International Journal of Computer Networks and Communications Security

VOL. 8, NO. 7, July 2020, 52–58
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Man in the Middle Attacks: Analysis, Motivation and Prevention

Danish Javeed[1], Umar MohammedBadamasi[2], Cosmas Obiora Ndubuisi[3], Faiza Soomro[4] and Muhammad Asif[5]

[1, 5] Northeastern University, Shenyang, Liaoning province, China

[2, 3] Changchun University of Science and Technology, China

[4] Central China Normal University, Wuhan China

[1]*thedanishkhn@gmail.com*

ABSTRACT

Computer systems and applications are improving day by day and with the advancement in such area it give birth to new cyber-attacks. Man in the Middle attacks (MITM) are one of those attacks. An attack where an outsider or third party enters in between two online users, where both of the users are unaware of it. The malware in such scenario mainly monitors and have the ability to change the information which is classified onsly to these two users. Mainly it is knows as a protocol to an unauthorized user within the system who can access as well as change the information of the system without leaving any trace to the existing users. This issue is critical. This paper aims to the understanding of the MITM and to understand its different categories. Finally this paper aims to present some of mechanism for the prevention of such attacks and to identify some of the future research directions in such area.

Keywords: *Information Security, Cyber Attacks, MITM Attacks, Network Security*.

1 INTRODUCTION

Internet has become the most important aspect of our life in this modern world. Most of our daily routine is based on cellular networks as well as internet. Social media is on the top. Furthermore internet banking, online shopping has become more easier day by day and it's not possible without the use of an internet. With the need of internet it gave the hackers an opportunity to be targeted easily. Hackers mainly target different organization in order to steal confidential data which may lead in to money loss [1]. Man in the middle attack is the most common attack in such case, which makes it the most primary threat to network security. The most common case of such attack consist of victims (two users) as well as the attacker which is a third party. The attackers acts as the middle man in between the two users and the users are unaware of it that there is actually a third person in between us. The assailant accesses the communiqué channel and it have the ability to operate the messages in between the two users. Such MITM bouts can be hurled in numerous communiqué straits comprising GSM, Wi-Fi, UMTS, Bluetooth. The adversary's objective is the definite data flowing among the endpoints as well as it infects the veracity and discretion of the data.

Attacker has the ability to harm the discretion by eavesdropping as well as veracity by message alteration by communiqué intervention. Attacker have also the ability to divert, change or abolish the messages to cause end of communiqué for one of the user which results in the compromise of availability issue. MiM MitM or MIM , MTIM are other names of man in the middle attack.

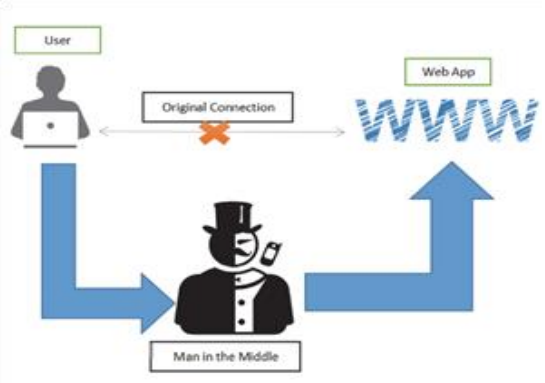


Fig. 1. MTIM attack

One of the cases of such attacks is known as dynamic eavesdropping in which the adversaries makes independent associations with the victims and affect the communication in between users by modifying the messages in between the two users in order to influence the trust in between them. The adversary has the ability to intercept the messages in between them in order to modify the messages. Most cryptographic agreements comprise some kind of endpoint verification chiefly to persevere MITM attacks [2]. For example, TLS can validate one or the two parties by a normally disclosed in endorsement expert [3]. These attacked can be further divided in to four different main types. The first one is spoofing based MITM, in which the attacker intercepts the traffic in between the two users with the help of spoofing attack and then control the transmitted data in between the two users without leaving any trace so the users are unaware of it. But in some other cases the attackers used different strategies i.e. in DNS spoofing the attackers spoofs the devices in between the endpoints while in ARP spoofing, the attacker directly spoofs the endpoints or the devices of the victims.

Secondly the TSL OR SSL attacks, in which the attacker put itself in the communication which is in between the two endpoints. The attacker establishes connection or two separate SSL connections and sees the message in between them. Which gives an opportunity to the attacker to modify and record all the communication in between the two victims. Third, the BGP MITM attack, in which the attacker provides the acquired traffic to the endpoint. This is IP hijacking. In this case, the traffic will pass through the opponent's independent location. In this case, the traffic is likely to be affected. Last but not least, fake base station attacks, where the attacker sets up fake transceiver stations and then uses them to manipulate the victim's traffic. MITM is just like a ball game where two people plays catch the ball while in the meantime the third person tries to intercept the ball. Major types of spoofing attacks has been explored in the remaining part of this paper as well as the future scope is also been explained in the remaining part of the paper.

2 SPOOFING BASED MTIM ATTACKS

Spoofing is a technique which name is originated from spying. In early times most of the European spies in order to hear the secrets conversations in between people by outing themselves in their normal life. The same technique is applied in the current spoofing techniques. The attackers intercept itself in the communication between two users or two victims and control the transferring data in between them while the victims are unaware of its happening [4]. When a user communicate with another user through the encrypted network, if their network is similar to the unidentified MAC address, the server will send an address determination protocol (also referred to as ARP) request to all users connected to the similar network. Users with declared Internet protocols can only predictably respond with their MAC address. Though, when ARP cache is accomplished in a dynamic approach, cache entrances can be easily fictitious by counterfeit ARP messages, meanwhile proper verification technique is missing. The MITM as message tempered the attacker only target the content of the message which will be received by the other user. And this attack has a severe impact on the network as the content of the message may contain sensitive and confidential information. Many authors show the state of art of using security weakness in order to conduct a faultless man in the middle attack.

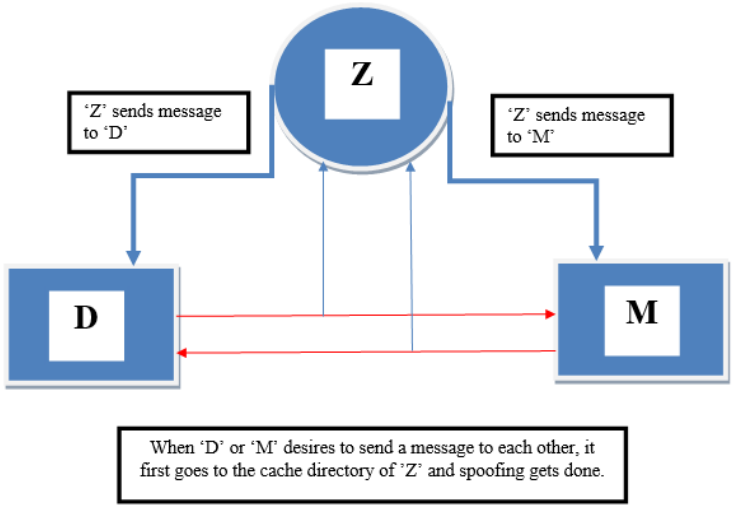
Supposing we have a network the attacker 'Z' (IP= 10.0.y.y3 MAC = FF:FF:FF:FF:FF:Y3), victim 'D' (IP = 10.0.y.y1, MAC CC:CC:CC:CC:CC:Y1), and victim 'M' (IP = 10.0.y.y2, MAC = DD:DD:DD:DD:DD:Y2). The next stages for a faultless spoofing founded on ARP are presented below:

[1] Z' directs an ARP answer to 'D', which declares that IP: 10.0.y.y3 has MAC address: FF:FF:FF:FF:FF:Y3. This note will apprise 'D''s ARP table.

[2] 'Z' likewise directs an ARP Answer to 'M', which declares that IP: 10.0.y.y2 has MAC address: DD:DD:DD:DD:DD:Y2. This note will apprise 'M''s ARP table.

[3] As soon as 'D' desires to direct a memo to 'M', it will go to 'Z''s MAC address FF:FF:FF:FF:FF:Y3, instead of 'M''s FF:FF:FF:FF:FF:Y3.

[4] When 'M' desires to send a memo to 'Z', it will likewise go to 'X'.The above instance is shown is the figure below for a better understanding.



ARP cache of 'D'

Before Spoofing	After Spoofing
IP_D: 10.0.y.y2 MAC_D: FF:FF:FF:FF:FF:Y2	IP_D: 10.0.y.y3 MAC_D: FF:FF:FF:FF:FF:Y2

ARP cache of 'M'

IP_M: 10.0.y.y1 MAC_M: DD:DD:DD:DD:DD:Y2	IP_M: 10.0.y.y3 MAC_M: DD:DD:DD:DD:DD:Y2

Fig. 2. Spoofing in between two users

2.1 ARP SPOOFING

These protocols plot net speeches to MAC speeches. ARP is a reliable as well as vital procedure for LAN infrastructures. Attackers amend the cache table of local ARP and subordinate the host's MAC speech with the target IP. The attack is accomplished in order to gain entrée to user's intimate material [6]. These ARP spoofing can be sectioned into two rudimentary types namely deceitful the host and deceitful the gateway of the interior network [7]. When a user desires to interconnect with another user belonging to the similar network with unidentified MAC address, it results in a broadcast where ARP request in the network. The cache accesses are easy to engineer as there is absence of any appropriate verification techniques. The source device can save the IP to the MAC entry for fast-moving up the transmission for the next time by broadcasts evasion.

ARP, a exiled protocol, has minor sanctuary in the hiding scheme.

2.2 Detection of ARP spoofing

There are multiple ways for detecting the ARP spoofing which are given as follow:

2.4.1 Cryptographic solutions

A retrograde well-matched postponement for ARP is S-ARP [8], that depend on on civic basic cryptography for ARP response verification. In order to check the alidity of a user such cryptographic methods can be used. This stops ARP spoofing. P-ARP is an improved form of this for the purpose of authentication. In order to do the authentication of the data It practices adding magic number and HMAC hash function.

2.4.2 Voting-based solutions

A VB spoofing resilient protocol. In case of entrance of any ARP response or demand messages, MR-ARP inquiries the device and authenticate whether the device practices the novel IP address.

2.4.3 Server-based solutions

A non-cryptographic clarification termed antidote remained suggested which stops ARP spoofing by locale advanced priority for the preceding proprietor of the IP address in case there happens a MAC conflict.

2.4.4 Host-based solutions

A middleware host-based clarification for asynchr-onous recognition and deterrence of ARP spoofing attacks is suggested in [13].

2.4.5 Hardware solution

Lively ARP examination was applied in certain switches in order to gain extra security and preservation the network from ARP spoofing attacks. It assurances promoting of only authorized ARP replies and demands. Ethernet switch observes the cogency of the established ARP packets.

2.3 DNS SPOOFING

DNS server an ordered identification scheme scale for url resolution and in client-server design. The names of Domain and servers of DNS are hierarchically systematized into subordinate level domains. This attack is the utmost hazardous attack performed using cache placing for performance enhancements.

It may comprise of three main natures of attacks. First, sniff the data packets during the response process. Secondly, use birthday atack for cache placement, and secondly, hack unauthorized DNS. In order to complete DNS spoofing, the attacker controls local DNS access, causing the target to use a rogue server. DNS is responsible for the TTL of entries, and DNS reintroduces its cache. Attackers use it for DNS spoofing attacks. In order to locate the cache, two methods must be used. First, insert a malicious DNS into the network that generates fraudulent data, and second, send a fake DNS reply before sending an authorized DNS reply.

2.4 Detection of DNS spoofing

In order to detect such attacks there is a very simple way given as follow:

2.4.1 Entropy increasing mechanisms

Additional unpredictability is added to the DNS packets for interweaving the false DNS responses inoculation. The addition of extra entropy does not assure DNS spoofing defense but still decrease the influence.

2.5 DHCP SPOOFING

The DHCP protocol provides the network arrangement parameters of the new host. These parameters include subnet mask, DNS server, default gateway, lease time and IP address. It provides a client-server architecture to exchange data packets between the DHCP server and the host. DHCP has extraordinary security standards and plays a vital role in network management. Each DHCP message is sent in unmodified text form, and there is no DHCP message source authentication. These do not guarantee a trusted DHCP server and communication with real clients. The attacker conducts a DoS attack on the DHCP server, or launches a DHCP starvation attack. This leads to the allocation of the IP address pool provided by the DHCP server, so that the new device cannot obtain an IP address.

2.6 IP SPOOFING

From one user/ sender to the endpoint depends on the IP address of the packet header. It describes the data packet structure which is used for the encapsulation of the data which is supposed to be carried. While by using endpoint and information of source it further defines an addressing mechanism for classifying datagrams. In an IP spoofing attack, a malicious adversary captures the communication between real parties.

Such attackers regulate the stream of communication and it has the ability of elimination of the information sent by the real participants without the information of the real endpoints.

Medium of Communication	Protocol	Concerns
Server Based Communication	ARP	Can't work for wireless communications.
Server Based/ Host Based	ARP, DHCP	Compatible for DoS, DHCP but has a single point of failure.
Host Based	ARP	Level of importance of each host is very difficult to decide.
Host Based	ARP	Works only with Linksys routers. Static IP not supported.
Cryptographic/ Host Based	UDP/ ARP	For UDP, authentication is a must need.
SYMMETRIC/PRIVATE-KEY CRYPTOGRAPHY	DHCP	Legitimate hosts must register in advance, adds additional message flow, hard to manage for large number of hosts.
SYMMETRIC/PRIVATE-KEY CRYPTOGRAPHY, RFC	DCHP, DHCP	The authors did not describe how the random value (the number, which used by the server and client to compute the session key) is determined.
Router Based	IP, ARP	Filtering-on-path method can't ensure a secure communication.
Router/ Host Based	IP, DHCP	This system is considered as the highest secured communication. But not so user friendly.

Fig. 3. Comparison of different types of spoofing prevention

3 MITM IN VANETS

A type of MITM attacks in which the attackers aims to alter the messages in between genuine vehicles and such attacks results are mostly critical because many time such messages contains safety information. Such attacks in vanets can be done in two different modes i.e. active mode and passive mode as shown in the figure 3a.

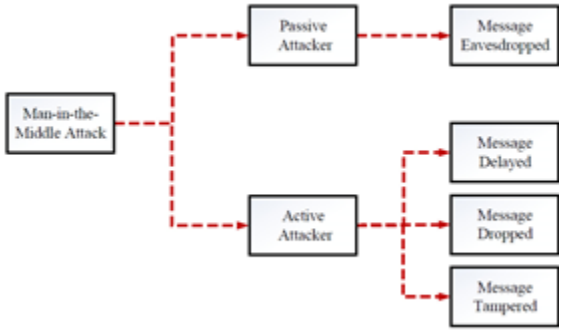


Fig. 3a. MITIM in vanets

4 SIMULATION RESULTS & DISCUSSION

In this part of the paper the simulation results has been given of two versions of MITM attacks in VANET i.e. message delayed and message tamper.

A. Message Delay Attacks:

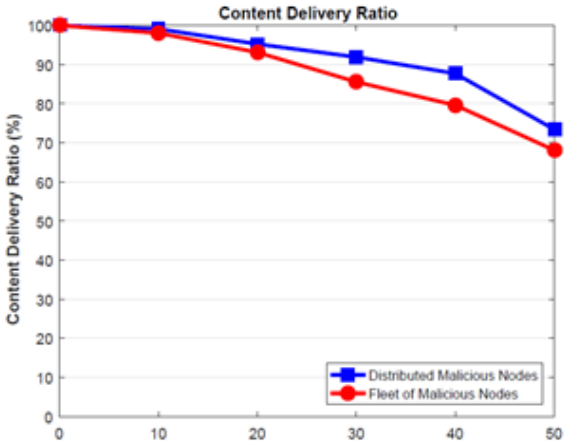


Fig. 4a. Malicious nodes (%)

As shown in the figure above after the man in the middle attacks the nodes are having a delay of 2 seconds. When some malicious nodes are introduced to such networks the delay will be increases directly. Without these nodes the message can be received at the end point without any delay. So as result a very wide portion of the network is affected due to such attackers. The delay has a direct proportionality with the malicious nodes. As shows only 10 percent of malicious nodes can produce a delay of about 47percent. If the number of malicious codes increases to 60 percent the delay will be 80 percent in such networks.

On the other hand if we look at figure 4b below it can be seen that the communication can still be occurs under such attacks with the delay in time. The metric in the below figure proves that the message has been arrived to the end point but with some certain delay.

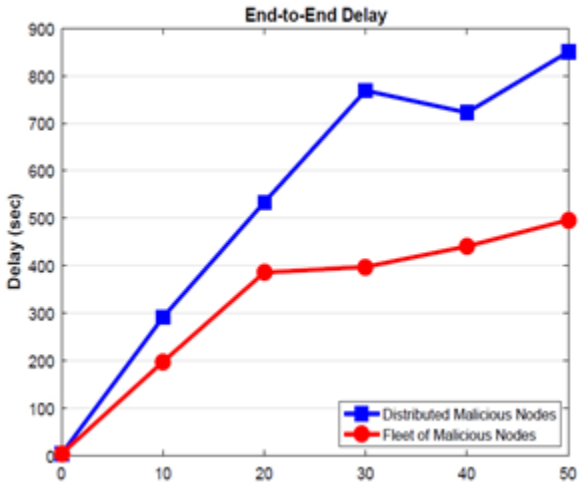
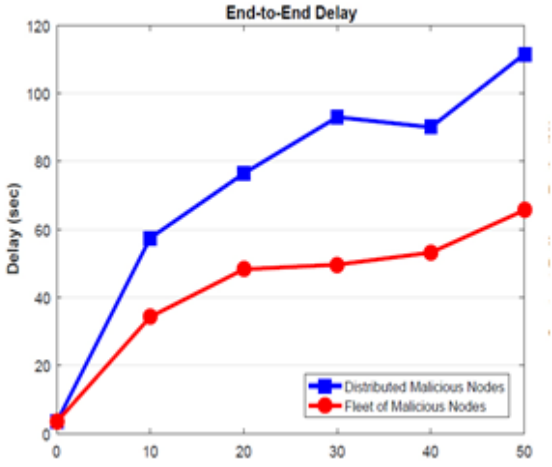


Fig. 4b. Malicious nodes (%)

By carrying on the above topic if the number of malicious nodes is increases it shows a clear increase in delay as well as packet loss. For examole if a network in injected with about 40 percent of malicious nodes it will results in about 20percent in packet loss.

B. Message Tamper Attacks

As it is already mentioned that at the presence of any malicious node in the network, it has the ability to change the data of the message or its location as well as some part of the data. In such case the paper aims to focus on the data of the message. Figure 5a shows delay in the network while in the presence of malicious node which have the ability to change the whole content of the message. With the increase in the malicious nodes, end to end delay of the network will be increased directly.



While on the other hand figure 5b shows a decrease in CDR with the increasing number of malicious nodes. Furthermore the CDR can be affected by the pattern of attack. As shown in the figure 5b a very small portion of the network is malicious which results in the delivery of genuine message from the user to the end points. As a result a high CDR is achieved.

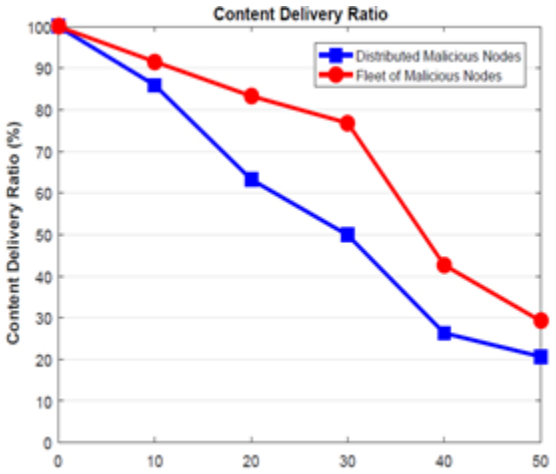


Fig. 5b. CDR

T he last part of the simulation contains the number of the compromised messages. It have the same nature like the above part of the research. A high amount of messages and its contents has been compromised due to a large amount on malicious modes all over the network. On the other hand due to the presence of such number of malicious nodes a high number of message contents has been tampered too. The percentage of the compromised messages has been shown in the figure 6 below:

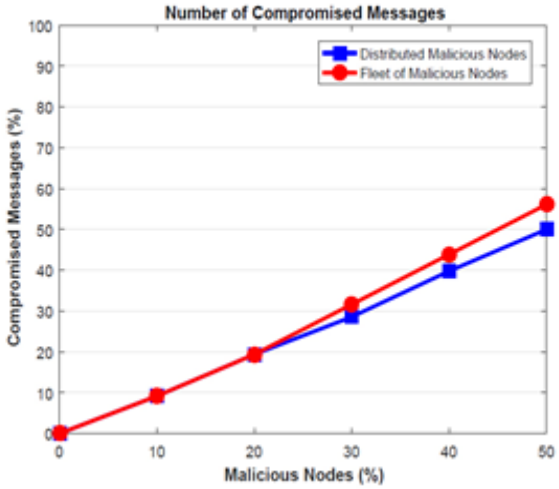


Fig. 6. No of Compromised messages

5 CONCLUSION

In this paper, various MITM attack has been analyzed as well as offered a inclusive survey of different attacks as well as defensive mechanism on the basis of caricature practices. Numerous MITM defense techniques have been shown lengthways with their descriptions. Real data flowing is the main objectives of the adversary i.e. the transmitting data among the two endpoints as well as the veracity and privacy of the data. In this paper different MITM attacks has been well explained with its defensive mechanism. The main problem with the current work related the Man in the middle attacks comprise circulation through a middleman, however still an innovative MITM procedure is not obtainable so this can be totally a different research direction. Man in the middle attacks can be combined with plentiful cryptographic approaches such as key dissemination and elliptic curve cryptography. As in the future work we aims to extend this research in order to evaluate the impact of such attack in different background of VANET by the flexibility of the nodes.

6 REFERENCES

[1] C. L. Abad, R. I. Bonilla, "An analysis on the schemes for detecting and preventing ARP cache poisoning attacks", Proc. 27th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW'07), pp. 60, 2007.

[2] S. Shukla, I. Yadav, "An innovative method for detection and preventionagainst ARP spoofing in MANET", Int. J. Comput. Sci. Inf. Technol. Secur., vol. 5, 2015.

[3] M. Oh, Y.-G. Kim, S. Hong, S. Cha, "ASA: Agent-based secure ARP cache management", IET Commun., vol. 6, no. 7, pp. 685-693, May 2012.

[4] Arpwatch the Ethernet Monitor Program; For Keeping Track of Ethernet/IP Address Pairings.

[5] S. Y. Nam, D. Kim, J. Kim, "Enhanced ARP: Preventing ARP poisoning-based man-in-the-middle attacks", IEEE Commun. Lett., vol. 14, no. 2, pp. 187-189, Feb. 2010.

[6] A. Herzberg, H. Shulman, "Antidotes for DNS poisoning by off-path adversaries", Proc. 7th Int. Conf. Availability Rel. Secur. (ARES), pp. 262-267, 2012.

[7] Javeed, Danish, et al. "An Efficient Approach of Threat Hunting Using Memory Forensics." International Journal of Computer Networks and Communications Security 8.5 (2020): 37-45.

[8] H.-M. Sun, W.-H. Chang, S.-Y. Chang, Y.-H. Lin, "DepenDNS: Dependable mechanism against DNS cache poisoning" in Cryptology and Network Security, New York, NY, USA:Springer, pp. 174-188, 2009.

[9] Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051.

[10] S. Y. Nam, D. Kim, J. Kim, "Enhanced ARP: Preventing ARP poisoning-based man-in-the-middle attacks", IEEE Commun. Lett., vol. 14, no. 2, pp. 187-189, Feb. 2010..

[11] M. Oh, Y.-G. Kim, S. Hong, S. Cha, "ASA: Agent-based secure ARP cache management", IET Commun., vol. 6, no. 7, pp. 685-693, May 2012.

[12] M. Antonakakis, D. Dagon, X. Luo, R. Perdisci, W. Lee, J. Bellmor, "A centralized monitoring infrastructure for improving DNS security" in Recent Advances in Intrusion Detection, New York, NY, USA:Springer, pp. 18-37, 2010.

[13] X. Bai, L. Hu, Z. Song, F. Chen, K. Zhao, "Defense against DNS manin- the-middle spoofing" in Web Information Systems and Mining, New York, NY, USA:Springer, pp. 312-319, 2011.

[14] X. Liu, A. Li, X. Yang, D. Wetherall, "Passport: Secure and adoptable source authentication", Proc. Netw. Syst. Des. Implement. (NSDI), vol. 8, pp. 365-378, 2008.

[15] Khan, Tahir Ullah. "Internet of Things (IOT) Systems and its Security Challenges." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 8.12 (2019).

[16] Fatima, A. (E-Banking Security Issues-Is There A Solution in Biometrics?. Journal of Internet Banking and Commerce, 16 (, 2011).