International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

Effective Role of Block Chain Technology for E-Commerce: A Case Study in Pub/Sub

Nomaun Rathore[1], Shrikant[2]
[1]*M. Tech. Student, Department of CSE, Sharda University, Delhi, India*
[2]*Professor, Department of CSE, Sharda University, Greater Noida, India*

***Abstract*: The asynchronous communication is required in the systems that are distributed. This is achieved by various means like the use of middleware's in the system. These can be message queuing, or some message oriented middleware's, publisher subscriber services etc. mostly the publisher and the subscriber services are used by involving the publisher (the message sender) publishing and on the other hand the subscriber(receiver) who subscribes. But these kind of systems suffer from a lot of potential threats, like the man in the attack, compromisation of the message confidentiality, the authenticity of the message, even the anonymity of the other end user (subscriber). There are other issue as well that are to be addressed like of the middle man (like a broker) or the third party which may also be compromised. Various publication methods are applied to these services for overcoming the problems(faults). Various Encryption techniques are used, with various algorithms to solve various faults (symmetric and asymmetric algorithms, identity based schemes, key exchange schemes, hashing techniques). The blockchain technology which is a comparatively new technology can be effectively used for meeting the security requirements of pub/sub systems.**

***Keywords*: Blockchain, Cryptography, Publisher-Subscriber Services**

1. Introduction

The new networking technologies and the other products allow the connectivity across a vast area and among the large computers networks connected, other the applications as well, among the various users on the netwok. Such places require the provision of asynchronous communications in the distributed systems which operate in an autonomous(independent) fashion and these are coupled loosely i.e spread over a vast area, with requirement immunity of the operation in case of network failures. These necessities has been crammed by varied middleware product that area unit characterised as electronic messaging, message queuing, message adjusted middleware (MOM), publish-subscribe.

Applications act using the publish/subscribe scheme, where there are publishers (sending applications) which need to publish the messages with having no information of the other party , the receiver's(subscribers).In the same fashion, subscribers (the recipients) should be receiving the subscribed messages only, for which they have subscribed. This decoupling is achieved by an intermediary entity between the sending publisher and the receiving subscriber,(middleware's) which can serve as an indirection.

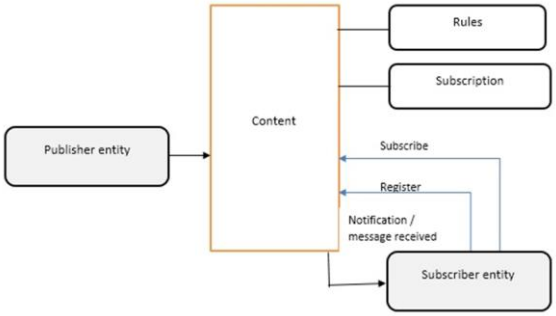

Fig. 1. Functionality of the pub-sub model

2. Theory in brief

A. *Publisher Subscriber services*

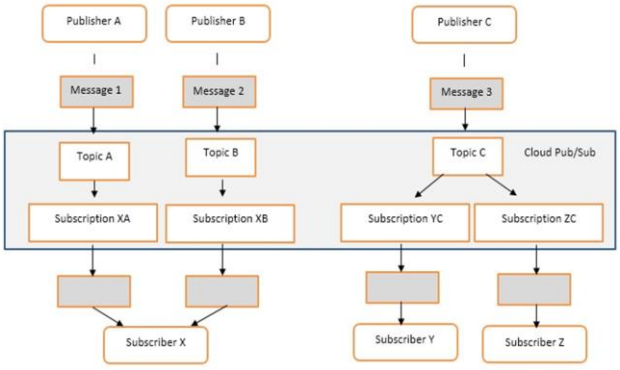

Fig. 2. Pub/Sub communication scenarios

There are various scenarios for the publisher and the subscriber services, like one publisher with multiple subscribers, many publishers with many subscribers.

There are various benefits as well as the disadvantages of these services

- Durability and low latency
- Globally connecting services anywhere in the world.
- Message delivery is guaranteed as the storage is replicated.

- Data on wire and rest is encrypted.
- The data flow control is dynamic.

Problems in the pub/sub services to be addressed: There are many problems also, which are faced in these type of services:

- Delivery should be guaranteed to the right person.
- The systems made should be fault tolerant otherwise during any system failure data may be lost.
- Authentication is another issue, i.e is the message being sent to the right person or someone else pretending to be the receiver.
- The anonymity of the user (subscriber) is another major issue to be handled.
- Other than these load surges, when multiple requests are made by multiple subscribers to various publishers, server failure can occur.

Various techniques have been implemented to overcome these problems, and to some extent they have over-come the issues, using cryptographic algorithms the encryption may provide help in confidentiality, the authentication problems etc. Now a new technology which is new to the system is being introduced, providing max security, and resolving almost all the issues in the system. This is the Blockchain technology. As this technology is new, it has various features of other techniques used before. Blockchain is the amalgamation of the three, i.e cryptography, the game theory statics and the computer science engineering.

The cryptography is a technique of encryption of the message into cipher text so that the third party cannot access or retrieve the information. On the other side decryption takes place which is the conversion of the cipher text to plain text again. Blockchain uses the cryptographic hash function, the game theory statistics is another part of blockchain ensuring the consensus of the blockchain or in other words it provides a stable state of the chain, and the third part is the computer science engineering which provides the peer-peer communication between two entities without the involvement of the third person.

B. Blockchain

The blockchain is a new technology on which recently work is being done. This technology consists of the three concepts put together, i.e cryptographic hash function is used, game theory statics which provide the consensus state of the chain, and thirdly the computer science engineering providing the per to peer communication. This technology has many applications and is still going on with development to newer strategies to be put into it so that these can be implemented further on in various fields. Conceptually a blockchain is a public distributed ledger storing records or any information required, having its timestamp, and in the encrypted format. It is a tamperproof technology as the hashing techniques used make it that way, there are block having their own hash and block headers, the next block in the chain consists of the hash of the previous block and so on upto the genesis block (first block).So the tampering will result in the chain fail as the hash won't match and it is infeasible to change the whole hashes of the blocks in the chain. So this technology can be used in various fields as well as in the publisher subscriber models as well.

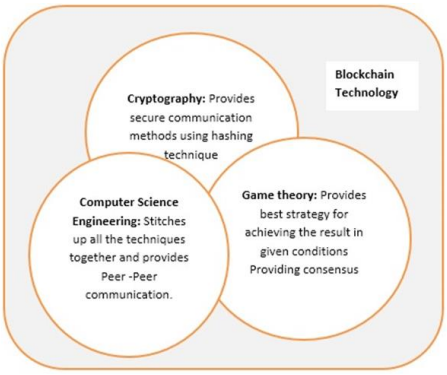

Fig. 3. Blockchain is amalgamation of three technologies into one.

3. Experiments

As the blockchain was first introduced in Bitcoins, an electronic cash system for the transfer of cash only in peer-peer network later on it was introduced for other uses also like the Ethereum blockchain. Studying blockchain technology reveals a lot can be introduced in the blockchain data structure and these can be applied in various applications like in the publisher subscriber services, securing cloud data , can be used in smart grid systems , ledger systems in various banks etc .and other fields where there are various security issues, because of its tamper proof nature and it can also be enhanced using new cryptographic techniques and game theory techniques. The cryptographic functions and schemes can be used with the blockchain (symmetric and asymmetric type, identity based schemes etc.) combined forming a model or architecture giving the necessary security features required.

4. Literature review

Various techniques and methods were proposed for the security of the publisher subscriber system. The literature review shows us that various techniques using cryptography etc. we're being used for the security of the publisher, subscriber system. Some of the survey done is as follows:

In a paper a technique is described in which the third party is eliminated and a fuzzy system is developed for the user identification. The fuzzy-logic, a unique technique, is used working on the setup, extraction and the encryption-decryption process. The fuzzy logic system has better results than the old traditional system (with broker) in providing the encryption and the decryption.[1]. Another paper describes a scheme proposed in which the middle party (third party, broker) is eliminated. Attribute based encryption mechanism is used for providing the security for the publishing based system. The ABE based scheme used here provides the encryption hence the security for the publisher/ subscriber system. The identity of the publishers

and the subscriber are hidden and the communication and transaction in b/w them are encrypted.[2]. As the real time pub-sub paradigm is important in the communication for the distributed network type in real time. The paper gives a new fault resistant duplex architect e is being described, and also the improvising of the time for key design decisions [3]. The blockchain technology is used for the various issues in the publisher subscriber systems. This is described The blockchain being tamperproof data structure, provides the confidentiality, anonymity, authenticity to the user. The old systems consisting of the third party involvement (which could cause the compromisation) is completely eliminated, moreover the new system provides various other security aspects required for the services making them more secure. Cryptographic hashing is used in blockchain and it provides the peer to peer communication with timestamp and other security features like the anonymity of the users etc. [4]. As all the schemes that have been proposed have been proven secure in the model used called the random oracle. The paper describes a new method without the random oracle model, which is an identity based sign-cryption method proposed. This proves the security of the simple standard model. The semantic security is proved in this paper under the Diffie-Hellman Decisional Bilinear hardness. [5]. As we know that the pub/sub model is loosely coupled, i.e the provision of security for such a model is a difficult task. Specifically, the provision of the confidentiality and the authentication. The IBE identity based encryption is also based on the cryptography pairing, the HIBE hierarchical based encryption is the generalized form of the identity based encryption .This provides an effective approach in resolving the security issues.[6]. The network architecture, the pub /sub architecture is used for providing the authorized distribution of data among the subscribers by the publishers. As the previous systems consists of the broker in between the publishers and the subscribers, a paper introduces a broker-less scheme for the network architecture. For more security the data shared between the publishers and the subscribers is in the encrypted format using an algorithm called ECC. The ECC uses the less size for the key for the encryption and the decryption process making this a computational easy and less memory used architecture [7]. The pub/sub approach is efficient in the sharing of the data and the receiving of the data on a large scale, so the amount of data shared and received is huge and requires economical and high storage source .A new technique is defined AKPS attribute-key-word based publisher subscriber scheme .for the protection of the attributes of the publisher , the attribute based encryption is used, and on the subscribers side , a new scheme is introduced for searching the data of their interest without the compromization of the publisher.[8]. The publisher subscriber services or paradigm has one to many, or many to many messaging types , where the group wants to receive the notification message or not . As the security based issues in the content-based publisher subscribers systems was addressed by other people in previously published papers, there is no correct definition of the necessary requirements for security of services and also there exists no particular scheme or model addressing all the security issues in the system. In this paper, the security model is defined for the content based publisher subscriber scheme [9]. The blockchain first introduced was implemented in the form of bitcoin, which had peer to peer communication eliminating the third party. The blockchain had the system for the storage of the transaction with the timestamp, encrypted using cryptographic hash function, on a distributed network. This is also called a distributed ledger. The bitcoin was the first blockchain for the cash transaction system [10]. The micro payments have a lot of potential applications. Micropayments means payments which are worth pennies. As the new distributed technologies are being adopted, the micropayments have become of use in various fields, as well these provide a cheap way for the transactions, which is in the interest of both the parties participating and are also easy to deploy. A new decentralized anonymous micropayments system DAM is introduced. This enables the parties to accomplish the transactions offline in private way also [11]. Publisher/Subscriber services provide a dynamic way of communication., one to many or, many to many on a network. The pub-sub systems which are based on content, are often used in the peer-peer infrastructure enabling the dissemination of the information from pub to sub mechanism.in the wide area network the scheme should handle information over different domains, raising the security issues. The paper defines the security issues in the wide area network(internet) for the publisher-subscriber systems.[12]. The blockchain has been studied and applied in various fields for the security and privacy reasons. A blockchain based punishment scheme is introduced, actions record for supressing attacks from the edge_servers and other devices in that particular network (mobile devices). There are various interactions which are between are the mobile devices which send the request to the server for obtaining of the service which is real-time or launching the attacks which are against the security gains of the illegal servers. Here the server chooses whether to perform an attack or an action, given from the device [13].

5. Results

As the publisher subscriber services are being used widely, there are security issues which are being solved using techniques with cryptographic functions and all. As blockchain is a new technology which is continuously evolving, newer techniques and methods are being implemented in it, so by providing the confidentiality, anonymity, authentication, and other security to the apps, this can be used further with other techniques for creating better and more secure systems.eg. the hashing techniques are evolving, so these can be applied to this technology, the new game theory statics are also being worked on which would make the technology more and more secure from the newer threats. So an enhanced blockchain system can be introduced to the previous systems with the symmetric and

asymmetric cryptographic models which will cover up all the security issues in the other systems moreover providing a better security module to be used in the pub-sub services.

6. Conclusion

The conclusion we can take from the above survey of the technologies used for the security and to solve the faults in the system (publisher subscriber system), blockchain technology can be implemented in these services with other techniques as well as modules making these services fault tolerant, tamperproof, helping providing the confidentiality, anonymity etc. for the users(subscribers). The blockchain technology can further be enhanced by using various other cryptographic algorithms and various techniques for making it more secure, thereby making the publisher subscriber-services safe.

References

[1] Maithily B, Swathi Y., "Securing Broker-less Publish/Subscribe System using Fuzzy Identity-Based Encryption". International Journal of Computer Science and Information Technologies, 2015, 6(3):2823-2826.
[2] Malpure V D, Deshmukh P K., "Provide security for broker-less content based publish system using pairing based cryptography". International Journal of Engineering Development and Research (IJEDR), 2016.vol.4 pp 1932-1938.
[3] Xiaoyan He, Lui Sha "A fault tolerant real-time publisher/subscriber inter-process communication architecture". Proceedings 6th International Conference on the Real-Time Computing Systems and its Applications. RTCSA'99 (Cat. No.PR00306), IEEE, 13-15 Dec. 1999.
[4] Yanqi Zhao, Yannan Li, Qilin Mu,Bo Yang, And Yong Yu,(January 29, 2018,),' "Secure Pub-Sub: Blockchain-Based Fair Payment With Reputation For Reliable Cyber Physical Systems."
[5] Yu Y, Yang B, Sun Y, et al., "Identity based signcryption scheme without random oracles". Computer Standards & Interfaces, 2009, 31(1): 56-62.
[6] Tariq M A, Koldehofe B, Altaweel A, et al., "Providing basic security mechanisms in broker-less publish/subscribe systems". In: Proceedings of the Fourth ACM International Conference on Distributed Event-Based Systems. ACM, 2010: 38-49.
[7] Shitole S, Gujar A D., "Securing broker-less publisher/subscriber systems using cryptographic technique". Computing Communication Control and automation (ICCUBEA), International Conference on. IEEE, 2016: 1-6.
[8] Yang K, Zhang K, Jia X, et al., "Privacy-preserving attribute keyword based data publish-subscribe service on cloud platforms". Information Sciences, 2017, 387: 116-131.
[9] Yuen T H, Susilo W, Mu Y., "Towards a cryptographic treatment of publish/subscribe systems". Journal of Computer Security, 2014, 22(1): 33-67.
[10] Nakamoto S., "Bitcoin: A peer-to-peer electronic cash system". 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf.
[11] Chiesa A, Green M, Liu J, et al., "Decentralized Anonymous Micropayments". in: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2017: 609- 642.
[12] Wang C, Carzaniga A, Evans D, et al., "Security issues and requirements for internet-scale publish-subscribe systems". System Sciences, 2002: 3940-3947.
[13] Dongjin Xu, Liang Xiao, Limin Sun, and Min Lei, "Game theoretic study on blockchain based secure edge networks", (2017), IEEE/CIC International Conference on Communications in China (ICCC).