International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 01, January 2016
www.ijirse.com
ISSN: 2454-9665

ANALYSIS OF SECURITY ISSUES IN PUBLISH/SUBSCRIBER SYSTEMS

Velivemula Nasaramma[1], J A Paulson[2]

[1]M.Tech (CSE), [2]Professor (CSE), Nalanda Institute Of Engineering& Technology (NIET), Kantepudi(V),Sattenpalli (M),Guntur(D, Andhra Pradesh (India)

ABSTRACT

Now a day's so many content based publisher/subscriber systems are available. But all these are in static format. Not possible to change network topology dynamically. In existing publisher/subscribers there is no access control mechanism. Unknown subscribers also possibility to download files security problems is in existing publisher/subscriber systems. In our proposed implementation overcome the drawbacks of existing publisher/subscribers systems. Provide bandwidth allocation for each subscriber based on payment of amount. After file downloading automatically reduce the bandwidth if bandwidth is insufficient send alert messages to subscribers. This implemented system is a distributed system in this publisher uploaded files are stored in drop box cloud server and subscribers download from files. By using identity based encryption mechanism provide more security for data in cloud server. Publisher identifies the hackers details based on token id. After registration of subscriber generate token id and send mail to subscriber. After login for accessing of services enter token id if it is invalid subscriber is identified as hacker. Publisher verify hackers details

I. INTRODUCTION

The publish/subscribe (pub/sub) system is effectively used in network applications. By using publisher/subscriber systems sharing the information to subscribers and broadcast the message to subscribers at a time. Publisher/subscribers communication system effectively used in cloud computing environment. In this publisher/subscriber system publisher upload the files and broadcast files to subscribers based on network. So all subscribers in a network receive files from subscribers at a time. Time is saved and within short time forward message or files to all subscribers. Subscribers are no need to wait for receiving files from publisher/admin in a network topology.

In this paper publisher/subscriber system is a content based system. Publisher upload different types of files and by using cryptography provide security for data in server. Publisher uploaded files all are stored in real time cloud server Drop Box cloud. All uploaded files are stored in this drop box cloud server if subscriber want to download files send request to publisher/admin. Based on amount payment of subscriber and allocation of bandwidth subscriber download files from cloud server. In publisher/subscriber system important functionality access control of subscribers in a system. In this publisher/subscriber system actually in present systems there is no particular access control in subscribers. At a time messages or files forward to all users in a network but some subscribers don't want documents but documents send to all subscribers. There is no accessing control mechanism in publisher/subscriber system. So finally providing the particular access control for all subscribers in a system. It is very important and security purpose this is very useful in implemented publisher/subscribers

content based systems. There is no access control mechanism all subscribers download the files from server in unauthorized manner.

The study of cloud computing storage of data and provide security for data is very important. Cloud computing is refers to maintaining of computer applications over the internet. The cloud computing applications are implemented based on internet and data is stored in cloud server. But in now a days all cloud computing applications so many data privacy problems are raised. So many data privacy issues are in cloud computing. The data privacy issues are occurred in group shared data applications in cloud computing environment. In group data sharing applications different virtual machines are assigned to different clients and all clients are connected to single physical machine. In this scenario providing confidentiality and privacy to shared data in different customers. In this applications using cryptographic techniques to provide security for data. In cloud computing data sharing functionality is very important. Data owners upload data in cloud server. In normal existing systems directly store original data but third party hackers hack the data and modify the data eaves droppers and tampering attacks are very high in cloud applications. So that's why in present cloud data share applications using encryption and decryption techniques provide security for data. Data owners upload data in cloud server before uploading the data is encrypted by using any cryptographic algorithm and stored in cloud server. If customers want to download data in that data owners share private key to particular customers. Based on private key customers decrypt the data and download original readable format of data from cloud server.

II. ARCHITECTURE

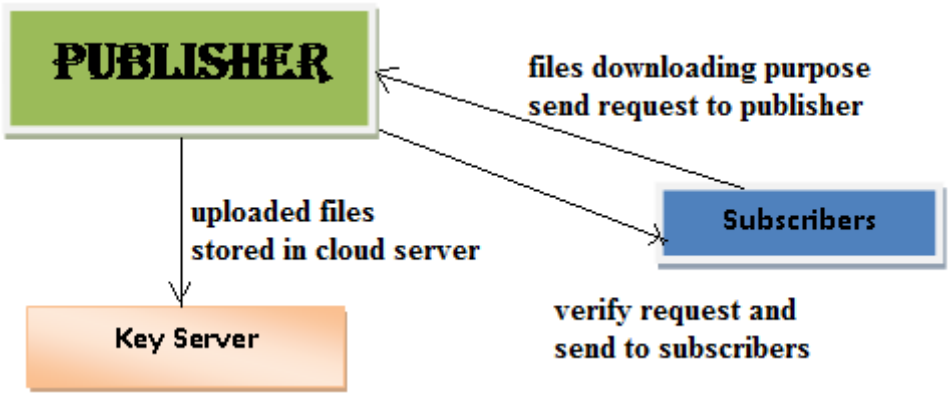

Fig 1.0: Architecture Diagram

In present system using symmetric cryptographic techniques to encrypt and decrypt the data by using single key. But it is not provide more security for data. Then compared to symmetric techniques asymmetric techniques provide more security by using different keys and encrypt and decrypt the data. So in this paper discuss about how to implement new cryptographic technique to provide more security for data cloud server. Encryption is one by one key and decryption is done by another different secret key in cryptography.

But in now a days all cloud computing applications so many data privacy problems are raised. So many data privacy issues are in cloud computing. These data privacy issues are overcome by provide authentication for users and server. If any unexpected privileges to users it occurs some data loss problems. These data privacy issues are occurred in group shared data applications in cloud computing environment. In group data sharing applications different virtual machines are assigned to different clients and all clients are connected to single

ISSN: 2454-9665

physical machine. In this scenario providing confidentiality and privacy to shared data in different customers. In this applications using cryptographic techniques to provide security for data.

III. A SEMANTIC OVERLAY FOR SELF-PEER-TO-PEER PUBLISH/SUBSCRIBE

In this publisher/subscriber system it is a static representation. In this type of publisher/subscriber system by default network topology is created. In this this network topology subscribers are ON/OFF position in static representation. If once create a network topology in publisher/subscriber system not possible to change the subscribers status at runtime. Statically all subscribers are configured if any subscribers in OFF position data is not forward to that subscribers and if publisher want to change the subscriber status at runtime but this is not possible in self peer to peer publisher/subscriber system. In this system there is no third party functionality but there is no particular security for data and there are no access control mechanisms for subscribers in a system. So finally next introduce the dynamic publisher/subscriber system implementation.

IV. ACCESS CONTROL IN PUBLISH/SUBSCRIBE SYSTEMS

In this access control publisher/subscriber system publisher providing the secured access policies to and privileges to subscribers in a system but there is no identity verification of subscribers in a system.

In this publisher/subscriber system publisher change the subscriber status dynamically and send data to all subscribers in a network. This is main drawback in this system. Some subscribers pay more amount and some subscribers pay less amount. Based on payment of amount of subscribers allocated bandwidth to subscribers and after downloading every time deduct the bandwidth of particular subscribers. But in this system there is no bandwidth allocation mechanism and there is no identity security for subscribers in a system.The traditional use of cryptosystems is original form of message is called plain text and mangled information is nothing but cipher text. The procedure to convert plain text to cipher text is called encryption technique. The reverse of encryption procedure is called decryption in that cipher format of data is converted to original format.

V. IMPLEMENTATION OF PUBLIC KEY CRYPTOGRAPHY SYSTEM

This system described as asymmetric cryptography it is introduced in 1975. In this each individual use has two keys private key it is no need to share to others. Public key it is shared to sender/publisher and receiver/subscriber in system. In this public key crypto system using mathematical functions that are inverse of each others.In advance of public key cryptography new concept is digital signature. Digital signature is number associated with any data. This system first one data privacy by using encryption decryption technique to provide security for data.In this encryption side using public key and decryption side using private key of receiver.In this public key cryptosystems main purpose of this is verification of identity of users if valid users are not. In this two functions one is signing and second is verifying. In signing using private generate signature for users. In verifying side using public of user and verify the signature if it is valid or not. By using digital signature technique provide more privacy for identity of users.

International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 01, January 2016
www.ijirse.com
ISSN: 2454-9665

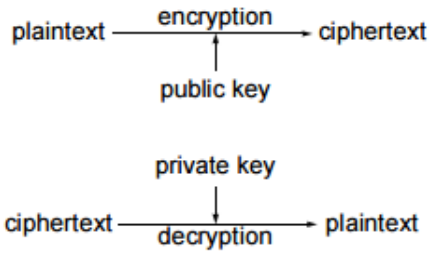

Fig 1.1: public key crypto systems

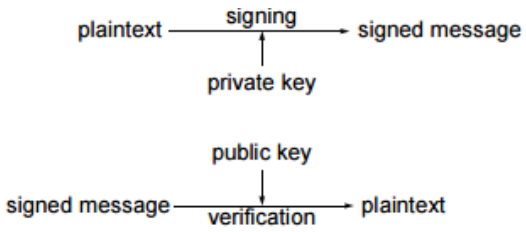

Fig 1.2: Digital Signature

VI. CRYPTOGRAPHIC KEYS FOR A PREDEFINED HIERARCHY

In this section discuss about cryptography assignments schemes. The main purpose of these schemes is to reduce storage and managing secret keys sizes in cryptography. In this using tree hierarchy of cryptographic schemes. Sandhuproposed method is tree hierarchy method. In this method parent key internally grants all descendant nodes. In this tree hierarchy generate pseudorandom function block cipher text with fixed size of keys in public key cryptography. In this tree hierarchy generate tree to graph by using two types of schemes like cyclic and acyclic graphs types.

These schemes are implemented based on symmetric key crypto systems. In this by using modular arithmetic functions to generate pseudorandom functions like public key cryptosystems but it is most expensive.In example tree structure format In this alice first classify the cipher classes according to subjects type. In this each node in tree shows the corresponding secret keys and leaf nodes shows the keys of cipher classes of individual nodes. Filled circles show the delegated keys and dotted lines shows the granted keys. In this every non leaf key is derived from descendant node. In this compact key is not possible every time for fixed hierarchy

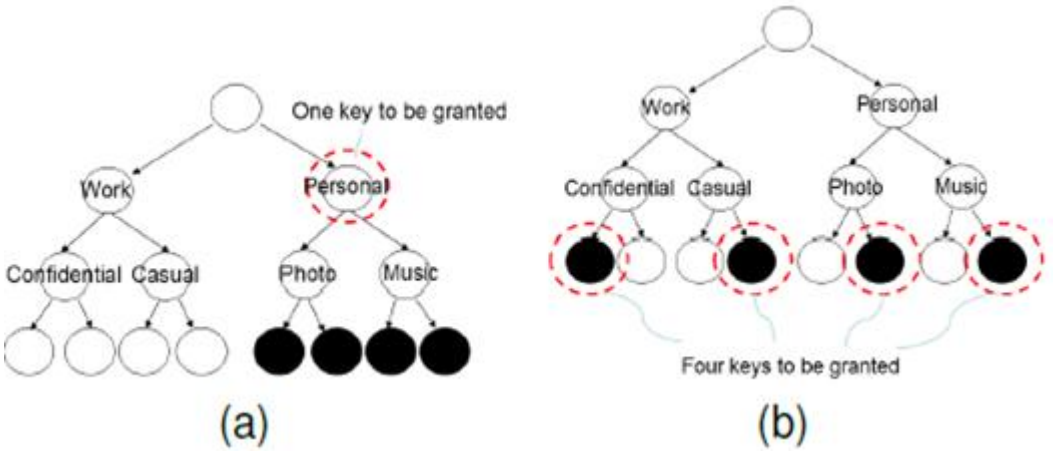

Fig 1.3: keys hirarchy

VII. COMPACT KEY IN SYMMETRIC-KEY ENCRYPTION

Benaloh et al. [8] introduces encryption scheme transmitting the large number of keys in broadcast format. In this the key construction is sub set of all cipher text classes.

1) In this first calculate N value N=p*q

ISSN: 2454-9665

2) Where p and q are large prime numbers.
3) Master key chosen generate a one random number Y
4) In this generate cipher text classes all these are in constant size
5) The key for classes are represented by e1, e2 and e3.
6) In encryption by using corresponding encryption keys to encrypt the data by using technique encryption data is time taking process. Calculations are high complexity format.
7) Finally some schemes are there to reduce key size and providing authentication. But in this present scheme does not discuss about sharing of decryption keys.

These are following properties of symmetric key encryption

Block size: symmetric encryption algorithm is working based on blocks of data

IV: Initialization vector used in encryption process. In this second block of data is encrypted with first block of data. There is no previous block to first block of data using initialization vector

Key: The key is automatically generated it is used in encryption and decryption. After encryption key is stored and same key used in decryption size also.

Key Size: The size of secret key in bits format. It is fixed length format in present system. It occupies more memory.

Padding: In this enumerate the values in padding mode.

VIII. COMPACT KEY IN IDENTITY-BASED ENCRYPTION

Identity based encryption is a part of public key crypto systems. In this public key of user is generated based on identity of user like email address or mobile number. In this truster third party is nothing but private key generator (PKG). In PKG holds master key and issue secrey key to users based on users identity. The encryption is done by public key and encrypts the message. The receiver decrypt the data based on private or secret key to decrypt the data. Guo et al. [23], [9] tried to build IBE using with aggregation of keys by using random oracle scheme [23]. In key aggregation all the keys must be aggregated and these are come from different identity divisions and polynomial numbers to be aggregated Most important thing is in key aggregation it is as an expense of O (n) sizes of both cipher texts and public parameters in n is number of secret keys to be aggregated with constant size. In this method the main drawback is increasing the cost of storing sizes and transmission of cipher texts.

ISSN: 2454-9665

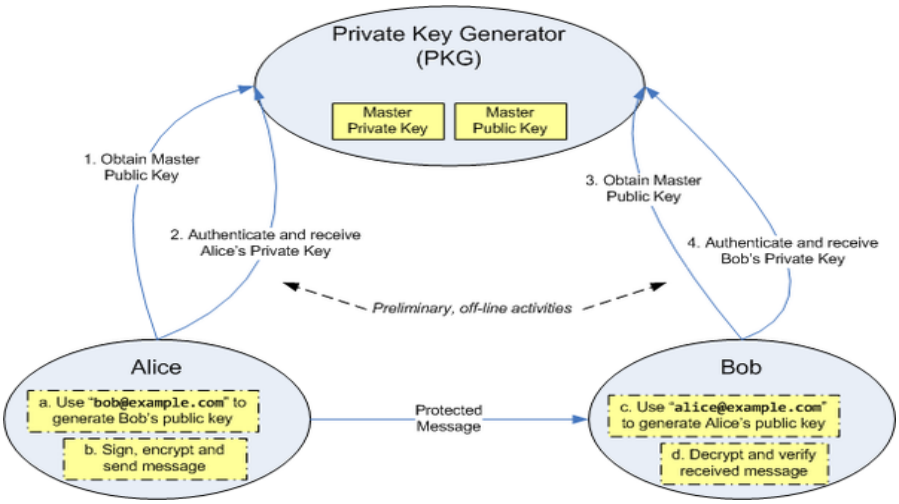

Fig 1.4: IBE Algorithm

8.1 Other Encryption Schemes

In Attribute-based encryption (ABE) [10], [24] algorithm cipher text generated based on attributes. The secret keys are extracted by master key holders and based on attributes policy provides access controls to users.

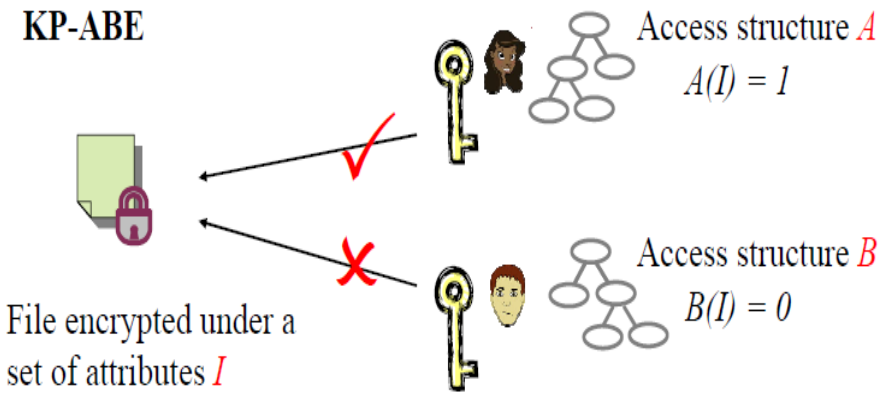

Fig 1.5: KP-ABE Encryption Algorithm

IX. CONCLUSION & FUTURE ENHANCEMENT

In this novel dynamic publisher/subscriber system implement the access controlof all subscribers in system and its provide more security them compared to existing systems. By using cryptography algorithm provide more security for data and implement identity verification procedure for each subscriber by using this approach if any hackers in system. Admin easily identify the hackers and block the attackers in system. Finally conclude that this dynamic content based publisher/subscriber system provide services effectively to all subscribers based on payment and allocation of bandwidth. Provide more security for subscribers and data in server. Subscribers download files from server in secured and efficient manner. In this present implemented system supports only for text files. This system future enhancement is publisher upload any type of files like audio, video and images, documents. Subscribers download the any type of files and provide more security for all types of files in system.

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 ComputingSystems (ICDCS), 2006.

[2]. J. Bacon, D.M. Eyers, J. Singh, and P.R. Pietzuch, "Access Controlin Publish/Subscribe Systems," Proc. Second ACM Int'l Conf.Distributed Event-Based Systems (DEBS), 2008.

[3]. W.C. Barker and E.B. Barker, "SP 800-67 Rev. 1. Recommendationfor the Triple Data Encryption Algorithm (TDEA) Block Cipher,"technical report, Nat'l Inst. of Standards & Technology, 2012.

[4]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute-Based Encryption," Proc. IEEE Symp.Security andPrivacy, 2007.

[5]. D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, "PublicKey Encryption with Keyword Search," Proc. Int'l Conf. Theory andApplications of Cryptographic Techniques on Advances in Cryptology(EUROCRYPT), 2004.

[6]. D. Boneh and M.K. Franklin, "Identity-Based Encryption from theWeil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology,2001.

[7]. S. Choi, G. Ghinita, and E. Bertino, "A Privacy-EnhancingContent-Based Publish/Subscribe System Using Scalar ProductPreserving Transformations," Proc. 21st Int'l Conf. Database andExpert Systems Applications: Part I, 2010.

[8]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proc. ACM 13th Conf. Computer and Comm. Security (CCS), 2006.

[9]. M. Ion, G. Russello, and B. Crispo, "Supporting Publication andSubscription Confidentiality in Pub/Sub Networks," Proc. SixthInt'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm),2010.

[10]. 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 DistributedEvent-Based Systems. IGI Global, 2010.

[11]. M. Jelasity, A. Montresor, G.P. Jesi, and S. Voulgaris, "PeerSim: APeer-to-Peer Simulator," http://peersim.sourceforge.net/, 2013.

AUTHOR DETAILS

	**VelivemulaNasaramma**pursuing M.Tech (CSE) from Nalanda Institute Of Engineering & Technology(NIET), Kantepudi(V), Sattenpalli(M), Guntur(D)-522438, Andhra Pradesh.
	**J A Paulson** working as Professor (CSE) fromNalanda Institute Of Engineering& Technology(NIET), Kantepudi(V), Sattenpalli(M), Guntur(D)-522438, Andhra Pradesh.