ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse209932020.pdf
https://doi.org/10.30534/ijatcse/2020/209932020

Security exploration of MQTT protocol in Internet of Things

Bhanujyothi H C [1], Dr. Dayanand Lal [2], Vidya J [3] , Swasthika Jain T J [4]
[1-4]Assistant Professor, Department of CSE, GITAM School of Technology, Bengaluru, India,
[1]baradhya@gitam.edu, [2]dnarayan@gitam.edu, [3]vjyothip@gitam.edu, [4]sjain@gitam.edu

ABSTRACT

Internet of Things (IoT) connects sensing devices and physical object/things to the internet for the purpose of exchanging information. Things have become smarter than it was before. IoT enables user to communicate and control smart objects to rescue information that is essential. Massive quantities of data will be generated and exchanged which in turn help in making decisions. However, security and privacy is important while exchanging data from anywhere and at anytime. IoT application protocols based on middleware play a key role in order to facilitate two-way communication and remote control of the IoT devices. Message Queuing Telemetry Transport Protocol (MQTT) is widely used lightweight messaging protocol in IoT. This paper describes security analysis and issues in MQTT protocol by considering different attacking Scenarios.

Key words: Attack, Broker, MQTT, Security

1. INTRODUCTION

The world has experienced rapid technological advances from the last few years, the likes of which have already had a major impact on people's lives. The growth of technology-mobile phones, laptops, and PCs has helped increase interconnectivity across time and spatial dimensions. Modern technology has moved beyond merely developing human interactions and now facilities provides all people with links to things and things to each other in order to achieve a common goal[5]. Internet of Things over the Internet enables contact among objects over the Internet [3]. Internet of Things holds a crucial role in the development of smart cities, such as smart house, car park and transport. In the area of IoT, five of the most prominent protocols used as a communication protocol are Hypertext Transfer Protocol, Message Queuing Telemetry Transport Protocol, Advanced Message Queuing Protocol, Constrained Application Protocol and Extensible Messaging and Presence Protocol. While choosing protocol for the purpose of communication, some consideration can be considered such as: Energy efficiency, reliability, resource utilization and Durability. Reliability, advanced functionality, and the capacity to encrypt multicast communications are also highly
rated. The Message Queuing Telemetry Transport Protocol is the best protocol which includes all the considerations [10].

The growing numbers of hacking criminal incidents that compromise connected devices to initiate cyber threats imply the adverse effect of the threats to IoT security [7]. Legitimate users can access IoT devices in the IoT ecosystem remotely by providing them with access directly from the Internet, or by using brokers or middleware technology for messaging applications. Revealing connected devices to the network for message exchange and remote control creates a considerable security risk, as IoT devices have less robust protection mechanisms due to resource constraints [8]. Many other connected devices perform behind the encryption, and use bidirectional communication and remote control middleware or message brokers[9].To achieve this bidirectional communication between IoT devices, and between devices and the server/cloud, several protocols have been developed. The MQTT protocol has appeared as the commonly accepted protocol among these because of low overhead and energy usage. This protocol uses an Internet broker server to enhance the interchange between clients of typical IoT devices, smart phones, and computer messages. Therefore the security vulnerabilities in the MQTT protocol need to be established to secure the IoT system that is based on this protocol.

2. BACKGROUND WORK

2.1 Literature survey

Syed Naeem Firdous et.al.[1] has proposed the MQTT threat model and carried out the Denial of Service attack evaluation which focus IoT application protocols such as MQTT. The IoT world puts great focus on IoT implementations focused on MQTT. IoT environment needs to be given security. This model did experiments to measure the effect of DoS attacks on MQTT communication broker. The results gained give insight into the problem domain. The main drawback of this model is model work on DoS attack only so it won't affect other targeted attack on IoT devices and MQTT message broker.

Haripriya A. P et.al.[2] introduced the MQTT-based IoT framework which implement a lightweight, fuzzy logic-based intrusion detection scheme called Secure-MQTT. The framework developed provides a significant method to secure low-configuration devices. This model is designed to identify malicious activity while IoT devices communicate. This model uses the method of fuzzy rule interpolation to detect the

node's malicious behavior. This model will also protect limited-configuration devices against DoS attack. The model Secure-MQTT identifies the threats quite accurately while compared with existing mechanisms. This model is for detecting various attacks in the security of application layers, it can also be extended to determine anomalous attacks in all other layers of IoT systems.

Syaiful Andy et.al.[3] have addressed security concerns in the MQTT protocol. There are many communication protocols in IoT among those IoT developers use MQTT protocol due to its low bandwidth and limited memory utilization. Here they discussed several reasons why a lot of IoT systems do not enforce proper security framework. After that it also illustrates and investigates how easily various attack scenarios used to attack this protocol. Finally, after analyzing the weaknesses of this protocol, in particular in the MQTT protocol, they have improved security knowledge and then incorporate protection measures in our MQTT framework to prevent such an attack.

Hector Alaiz-Moreton et.al.[4] have developed classification models that can use the MQTT protocol to feed an IDS using a sample containing frames in an IoT device attack. In this paper, they have presented two types of methods for categorizing attacks, ensemble methods and deep learning models, specifically to obtain recurrent networks with quite good result. Machine learning techniques can be used to classify frames that may be assigned by IDS as either attack or normal. Here they selected models LSTM, GRU, and XGBoost for classification problem. These three models are important in network attacks when considering the time and sequencing. These three methods of classification are all highly efficient. Among these, the XGBoost model allows for maximum accuracy.

3. ATTACKS ON MQTT PROTOCOL

MQTT is generally used application layer protocol compared to all other protocols due to its simplicity and scalability. MQTT was designed for light-weight communications between constrained resource devices such as mobile phones and servers. Figure.1 shows general MQTT Protocol Publish-Subscribe model [6]. Publisher, subscriber, and broker are the basic components in this pattern for enabling connections among several IoT devices. This protocol follows the process of establishment of connections based on TCP. At first, the publisher system will send connection request to communicate with the broker, i.e. Link. The broker must give the acknowledgment, CONNACK, to the publisher device until the broker receives the submission. Upon receiving a response from the broker, the publisher machine sends or publishes the message regarding a specific topic to the broker, and eventually the receiver devices subscribe to the messages from the broker[19].

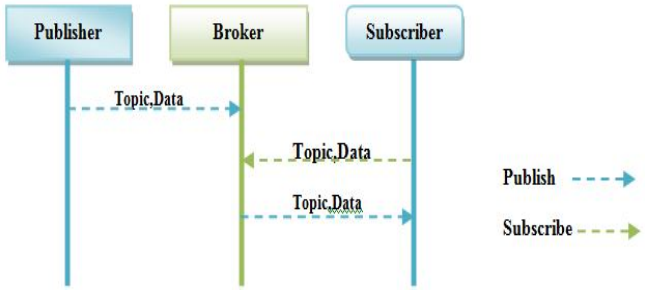

Figure 1: MQTT Protocol Publish-Subscribe model

The test environment contains several attacks against the MQTT protocol. Suspicious devices obtain network access while the messages are being published and subscribed, and prevent services provided by the broker. Through analyzing the published-subscribe messages, we can identify the attacks against the MQTT broker. Here, these attacks are at network level and all traffic generated there. The attacks which were carried out were:

A. Denial-of-service attack

Figure 2 shows the scenario for the DoS attack, the MQTT broker has to be scrutinized by obtaining the network traffic. An attacker can initiate a DoS attack in the broker by repeatedly sending multiple connection requests, thus making the broker as busy as in flooding. If multiple requests for connections reach simultaneously, then the buffer will be exhausted and the broker will not be able to manage all new requests coming in. The broker also cannot distinguish between the normal message packets and the hoax CONNECT message packets [16]. When the broker gets messages for flood requests, it starts to acknowledge with the message CONNACK. During DoS attack, the number of CONNECT and CONNACK packets grows rapidly which brings the broker service to halt and prohibits the operation of the intended IoT network.

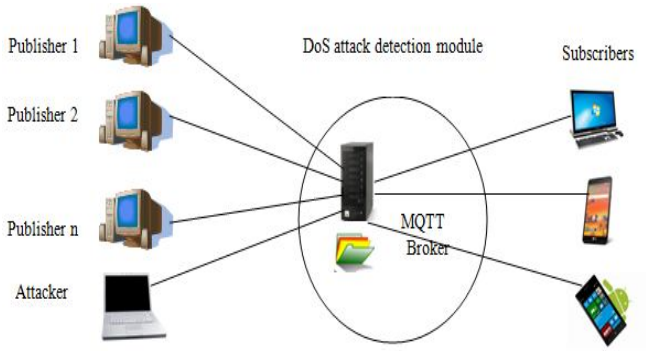

Figure 2: DoS attack scenario in MQTT

B. Man-in-the-middle attack

MitM interrupts the messages to communicate with various points to change the information; it is done by changing the sensor data between a broker and the sensor. Attack implementing tools are the Kali Linux distribution and the Ettercap tool.

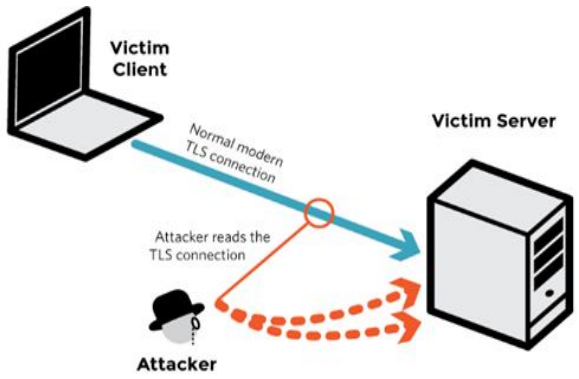

Figure 3: Man-in-the-middle attack in MQTT

Figure 3 shows MitM attack in MQTT protocol. MQTT was designed for light-weight communications between constrained resource devices such as mobile phones and servers. Although security was not designed into the protocol, it provides some security safeguards. This protocol enables a two-way hand shake by allowing client authentication. If SSL/TLS is available on the constrained resource devices then this mechanism allows for encryption of data in the message. When SSL/TLS is not available, the user name and password that authenticate the client are in the clear instances. This two-way handshake is vulnerable to man-in-the-middle attacks. Both mutual authentication and encryption are needed to avoid MitM attacks.

C. Intrusion

An intrusion into a network is an unauthorized activity on a computer network. Intrusion is observed in terms that the defenders understand clearly how the attack can work [4]. Such an unclaimed activity in certain cases uses network resources for many other uses and almost always affects the safety of the network and its data, or even both. Proper design and deployment of an IDS network (intrusion detection system) will help to block the intruders. Intrusion which takes the features of the MQTT protocol into account. This attack includes the use of the possibly the best-known port for this protocol and a command that uses the special character "#" is also used by an external attacker to know the active subjects that are available for subscription.

4. SECURITY ANALYSIS

4.1 Security Overview

An attack on various domains can cause damage to the user. MQTT provides various security mechanisms in that many of them are not configured as data encryption or authentication of the entities. During authentication mechanisms, the broker registers device information that includes physical device address (MAC) when the device attempts to connect with the broker. And broker can use Access Control List (ACL) to do access authorization. The ACL contains data such as the different clients' password and identifier which allows access to various objects and can also describe the client which function it needs to perform.

Confidentiality is an important requirement for a system of security. This can be done by encrypting message at the publisher side of the application layer. This type of encryption can be accomplished either as a broker model end to end, or as a client. Broker decrypts the information that comes from the publisher in client to broker form, and encrypts the information that is required to be forwarded to other side client. Broker cannot decrypt the relevant data from the publisher in the end-to - end type instead of forwarding cipher text directly to another device. In other methods broker does not requires any additional requirements for encrypt/decrypt messages except few computational resources and less energy.

4.2 Security Requirements

Data security is most important constraint to be considered to select protocol for IoT devices due to lack of data security mechanism in IoT communication protocol [3]. Data security is composed of three main parts: data confidentiality, data availability, and data integrity. It also includes additional security requirements such as authentication, authorization to allow access. There is no full security method in MQTT protocol; it only includes authentication methods without encoding capabilities [14].

IoT developer has to take some considerations to design solution for security in the IoT communication protocol while developing applications they are: 1) IoT device requires a lightweight security protocol because of limitations in IoT devices, 2) Each of connected IoT devices uses different protocol and different security mechanism in heterogeneous environment, 3) The reliability of network might force us to use minimum overhead in security mechanism. While considering the requirement for security we need to concentrate on attack surface in IoT. [15] The IoT attack surface is split into the Public and Local networks. The local network is called an internal attack; here the attacker and the IoT devices will be in the same network, while the public network is also called an external attack, where the attacker could be present to attack the IoT system anywhere in the public network.

4.3 Limitations of security mechanism in IoT

A. Resource Constrained Device

One of the key reasons why IoT systems do not use security mechanisms is resource constraint limitation. Numerous devices are classified as a restricted device based on RFC 7228[17], further splitting these devices into three classes depending on their RAM data size and ROM code size as shown in Figure 4.

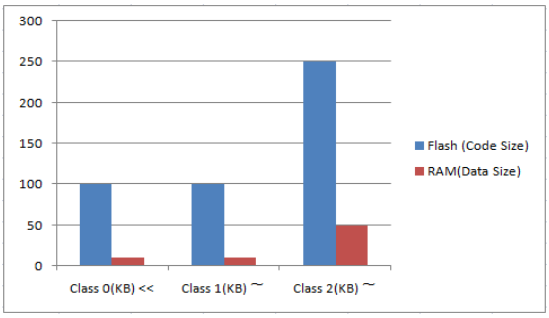

Figure 4: Classes in Constraint Device - RFC 7228

B. Lack of security awareness

IT and other organizations need to improve the awareness of IoT treats. Lack of knowledge on security leads to increase the challenges in security of connected devices also increases treat level, which keeps organization at risk. Few key capabilities are considered by IT and security decision makers to protect against security attacks in IoT.

C. Huge number of devices

In IoT a large number of devices are connected. Number of connected devices creates greater vulnerability. In the IT department, when IoT system is applied with security mechanism, it is necessary to manage a large number of different types of devices [18]. For example, if IT department gives authentication by using username and password then they have to put a lot of effort into maintaining credentials for security.

5. ATTACK SCENARIOS

Initially attacker had no idea about the prey system that they want to attack, like no idea about communication channel, infrastructure and defense mechanism [13]. Attack can be begins by collecting the related information by using Massca or Shodan search engine. This paper uses Shodan search engine to collect related information to attack on MQTT protocol. Attacker can use port number 1883 to search about MQTT protocol. Attacker has to type “port: 1883 “MQTT” ” inside of search box of Shodan. Port number 1883 is the default port for MQTT broker. Finally Search result shown in the Figure 5. This shows 24998 brokers with default port successfully displayed on Shodan page.

Figure 5: MQTT broker on port 1883 in Shodan

The code for the MQTT connection is shown in Figure 6. When brokers have "0" link code, no client authentication mechanism is used by the broker, so that unknown user or publisher can easily connect to the broker. All brokers have code "0" in Figure 6, so attackers can easily target all brokers.

Figure 6: Connection code in Shodan Page

First scenario illustrated in Figure 7.When all broker connection code is “0”, attacker start subscribe with all broker topics (subscribe to #) that can provide sensitive information that is to be analyzed later.

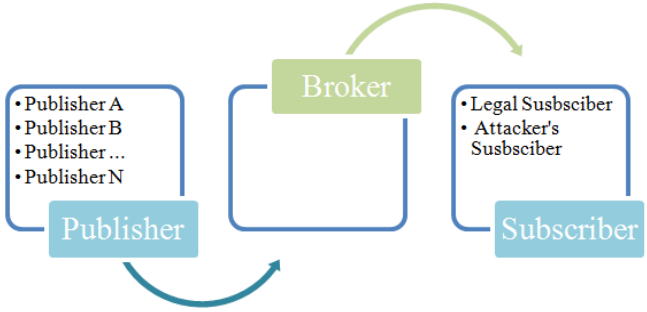

Figure 7: Attacker subscribe with all broker topics

Another Scenario provided in Figure 8. Attacker can start the attack by posting details to the broker here. In this scenario subscriber are street lamps, to control street lamps legal publisher has to publish a message. On another side attacker can get a related messages to control street lamps by subscribing to broker. The attacker can easily publish his data, by examining the control information. The attacker will use this sort of scenario to publish information concerning spam.

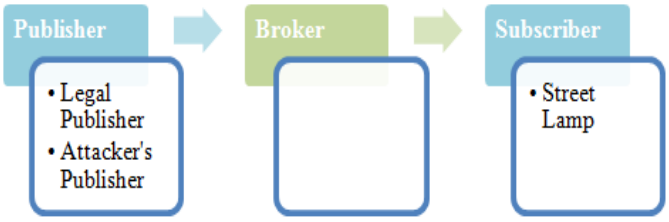

Figure 8: Attack initiated using control message

Two scenarios discussed above are common scenarios that can impact both the local and public networks. Next scenario assumes IoT system connects the attacker to the same network. Based on this assumption attacker can get related information by analyzing network traffic when in-transiting data. Collected information is in the form of plain text, like name of topic, port number, IP broker and data payload of

MQTT used in IoT system. The Wireshark and Ettercap can be used to perform an attack. [18] Attacker and publisher are in the same network. Publisher may detect and alter transit data so attacker can perform data authentication, data protection and data integrity of MQTT packets.

5.1. Authentication

The username and password must be used to get an authentication, if the broker uses the client authentication method. Attacker is not permitted to play the role of publisher or subscriber unless he knows username and password. Both attacker and publisher are in the same network in the above scenario.[20] Therefore hackers can simply detect the traffic on that channel. Whereas CONNECT packet transit to get connected with Broker from publisher to broker, the username and password are revealed so attacker can easily attack. Figure 9 shows the CONNECT packet transit from publisher to broker which the intruder sniffed. CONNECT packet includes header in Authentication Process i.e. KeepAlive which informs that how long IoT device connects with broker. Thus the system sends the Link packet to broker again to restart the connection when header time has expired.

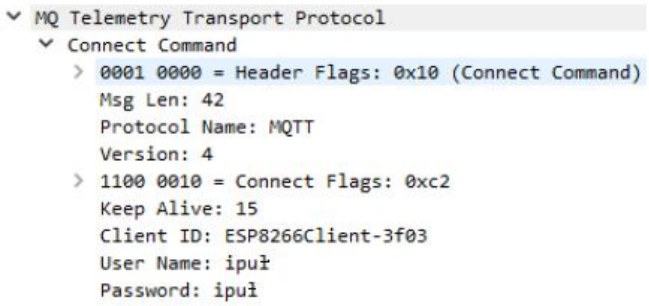

Figure 9: Connect command packet

5.2. Data integrity

Data integrity is another type of attack, which is primarily geared to data integrity in transit. Attacker already knows in this attack about data packets which can be altered during transmission. In this scenario attacker should change the name of the subject from "testTopic" to "testTopuc". To change the name of the topic, the attacker creates a filter file called owned.filter which filters in transit data packet with broker IP as destination address and TCP port 1883[21]. When the packet identifies the matched filter criteria, it starts searching for "testTopic" and changes it as shown in Figure 10 with "testTopuc." Once the subject name has been changed, the Etterfilter application is used to compile the filter file which finally gives an output file to "owned.ef."

```
#owned.filter
if (ip.proto == TCP && tcp.dst == 1883 && ip.dst == 'IP Broker' &&
search(DATA.data, "testTopic" )) {
  replace( "testTopic" , "testTopuc" );
  msg("payload replaced\n");
}
```

Figure 10: Replacing topic name of MQTT data packet

Ettercap is an free and open source tool or application which run on specific interface, the attacker use this interface to link with the internet and attacker uses compiled filter file to modify the packet. This step is given in Figure 11.

```
etterfilter owned.filter -o owned.ef

ettercap -T -q -i eth0 -F owned.ef -M ARP /// ///
```

Figure 11: Command to run ettercap application on specific interface

After successfully change the published message topic name that is received by subscriber device. This is represented in Figure 12.

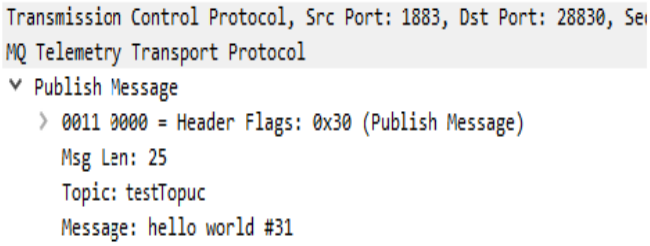

Figure 12: Result of change in topic name

6. CONCLUSION

Message Queuing Telemetry Transport Protocol is a widely used application protocol in IoT system. Providing security to MQTT protocol is very important compare to all other protocols because of its simplicity and scalability. The overview of this paper says it is needed to safeguard the IoT-connected devices from targeted hackers and misuse which could prevent IoT from developing as a robust and scalable paradigm. This paper identifies different attacking scenarios to detect different attacks that target the IoT connected devices in MQTT protocol and also discussed about the necessary requirements to provide security to MQTT protocol.

REFERENCES

1. Syed Naeem Firdous, Zubair Baig, Craig Valli and Ahmed Ibrahim "**Modeling and Evaluation of Malicious Attacks against the IoT MQTT Protocol**", 2017 IEEE International Conference on Internet of Things, 2017.

2. Haripriya A. P and Kulothungan K, "**Secure-MQTT: an efficient fuzzy logic-based approach to detect DoS attack in MQTT protocol for internet of things**", A. P. and K. EURASIP Journal on Wireless Communications and Networking, 2019. https://doi.org/10.1186/s13638-019-1402-8
3. Syaiful Andy, Budi Rahardjo and Bagus Hanindhito, "**Attack Scenarios and Security Analysis of MQTT Communication Protocol in IoT System**", Proc. EECSI 2017, Yogyakarta, Indonesia, 19-21 September 2017.
4. Hector Alaiz-Moreton and Jose Aveleira-Mata, "**Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol**" in Research Article, 2019. https://doi.org/10.1155/2019/6516253
5. Ahmad W. Atamli and Andrew Martin, "**Threat-based Security Analysis for the Internet of Things**", International Workshop on Secure Internet of Things, 2014.
6. Juanita Koilpillai, is MQTT is secure for IoT, [Online], Available: https://www.waverleylabs.com/is-mqtt-secure-for-the-iot-only-with-an-sdp/
7. Tarfa Hamed, Jason B. Ernst, and Stefan C. Kremer, "**A Survey and Taxonomy of Classifiers of Intrusion Detection Systems**", Springer International Publishing AG 2018. https://doi.org/10.1007/978-3-319-58424-9_2
8. Lane, T. (2006). **A decision-theoritic, semi-supervised model for intrusion detection**. In Machine learning and data mining for computer security, pp. 157–177. London: Springer.
9. Dan Dinculeana and Xiaochun Cheng, "**Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices**", Applied Science 2019, 9, 848, 2019.
10. Bhanujyothi H C, Rajesh S M, Vidya J and Sahana D S, "**A Study on IoT Messaging Protocols and it's Comparision for implementation of IoT Services**", in International Journal of Scientific and Research Publications 2019,Volume 9, Issue 3, pp. 596-601.
11. A. Banks and R. Gupta, "Mqtt version 3.1. 1," OASIS standard, vol. 29, 2014.
12. AMQP protocol specification. [Online]. Available: https://www.amqp.org/
13. S. Andy, B. Rahardjo, and B. Hanindhito, "**Attack Scenarios and Security Analysis of MQTT Communication Protocol in IoT System**," in Proceedings of the 4th International Conference on Electrical Engineering, Computer Science and Informatics, EECSI 2017, pp. 19–21, IEEE, Yogyakarta, Indonesia, 2017. https://doi.org/10.1109/EECSI.2017.8239179
14. ISACA Volunteer Member, "**Cybersecurity Fundamentals Study Guide**," ISACA, 2015.
15. M. M. Hossain, M. Fotouhi and R. Hasan, "**Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,**" 2015 IEEE World Congress on Services, New York City, NY, 2015, pp. 21-28.
16. Denial-of-Service, [Online], Available:https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
17. C. Bormann, M. Ersue, and A. Keranen, " **RFC 7228 Terminology for Constrained-Node Networks**," IETF, May 2014.
18. Iot Security Awareness. InfoSec Institute [Online]. Available: http://resources.infosecinstitute.com/iot-security-awareness/
19. **Fuzzy logic based proportional integral control of frequency for small, International Journal of Advanced Trends in Computer Science and Engineering**, 2020, volume 9, number 2, pages 1275-1279 Ramaswamy, K. and Dayanand Lal, N. and Parikshith Nayaka, S.K. and Venna, R.C. and Brahmananda, S.H https://doi.org/10.30534/ijatcse/2020/57922020
20. **Effective and Secure Approach for Multi-Keyword Quest Graded over Authenticated Data, International Journal of Advanced Trends in Computer Science and Engineering**, 2020, volume 9, number 2, pages 2278-3091, Shobharani D, Parikshith Nayaka S K, Swasthika Jain T, Dr. Dayanand Lal https://doi.org/10.30534/ijatcse/2020/72922020
21. Mr. Parikshith Nayaka S K, Mrs. Shobha Rani, Dr. Dayanand Lal, Dr. M Anand. (2020). **Convert Channel and Information Hiding in TCP/IP** . International Journal of Control and Automation, 13(02), 582 - 591. Retrieved from http://sersc.org/journals/index.php/IJCA/article/view/11199