A Study on Methodologies for Solving the Problem of Maintaining Confidentiality in a Publish/Subscribe Network

A.Mahalakshmi[1] Dr.D.C.Joy Winnie Wise[2] V.Perathu Selvi[3]
[1]P.G Student [2]Professor & Head [3]Assistant Professor
[1,2,3]Department of Computer Science & Engineering
[1,2,3]Francis Xavier Engineering College

Abstract— In today's modern world, the storing and sharing of information plays a vital role. The information can be either important or unimportant but they are meant to be shared for some purpose. They can be shared in many ways, but publish subscribe method is one which is becoming more popular nowadays. A wide range of people started using this method for sharing their information with others. However, some metrics such as authentication, confidentiality of information are need to be considered as they are the most important problems of a data sharing environment. This problem can be solved using some cryptographic encryption techniques. The two important categories of encryption are symmetric key encryption and asymmetric key encryption. They can be used to secure the information by converting it into some other unreadable format.

Key words: Symmetric key encryption algorithm, Content based filtering, cryptographic encryption techniques

I. INTRODUCTION

In our daily life, the number of technologies used in various fields are increasing at a faster rate. Various computing technology allows many people to share their data easily with others. The information which has been shared among us can be a photograph, a word document etc. The sharing of information can take place in various ways. The major ways in which sharing take place are

- Internet,
- Social network,
- Mobile phones,
- Bluetooth etc.

` Such kind of information sharing system plays a significant role in today's life. There are many advantages in using these technologies, but at the same time, the concern about security of the shared information also increases automatically.

Intrusion by unknown person during the data sharing process is one of the most important thing to be considered. There are chances for the data to be accessed improperly by any outsiders. Hence there should be some sort of security mechanisms need to be implemented on the system, mainly in order to improve the security.

Following are the main reasons for enforcing security

- Increasing online transaction
- Sharing of individual's personal and confidential information over the network.

One of the most important tool for enforcing security is encryption. Enforcing encryption implies that the particular message cannot be viewed by others. The original data will be converted into a different format. There are various algorithms available for implementing encryption.

The Publish/subscribe system can be defined as the one, which is mainly used for the purpose of sharing the information with other people. It provides a flexible way for exchanging data between the publishers and the subscribers. This system has emerged recently and also gained more popularity among people. In addition, it is also an important and efficient method for implementing the distributed applications. The main reason for the popularity of this system is the subscriber can subscribe an information even without the knowledge of publisher. The communication which is taking place in this Publish/Subscribe system is asynchronous [4]. Publishers of events do not need to know the set of subscribers who are accessing their information. This makes the communication to be asynchronous. The main advantage of using publish subscribe model is that the communicating parties can be decoupled from each other. An important challenge faced by this model is protecting the confidentiality of the information.

Filtering refers to the process of selecting messages. There are two types of filtering available. They are

- Content based filtering
- Topic based filtering

In content based filtering, subscribers will be able to access information only if the constraints defined by them match the attributes or contents of information.

In topic based filtering, subscribers access the information according to a keyword or a topic. This type of filtering is easier when comparing to the content based method because the later one is difficult to implement.

II. RELATED WORKS

The existing method is a content based publish subscribe method. In addition, to improve the confidentiality, the approach uses identity based encryption algorithm [1]. In a content based system, the messages will be provided only when the content of the data matches the constraints defined by the subscribers.

The same Identity based encryption algorithm has been used in [2]. But in this approach, the private keys of users are issued by a trusted third party called private key generator.

In [3], for a content based publish subscribe, a design principle is presented. This system is called as Dynamic Publish/Subscribe. In Dynamic Publish/Subscribe system, two subscribers are considered to be similar whenever a subscription with common attributes is shared among them. Then, the similar subscriber will be connected to form a same group. These groups of subscribers will self-configure in order to form tree structures such that for each attribute a single tree is built. Here DHT-based overlay need not be mapped. In this approach all types of attributes and constraints are supported directly.

In [4] CP-ABE has been used where, some set of attributes will be associated with a user's secret key and the

access policies for the attributes will be associated with ciphertext. In this method, a user will be able to decrypt the ciphertext only if the attributes associated with the user's secret key satisfies the access policy associated with the ciphertext.

In [5] systems with small cryptographic private and public keys are created. The two important features that are related to this system is the size of public and private key size respectively. First, public keys is used to create a ciphertext that eliminates an unbounded number of users, and the public key is small. Second, on the receiving devices, there should only be small number of key materials for cryptography available.

III. PROPOSED WORK

A. *Alphanumeric ASCII Character Encryption:*

The publish/subscribe system can be either content based or topic based. The existing approach used content based, but the proposed method uses topic based. It is very much essential that the information being exchanged must be kept confidential in data sharing process. The confidentiality can be achieved by using some encryption technique.

Encryption refers to the process of converting the original information into some other format, such that the encrypted information cannot be easily read by any outsiders.

The original message is called the plaintext and the converted message is called the ciphertext. This technique is widely used in order to prevent the data. Cryptography is one important technique for enforcing security.

There are two different types of encryption algorithms available nowadays. They are given as

- Symmetric key encryption algorithm
- Asymmetric key encryption algorithm

In symmetric key algorithm the same key will be used by the publisher and subscriber for the encryption and decryption of information. In asymmetric key algorithm different keys will be used by publisher and subscriber for the encryption and decryption process. The proposed system uses symmetric key encryption algorithm. Individual identity information refers to the information provided by users of the system to ensure their uniqueness. These values can be a string or numeric. Each user of the system must specify their individual identity information. They can give any number of values to specify their uniqueness.

In this system, the key for each publisher can be generated by concatenating the different individual identity information values specified by them and then convert the concatenated value character by character according to the ascii value conversions concept used in many programming languages such as C, C++, java. Then the resulting value would be the key value for that publisher. Then the keys which are generated using the individual identity information details will be used further for the encryption process.

In many systems there are always problems regarding the maintenance of keys which are generated. It is difficult to maintain all those keys. This problem mainly arises in many scenarios but most important ones are

1) When asymmetric key encryption algorithm used, since different keys will be used for encryption, decryption and it will be cumbersome to maintain all those keys.
2) When the number of users in the system increases.

These are also some situations which makes the management of the keys as a difficult process. Hence in order to make this process of key maintenance as an easy one, the number of generated keys must be less. This can be achieved by use of symmetric key encryption algorithm.

In this system each publisher will be provided with a key which they can use for encryption of information being published and this key remains the same, even when the number of publications by that publisher is more than one. A publisher may publish any number of information, but the same key will be used for any number of encryption by that publisher. This makes the Key management process as an easy and efficient one, so that it does not become a cumbersome process. In proposed system, initially the key value which has been generated using the Individual identity information value specified by each publisher is to be considered and then converted into a different data type (Ex: say to an integer type), then the each character of the information to be published will also be converted into an integer format, which will then be concatenated with the key value generated.

Finally, after all these conversions and concatenation have been completed, the value obtained from this process is again to be converted character by character into different format based on the ascii values and the resulting data will be the information published by a publisher in an encrypted format.

The Individual identity information value plays a vital role in this process. Since the proposed system is topic based, the encrypted information will not be provided to all the subscribers in the system, Instead it will be given only to some subscribers whose individual identity values matches with the topic Individual identity value of publisher. This makes the information being prevented from access by any other subscriber who is not supposed to access that information. Decryption is the reverse operation of encryption. Since the proposed system uses symmetric key encryption algorithm, the decryption can also be done with the help of same key.

In this approach, during the encryption process the key value which has been converted into an integer format will be added with the original information which has also been converted into an integer format, and then final value will be converted based on ascii value, while during decryption process the key value will be eliminated from the encoded message and the resulting data will be converted based on ascii values in order to get the original data.

IV. CONCLUSION

In this system, to enhance the confidentiality of information being published, a new technique namely alphanumeric ascii character encryption has been followed. As this method encodes information to be published character by character along with the already converted key value, the information will be kept more secured. In addition, this method has also made the process of managing the keys of publishers as an easy one and at the same time, the encoding mechanism has also made the confidentiality being improved. The efficiency can further be improved by classifying the

information into important and non-important, finally encrypt only important information.

REFERENCES

[1] Muhammad Adnan Tariq, Boris Koldehofe, Kurt Rothermel, "Securing brokerless publish/subscribe system using identity based encryption," IEEE Trans. Parallel and Distributed Systems vol. 25, No. 2, 2014.
[2] Alexandra Boldyreva, Vipul goyal, Virendra kumar, "Identity based encryption with efficient revocation," Proc. ACM 14th Conf. Computer and Comm. Security (CCS), 2008.
[3] 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 Computing Systems (ICDCS), 2006.
[4] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "Mediated Cipher text-Policy Attribute-Based Encryption and Its Application," 10th Int'l Workshop (WISA), 2009.
[5] Allison Lewko, Amit Sahai, and Brent Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, 2010.
[6] Udepal Singh, Upasna Garg, "An ASCII value based text data encryption System," IJSRP, vol. 3, Issue. 11, 2011.
[7] Akanksha Mathur,"A research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms," IJCSE, vol. 4 No.09, 2012.
[8] Mihaela Ion, Giovanni Russello, and Bruno Crispo, "Supporting publication and subscription confidentiality in pub/sub networks," Springer, vol. 50, pp. 272-279, 2010.
[9] Vineet Sukhraliya, Sumit Chaudhary, Sangeeta Solanki, "Encryption and Decryption Algorithm using ASCII values with substitution array Approach," IJARCCE, vol. 2, Issue. 8, 2013.

