One Time Password Scheme for Identity Based Encryption

Padmavati Kshirsagar[1], S. Pratap Singh[2]

[1]Assistant Professor, Savitribai Phule University of Pune, SP's Institute of Knowledge College of Engineering, Pune, Shikrapur, India

[2]Professor, SP's Institute of Knowledge College of Engineering , Savitribai Phule University of Pune, *Pune, shikrapur, India*

Abstract: ***In content-based publish subscribe system authentication and confidentiality are most challenging security issues. This project presents a novel approach to provide confidentiality and authentications in a broker-less content-based publish subscribe system. The authentication of publishers and subscribers is done using pairing based cryptography. confidentiality of events is also ensured, by adapting the pairing-based cryptography mechanisms. IBE algorithm is used to solve confidentiality issue. 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 public and private master keys. The master public key can be 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. The overall approach provides fine-grained key management. Published events are routed to their relevant subscribers. The evaluation of this project provide security regarding 1) authentication and confidentiality of event dissemination. To achieve the authentication and confidentiality of user's and message OTP i.e One Time Password is used. OTP is dynamic password which changes every time the user logs in. An OTP is a set of randomly generated numbers that can act as a form identity for one time only. Once the password is used, it is no longer used for any further authentication. Whenever subscriber want to decrypt an event he has suppose to enter valid password that received as e-mail.***

Keywords: content-based, publish subscribe, peer to peer, security, identity-based encryption, OTP

1. Introduction

Publisher Subscriber System is Messaging pattern. Where the sender of system is called publisher and receiver of system is called subscriber. Publishers inject information into the publisher subscriber system, and subscribers specify the events of interest by means of subscriptions. Published events are routed to their relevant subscribers, without the publishers knowing the relevant set of subscribers, or vice versa. As this system is broker less, publisher subscriber contribute as peers to the maintenance of a self-organizing overlay structure. To authenticate publishers, we use the concept of advertisements in which a publisher announces beforehand the set of events which it intends to publish[1].There are three major goals for the proposed secure publishers subscriber system, namely to support authentication, confidentiality, and scalability. Authentication to avoid non eligible publications, only authorized publishers should be able to publish events in the system. Similarly, subscribers should only receive those messages to which they are authorized to subscribe. Confidentiality. in a broker-less environment, two aspects of confidentiality are of interest: 1) the events are only visible to authorized subscribers and are protected from illegal modifications, and 2)the subscriptions of subscribers are confidential and unforgeable.

2. Literature Survey

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system. Publish/Subscribe systems offer a helpful platform for delivering information (events) from publishers to subscribers in an anonymous fashion in distributed networks. These systems have several applications, including net services, stock quotes, free riding observation, and net games. Developing reliable publish/subscribe schemes for dynamic distributed systems is difficult owing to the wants for scalability for giant teams of unpredictable subscribers[2]. In this paper, a completely unique style principle for self dynamic and reliable content-based publish/subscribe systems and perform a comparative analysis of its probabilistic and settled implementations. Additional specifically, content-based publish/subscribe system, referred to as DPS (Dynamic Publish/Subscribe).DPS graciously adapts to failures and changes within the system whereas achieving ascendancy events delivery. DPS includes a spread of fault-tolerant settled and probabilistic content-based publication/ subscription schemes. These schemes area unit targeted toward measurability, and aim at reducing and distributing the amount of messages changed [2].

2.1 Encryption Decryption

Plaintext this is what you want to encrypt. That is text or message that user want to send securely. Cipher text the encrypted output. By applying some encryption method message is encrypted , original message is hide by some other text. Enciphering or encryption the process by which plaintext is converted into cipher text. The method by message is encrypted is called encryption technique or encryption algorithm. Decryption is nothing but converting encrypted text into original plain text[9].Secret key a secret key is used to set some or all of the various parameters used by the encryption algorithm. The important thing to note is that, in classical cryptography, the same secret key is used for encryption and decryption. In classical cryptography, the various parameters used by a decryption algorithm are derived from the same secret key that was used in the encryption algorithm[9].

3. Identity Based Encryption

3.1 Algorithm

In 1984 Shamir asked for a public key encryption scheme in which the public key can be an arbitrary string. In such a scheme there are four algorithms[17]: (1)setup generates global system parameters and a master-key, (2) extract uses the master key to generate the private key corresponding to an arbitrary public key string ID 0,1 (3) encrypt encrypts messages using the public key ID, and (4) decrypt decrypts messages using the corresponding private key. Shamir's original motivation for identity-based encryption was to simplify certificate management in e-mail systems. When Alice sends mail at bob@hotmail.com, she simply encrypts her message using the public key string bob@hotmail.com. There is no need for Alice to obtain Bobs public key certificate. When Bob receives the encrypted mail he contacts a third party, which we call the Private Key Generator(PKG).Bob authenticates himself to the PKG in the same way he would authenticate himself to a CA and obtains his private key from the PKG. Bob can then read his e-mail. Note that unlike the existing secure e-mail infrastructure, Alice can send encrypted mail to Bob even if Bob has not yet setup his public key certificate. Also note that key escrow is inherent in identity-based e-mail systems: the PKG knows Bobs private key [17].

3.2 Approach Overview

Publisher Subscribers provide credentials to the key server and in turn receive keys which fit the expressed capabilities in the credentials. Subsequently, those keys can be used to encrypt, decrypt, and sign relevant messages in the content based publisher subscriber system, i.e., the credential becomes authorized by the key server. A credential consists of two parts:
1) A binary string which describes the capability of a peer in publishing and receiving events.
2) A proof of its identity.

4. Techniques For Authentication

To days authentication methods can be classified as follows:
1) Token based authentication
2) Biometric based authentication
3) Knowledge based authentication

Token based techniques, such as key cards, bank cards and smart cards are widely used[12]. Many token based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used with a PIN number.

Biometric based authentication techniques, such as fingerprints, iris scan and facial recognition are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security[12].

Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture based techniques can be further sub divided into two categories: recognition-based and recall based graphical techniques.

4.1 Techniques for OTP Generation

One time password can be generated in any of the two ways:
1) Time-synchronized OTP: In time-synchronized OTPs the user should enter the password within a certain period of time else it gets expired and another OTP must be generated.
2) A counter-synchronized OTP: With counter synchronized OTPs, a counter is synchronized between the client device and the server. The device counter is advanced each time an OTP is requested. For example, consider hash-based OTPs where in we use hash algorithms such as SHA-1 and MD5 that can be used to compute the OTP. A cryptographic hash function also called one-way function maps message of arbitrary length to a fixed-length digest. Thus, a hash-based OTP starts with the input parameters (synchronization value, user name, password), runs them through the cryptographic hash function, and produces the fixed-length password, i.e. OTP[12].

4.2 Modes of OTP Delivery

- Text messaging: It is the common method used for the delivery of OTP.
- Instant Message Services and Email: These services are almost common and the cost of using them is negligible[12].

5. System Architecture

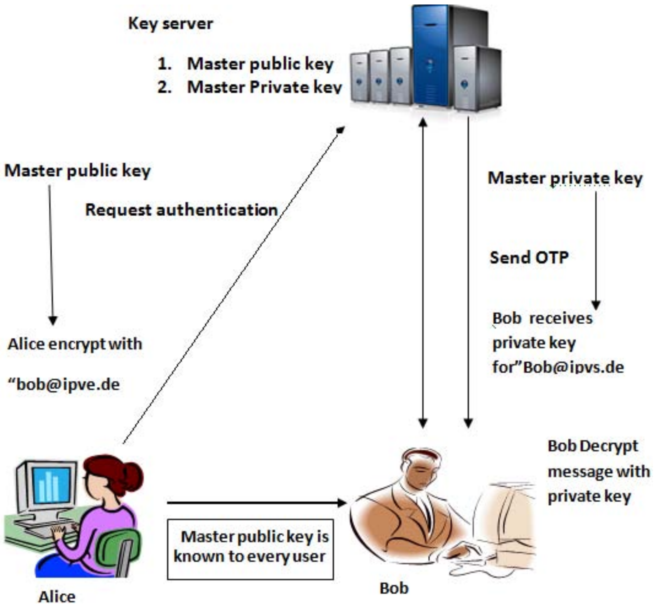


Figure 1: System Architecture

5.1 Important Modules in System

5.1.1 Content Based Publish-Subscribe System

The routing of events from publishers to the relevant subscribers. Content-based data model is used. Consider publisher subscriber in a setting where there exists no dedicated broker infrastructure. Publishers and subscribers contribute as peers to the maintenance of a self-organizing overlay structure[4]. To authenticate publishers, we use the concept of advertisements in which a publisher announces beforehand the set of events which it intends to publish.

5.1.2 Identity Based Encryption Module

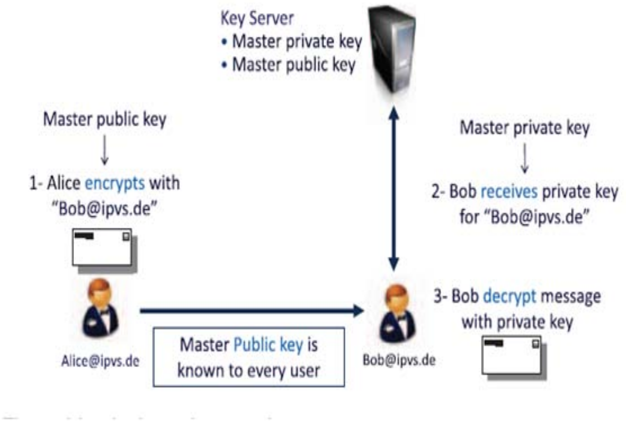


Figure 2: Identity Based Encryption

The IBE algorithm consists of four operations:

1. Setup, which initializes a key server
2. Encrypt, which encrypts a message for a given user
3. Key Generation, which generates a private key for a given user
4. Decrypt, which given a private key, decrypts a message

5.1.3 Key Generation

Publisher keys, before starting to publish events, a publisher contacts the key server along with the credentials for each attribute in its advertisement. If the publisher is allowed to publish events according to its credentials, the key server will generate separate private keys for each credential[20]. The public key of a publisher for credential is generated. Subscriber keys: Similarly, to receive events matching its subscription, a subscriber should contact the key server and receive the private keys for the credentials associated with each attribute A.

5.1.4 OTP(One Time Password)

Access controls exist to prevent unauthorized access. Companies should ensure that unauthorized access is not allowed and also authorized users cannot make unnecessary modifications[12]. The controls exist in a variety of forms, from Identification Badges and passwords to access authentication protocols and security measures. There are mainly two types of password

1. Static password
2. Dynamic Password

Static password is the traditional password which is usually changed only when it is necessary: it is changed when the user has to reset the password, i.e., either the user has forgotten the password or the password has expired. Static passwords are highly susceptible to cracking, because passwords used will get cached on the hard drives[12]. To solve this One Time Password Token’s are used. Unlike a static password, dynamic password is a password which changes every time the user logs in. An OTP is a set of characters or numbers that can act as a form identity for one time only. Once the password is used, it is no longer used for any further authentication. Even if the attacker gets the password, it is most likely that it was already used once, as it was being transmitted, thus useless to the attacker. This reduces the vulnerability of the hacker sniffing network traffic, retrieving a password, and to successfully authenticate as an authorized user. This password is used only for that session and when the user logins next time, another password is generated dynamically [12].A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keying fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows.

5. Result Analysis

Following table shows result of Existing System and Our System values.

Table 1: Margin specifications

	OUR System			
	Encryption	*Decryption*	*OTP*	*Verification*
Throughput in (B/S)	10	15	159	52
CPU utilization(ms)	0.192	0.1372	0.202	0.0000399
Computation Time for publisher and subscriber in (ms)	2.075	3.16	2.95	0.0198
	Existing System			
	Encryption	*Decryption*	*Sign*	*Verification*
Throughput in B/S)	8	12	150	46
CPU utilization(ms)	0.19	0.095	0.1536	0.0000099
Computation Time for publisher and subscriber in (ms)	2.54	3.02	9.014	0.0174

In existing system signcryption technique is used for the authentication and now in our system we used OTP(One Time Password).

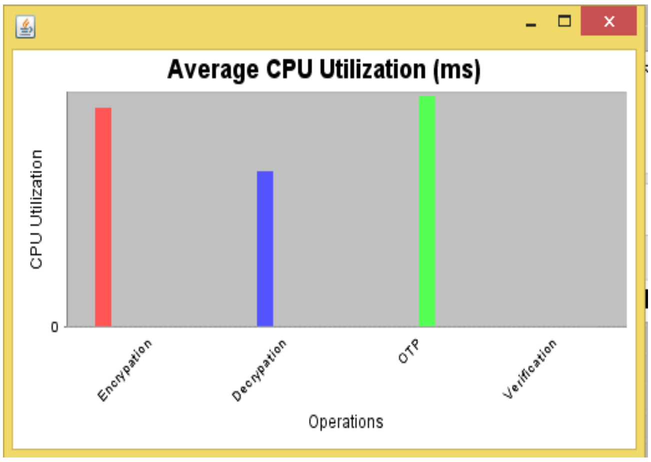


Figure 3: Average CPU Utilization in (ms)

Above chart shows Average CPU utilization in (ms).By considering time parameters for the operations like encryption, decryption and for OTP ,verification.

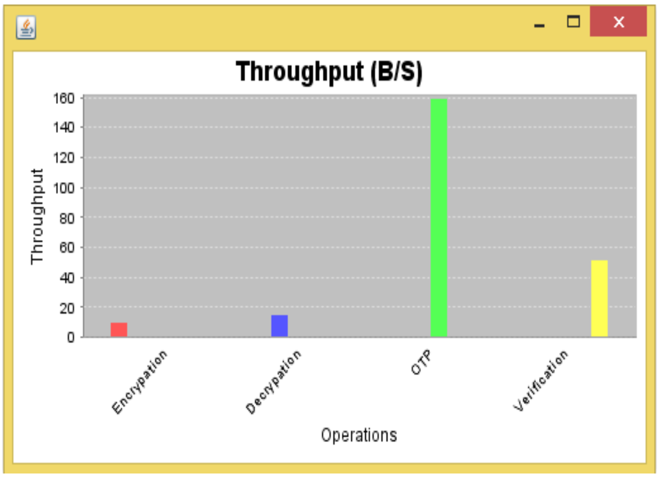


Figure 4: Throughput of system in (B/S)

Above result chart shows throughput of system in bits per second.

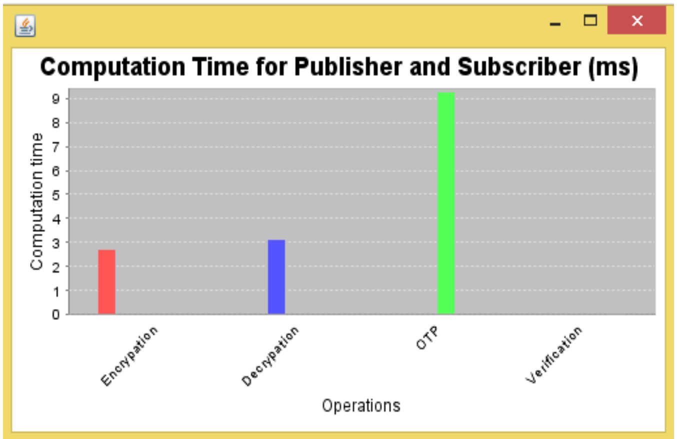


Figure 5: computation time in (ms)

Above result chart shows computation time required for the publisher and subscriber. Bellow result chart shows the comparison between existing system and our system.

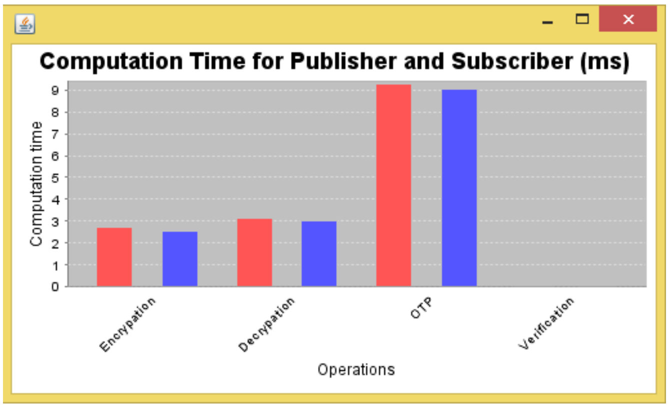


Figure 6: Computation time Required (ms)

Bellow result chart shows comparison for both the system for average CPU utilization in(ms)

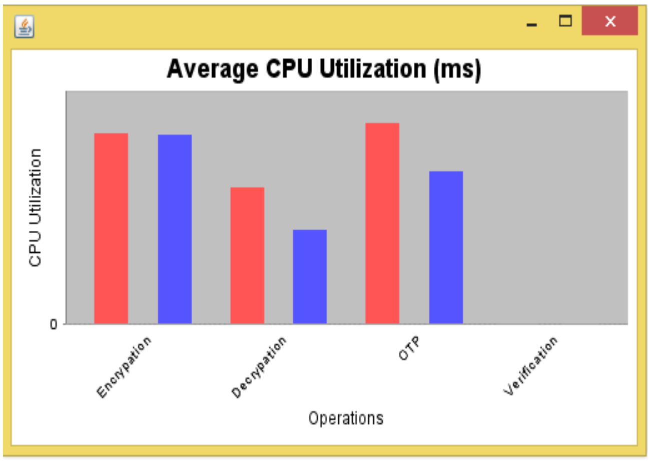
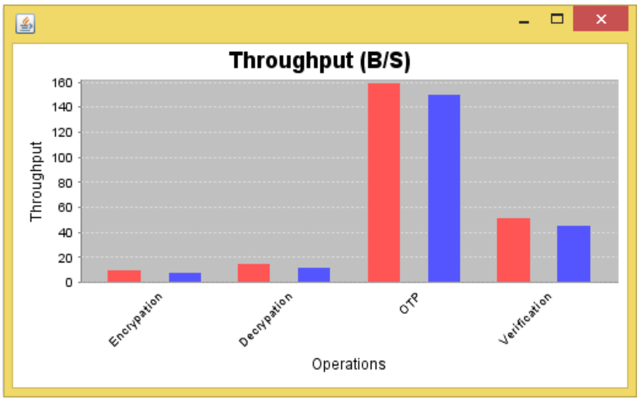


Figure 7: Computation time Required(ms)



References

[1] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel, “Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption”, *IEEE Transactions On Parallel And Distributed Systems,Vol. 25, No. 2, February 2014*

[2] 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 Intl Conf. Distributed Computing Systems (ICDCS), 2006*

[3] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption”, *Proc. IEEE Symp. Security and Privacy, 2007.*

[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] J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch, “Access Control in Publish/Subscribe Systems”, *Proc. Second ACM Intl Conf. Distributed Event-Based Systems (DEBS), 2008.*

[6] A. Shikfa, M. O nen, and R. Molva, “Privacy-Preserving Content-Based Publish/Subscribe Networks”, *Proc. Emerging Challenges for Security, Privacy and Trust, 2009.*

[7] 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*

[8] Ahmet Burak and Bharat Bhargava, “SORT: A Self-Organizing Trust Model for Peer-to-Peer Systems”, *IEEE transactions on dependable and secure computing,vol. 10, no1, january/february 2013.*

[9] William Stallings, Fifth Edition ”CRYPTOGRAPHY AND NETWORK SECURITY Principles and Practice”

[10] David Tam, Reza Azimi, and Hans-Arno Jacobsen, “Building Content-Based Publish/Subscribe Systems with Distributed Hash Tables”

[11] Shou-Chih Lo, Regular member and Yi-Ting Chiu, ” Design of ContentBased Publish/Subscribe Systems over Structured Overlay Networks ”.*IEICE TRANS. INF. SYST., VOL. E85-A/B/C/D, No. 1 JANUARY 2000*

[12] Himika Parmar, Nancy Nainan and Sumaiya Thaseen,” GENERATION OF SECURE ONE-TIME PASSWORD BASED ON IMAGE AUTHENTICATION ”

[13] Vishal M. Shah,Viral V. Kapadia,” A Review on Modern Methods of Encryption: Tendencies and Challenges,” *Volume 4, Issue 9, September 2014 ISSN: 2277 128X.*

[14] Dan Boneh Matthew Frankliny,” Identity-Based Encryption from the Weil Pairing”,*Appears in SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.*

[15] Pengqi Cheng, Yan Gu, Zihong Lv, Jianfei Wang, Wenlei Zhu, Zhen Chen,Jiwei Huang” A Performance Analysis of Identity-Based Encryption Schemes”

[16] Emmanuelle Anceaume, Ajoy K. Dattaz Maria Gradinariu,Gwendal Simony ” Publish Subscribe Scheme for Mobile Networks”*POMC02, October 30-31,2002, Toulouse, France. Copyright 2002 ACM 1-58113-511-4/02/0010*

[17] Joonsang Baek Jan Newmarch, Reihaneh Safavi-Naini, and Willy Susilo,” A Survey of Identity-Based Cryptography”

[18] Xuhua Ding and Gene Tsudik,”Simple Identity-Based Cryptography with Mediated RSA”.

[19] Divya Nalla, K.C.Reddy,” Signcryption scheme for Identity-based Cryptosystems”.

[20] Dmitrij Lagutin, Kari Visala, Andras Zahemszky,Trevor Burbridge,Giannis F. Marias”Roles and Security in a Publish/Subscribe Network Architecture”.*978-1-4244-7755-/5/10 2010 IEEE.*