Success or failure condition of system.

IV. SYSTEM ANALYSIS

Experimental evaluation is done to compare the proposed system with the existing system for evaluating the performance. The simulation platform used is built using Java framework (version jdk 7) on Windows platform. The system does not require any specific hardware to run; any standard machine is capable of running the application. By observing the graph we can conclude that the graph shows event related file downloading time.

The above figure shows that File Downloading Time of proposed system. As can be seen in Fig.2 x-axis represent File.

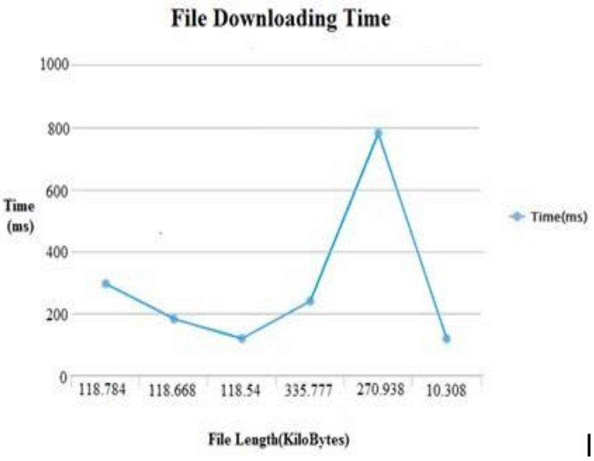

Fig.2. File Downloading Time

Length in Kilobytes and y-axis represents time in milliseconds. The above graph shows how much time system takes when subscriber want to download file.

Table 1: File Downloading Time

File Length (Kilobytes)	Time(ms)
118.784	300
118.668	190
118.54	120
335.777	250
270.938	800
10.308	60

V. CONCLUSION

The System developed a broker-less publish-subscribe sys- tem 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.

ACKNOWLEDGMENT

We take this golden opportunity to owe our deep sense of gratitude to our project guide **Prof. N.D. Kale**, for his instinct help and valuable guidance with a lot of encouragement throughout this paper work, right from selection of topic work up to its completion. Our sincere thanks to Head of the Department of Computer Engineering **Prof. B, K. Sarkar** who continuously motivated and guided us for completion of this paper. I am also thankful to all teaching and non-teaching staff members, for their valuable suggestions and valuable co-operation for partially completion of this work. We specially thank to those who helped us directly-indirectly in completion of this work successfully.

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, Natl Inst. of Standards Technology, 2012.

[3] M.A. Tariq, B. Koldehofe, G.G. Koch, I. Khan, and K. Rothermel, Meet- ing 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 Architec- ture 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, Princi- ples and Applications of Distributed Event-Based Systems. IGI Global, 2010.

[7] M. Ion, G. Russello, and B. Crispo, Supporting Publication and Subscrip- tion Confidentiality in Pub/Sub Networks, Proc. Sixth Intl 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 Transforma- tions, Proc. 21st Intl 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.

DOI 10.17148/IJARCCE.2018.7625