**Name: Tejas Rahul Rokade**

**Reg. No.: 20BDS0033**

**Cryptography and Network Security Theory DA-1**

**Submitted to: Dr. Santhi H**

**Topic: Man in The Middle Attack**

**Research Paper 1**

**The Use of Machine Learning Algorithms to Detect Man-In-The Middle (MITM) Attack in User Datagram Protocol Packet Header.**

**Problem Addressed/Objectives Stated:**

Attacks on the internet are becoming an uncontrollable issue due to the fact that, many people, co-corporations and the entire social space depend on the accurate working capacity of the internet. An older, yet still, very common and popular attack on computer networks is the Man-In-The-Middle attack (MITM). MITM attack is defined as a real-time private listening, which enables a malicious user to intrudes into an already established networks amongst hosts exchanging data with the intention to infuse false information. In today’s advanced technological era, machine learning algorithms (MLA) are felt in numerous applications which are beneficial in everyday life, making the impossible possible. Currently, machine learning (ML) approaches have been deployed to erect predictive models for the supervision of network attacks. In the light of above, this research proposes the application of the Forward Greedy Stepwise Selection machine learning algorithm to improve detection of MITM attacks in the User Datagram Protocol (UDP) Packet header fields in computer networks by achieving the outlined objectives of examining a switch network using Packet Tracer to probe physical and logical environments required to run ARP simulations efficiently, analyse UDP packet headers using Wireshark to identify and capture ARP Spoofing attacks and to evaluate the efficiency of the Forward Greedy Selection algorithm in selecting packet header fields to provide better performance results for the detection of MITM data.

**Proposed Methodology:**

1 METHODOLOGY FOR SIMPLE ARP REQUEST IN PACKET TRACER

− Design a simple switch network using Packet tracer to provide a simulation and logical environment.

− Run simulation after assigning IP addresses to all pc nodes and router interfaces to initiate an ARP session.

− Each device will send an ARP request to the routing device to map corresponding ip addresses to mac addresses (physical interface).

− Capture ARP packet for TCP/IP session and view header information to validate the fact that packet header information can be captured and analysed.

2 TO IDENTIFY UDP PACKET HEADER FIELDS AND OPERATION USING WIRESHARK BEFORE AND AFTER MITM SESSION ESTABLISHED.

The TFTP client may represent a workstation or workstations connected to a layer 2 device to provide a realistic view of network data. Thus, allowing a realistic demonstration of UDP capture of a TFTP session. The Pc must have both a connection to the switch and wired/ethernet connection.

**Results Obtained:**

Forward Feature selection subset method was used as a pre-processing step in classification tasks to evaluate different subsets of features in order to make a decision on which subset provides better performance while Random Forest classifiers provided an automated way of identifying multiple combinations of features that provide different accuracy values, thus, allowing easy identification of key trends and anomalies. It ignores redundant and irrelevant features which results in limited processing time and has the capacity to increase classification performance. This approach was employed to aid select a subset of packet header fields that can be compared between different packets to detect MITM semi-duplicated packets.

**Conclusion:**

The overall driving objective of this research work is to design a systematic approach to help detect UDP packet headers from MITM attack using the Forward Greedy Selection algorithm in a network was successfully achieved by undertaking the following specific objectives by examining a switch network using Packet Tracer to probe physical and logical environments required to run ARP simulations efficiently, analysing UDP packet headers using Wireshark to identify and capture ARP Spoofing attacks and finally, evaluating the efficiency of the Forward Greedy Selection algorithm in selecting packet header fields to provide better performance results for the detection of MITM data. For network, data and cyber security enthusiasts, this research work can be of great importance to them as a benchmark for further research solutions to enhance security in data and network attacks. The researchers call for other efficient algorithms and techniques to help fortify the security gaps in the UDP protocol. As an extension of this study, the application of cryptographic algorithms and approaches can be used to enhance security in the UDP transport protocol.

**Limitations:**

The accuracy in results are lower due to the inconsistencies of UDP traffic displayed in thus, we are able to identify trends only during the forwarding process of an MITM attack. All other UDP header data are inconsistent because UDP traffic is connectionless and does not require sequence numbering or management of data authentication. Therefore, in order to effectively identify MITM trends in UDP traffic, we require the consistent observation of packet length and UDP checksum validation, which could influence decisions on mitigating and refreshing ARP address tables or DHCP configurations.

**References**

Fayyaz, F., & Rasheed, H. (2012). Using JPCAP to prevent man-in-the-middle attacks in a local area network environment. *IEEE Potentials*, 31(4), 35–37.

Narayan, S. (2014). Improving Network Performance : An Evaluation of TCP / UDP on Networks. (December).

Roblek, V., Meško, M., & Krapež, A. (2016). *A complex view of industry 4.0.* Sage Open, 6(2), 2158244016653987.

Sanders, C. (2017). Practical packet analysis: Using Wireshark to solve real-world network problems. No Starch Press.

Sumiahadi, A., Acar, R., Odoh, C. K., Martins, P. E., Akpi, U. K., Okekeaji, U., … Glick, B. R. (2017).

**Research Paper 2**

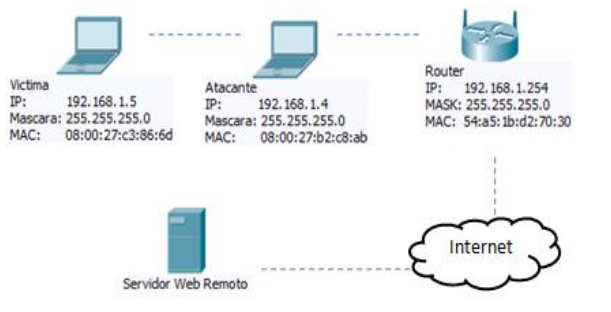
**Man in the Middle Attack: Prevention in Wireless LAN. International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 7 (2018) pp. 4672-4671 © Research India Publications.**

**Problem Addressed/Objectives Stated:**

For a computer to send data to another through a network, the compliance with some agreements at the hardware and software level is required, for handling, transporting, and ensuring the delivery of the traveller data to its specific destination, each data is fragmented into packages that have a low level structure that pass through thanks to a series of protocols that are stacked in a standardized model. Packets of information travel through a channel that can be wireline, fiber optic, or electromagnetic signals among others, this means that in any of these means is possible to intercept such messages and get to know part of the content of the message, its origin, its provenance and its structure.

**Proposed Methodology:**

To reproduce the MITM attack, there has been implemented two types of attacks: ARP Poisoning and DNS spoofing. The first one consists of sending fake ARP messages containing manipulated MAC addresses to make a machine pass off as a different one, each machine maintains a cache with the translated addresses to reduce the delay and the load by which this attack aims to fix and maintain the false values in its cache. The second consists of generating false responses to the name resolution requests made by the victim host.



In this implementation the objective is to generate a DNS false resolution when the host victim is trying to navigate anywhere on the internet through a router, so that it will be redirected to a web service that runs on the host of the attacker.

Sending ARP Requests to the Router

Monitoring the ARP Host Table

Configure Static Entries in the Table of the Customer

Restrict Client ICMP Packets

Use a Public Key System

**Results Obtained:**

Sending ARP Requests to the Router

The effectiveness of the attack varies regarding the strategy employed, when a thread for ARP requests is created from the application, the client’s ARP modification table remains unchanged with false data; When the attack is launched releasing ARP requests without the use of attack threads, is not effective against the mechanism that has been installed on the victim machine. The interval of sending ARP requests also significantly affects the result of the test, when the attack is made by launching the ARP request in 30 seconds interval and the script on the victim runs every 15 seconds the attack is unsuccessful, but when is done in an interval of 5 seconds is an effective attack. A running time of 3 seconds on the script on the victim, avoided carrying out the attack when it generated ARP requests at 3 second intervals.

Monitoring the ARP Host Table

This strategy basically consisted of setting up a validation of the MAC of the gateway in the ARP table of the victim, this measure does not prevent the attack but it generates an indicator that our machine is being attacked. Establishing awareness levels of an attack of man in the middle, this strategy would be complementary as for example to the script settings mentioned in paragraph A.

Configure Static Entries in the ARP Table of the Customer

This strategy was effective in a 100% to prevent ARP Poisoning and it requires the registration of the MAC address of its gateway to be set in all computers in a network however, it is not effective to prevent DNS spoofing, recording manually the IP addresses of the sites visited by a customer is not a feasible option because it requires to add to the hosts files of the victim the resolution of the frequented servers and for an internet user, this is not a practical solution.

**Conclusion:**

The Recurrent sending of ARP requests to the router from the victim is effective, depending on the refresh interval of the ARP table and the attacker code programming strategy, this result demonstrates the variety of solutions to the attack against the variety of ways to carry it out. For the test conditions the refresh every 15 seconds or less of the ARP table was effective to prevent man in the middle attack, this value can vary substantially depending on the characteristics of the attack. This defence was not effective when the attacker launches the attack at an interval of 1 second using threads. Another aspect to consider in this solution is the traffic that is generated on a network if all of your hosts are permanently launching requests to the router.

**Limitations:**

Some of the strategies proposed in this article are complementary, for instance, the script that runs on the client and maintains the ARP table updated, and the script that keeps monitoring the system by comparing the current record against one fixed.

The static configuration of the MAC addresses of the computers can be a tedious task for a network administrator and this aspect should be considered when defining the set of measures that are to be planned in order to secure the network.

**References:**

Cagellati Franco. Man in the middle attack to the HTTPS protocol (2009, January February). Security & Privacy, *IEEE (Volumen 7*) [On Line] http://ieeexplore.ieee.org. Páginas 78-81.

DaleAthanasias (2014, April 19).

DNS Spoofing .[On Line] Available: http://blog. vidasconcurrentes.com/seguridad/dns-spoofing [4] *Colasoft LLC*.

Kumar, S., Tapaswi, S. A centralized detection and prevention technique against ARP poisoning. *SANS Institute. ICMP Attacks Illustrated (2001).* June 2012.

Nayak Gopi Nath, Samaddar Shefalika Ghosh. "Different Flavours of Man-In-The-Middle Attack, Consequences and Feasible Solutions". *Computer Science and Information Technology (ICCSIT).*

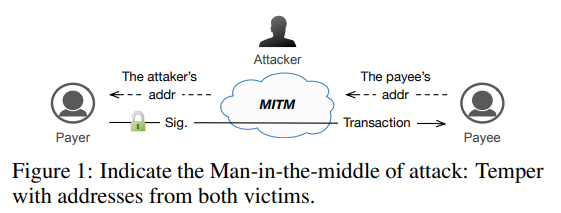
**Research Paper 3**

**Analysis of Man-In-The-Middle of Attack on Bitcoin Address by Abba Garba, Zhi Guan, Anran Li, and Zhong Chen**

**In Proceedings of the 15th International Joint Conference on e-Business and Telecommunications (ICETE 2018) - Volume 2: SECRYPT, pages 388-395 ISBN: 978-989-758-319-3 Copyright © 2018 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved.**

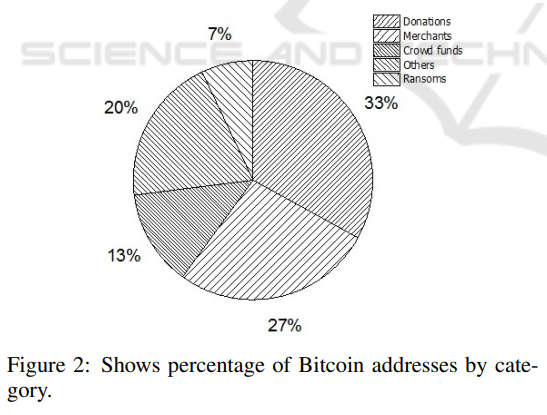
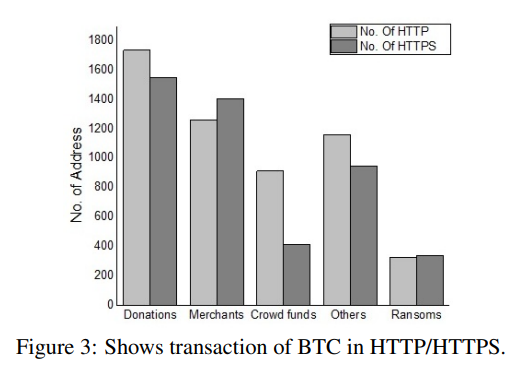
**Problem Addressed/Objectives Stated:**

During the last few years bitcoin and other alternate cryptocurrencies have increasingly become popular mediums for exchanging assests over the internet. To receive payment in Bitcoin, a payee anonymously publishes her address over the internet. After the payer transfers coins to payee’s address, the payee redeems the transaction with her private key through p2p network protocol. Bitcoin as a system and its official implementation does not provide an integrated mechanism to check the authenticity of the addresses, user cannot identify the payment source. However, little attention has been focused on the security of Bitcoin addresses placed randomly on the over the internet. This may allow a Man-in-the Middle attack to tampers payee’s address on the web pages. In this paper we begin by examine how MitM attack is subject to tampering with Bitcoin addresses over the internet using HTTP/HTTPS.



**Proposed Methodology:**

Here they have combined different methodologies to analyse bitcoin addresses collected from websites and global ledgers. Websites consist of crawling many web pages related to cryptocurrency transactions and Bitcoin blockchain were accessed through Blockchainifo. They have used this information to classify addresses based on the transaction distribution. They have also showed us how REGEX filtering can be used to obtain the Bitcoin addresses in the network traffics and also analyse how many proportions of addresses use HTTP/HTTPS during transaction. Finally, they examined number of active and non-active addresses.



After analysing the addresses, they realized that there were Total of 845,370.19BTC associated with 10,045 addresses collected in addition to that 749,894.00 addresses were involved in the input transactions with each corresponding addresses.

A vanity address is an address with some meaningful sub-string in the address. For example, the Bitcoin address of a valid key pair (d, P) is: 1anaLysis Vj8ALj6mfBsbifRoD4miY36v. The vanity address is produced through brute-force searching of elliptic curve key pairs that can produce an address with a pre-defined pattern. The Bitcoin project provides a command line tool, vanitygen for the generation of vanity addresses.

Alternative to Vanity Address:

1. Outsource Vanity address.
2. Blockchain Domain service.
3. Anti-tampering address mechanisms.
4. Integrating HTTPS with X.509 during payment.

**Conclusion:**

They have analysed a large portion of bitcoin addresses placed on web pages randomly. In our analysis, we have demonstrated that this creates significant security challenges. Particularly, it was showed that MitM attacks may tamper with a victim’s address posted on web site that are not well secured. Alternative digital currencies following Bitcoin may also face the same security challenges. In summary, this form of attack can happen not only with bitcoin addresses but with any unauthenticated information. Given counter measures will provide sufficient guidelines to users who posted their bitcoin addresses on web pages randomly

**Limitations:**

Future research is needed on the potential effects of MitM and bitcoin and alternate cryptocurrencies transactions on HTTP/HTTPS.

**References:**

Ateniese, G., Faonio, A., Magri, B., and De Medeiros, B. (2019). Certified bitcoins. *In International Conference on Applied Cryptography and Network Security*, pages 80–96. *Springer.*

Cheng, K., Gao, M., and Guo, R. (2019). Analysis and research on https hijacking attacks. In Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on, volume 2, pages 223–226. IEEE.

Kumar, A., Fischer, C., Tople, S., and Saxena, P. (2017). A traceability analysis of moneros blockchain. *In European Symposium on Research in Computer Security*, pages 153–173*. Springer.*

Stricot-Tarboton, S., Chaisiri, S., and Ko, R. K. (2016). Taxonomy of man-in-the-middle attacks on https. *In Trustcom/BigDataSE/I? SPA, 2016 IEEE*, pages 527– 534. *IEEE.*

**Research Paper 4**

**Man in the Middle: Attack and Protection by Enkli Yllia , Dr. Julian Fejzajb, Proceedings of RTA-CSIT 2021, May 2021, Tirana, Albania**

**Problem Addressed/Objectives Stated**

Man-in-the-middle attacks are one of the most commonly used network attacks. This attack happens when the attacker manages to get in the middle between two parts of communication: the sender and the receiver.

DNS is a protocol that translates domains into IP addresses [6]. It is an important internet protocol but has security problems and one of them is that the client can’t verify the authenticity of the DNS Response that he gets. This means that the first response that the client gets, it’s the one that is trusted and used. This flaw is used to perform DNS Spoofing.

Removing SSL encryption in a segment between source and destination is a serious threat to the confidentiality claimed and offered by the service offering.

Wi-Fi eavesdropping has to do with creating a fake AP and let other users connect to IT. The most classic scenario is when the AP doesn’t have a password. Being in complete control of the AP one can sniff all traffic and also implement in a successful manner SSL Stripping and HTTPS Spoofing. This can also be implemented with ARP spoofing of a legitimate SSID in a hotel or nearby a bank so that the probability of accessing any important information is higher.

Another way to perform MITM attacks is by using DHCP Spoofing and can be executed in LAN networks.

**Proposed Methodology**

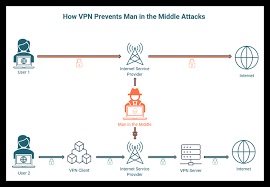
There are a number of implementations that have proved to be helpful in preventing a MITM attack. A simple approach is the implementation of Hypertext Transfer Protocol Secure (HTTPS) which is used to offer a secure communication environment in a network context.

Relating to ARP Poisoning, some methods for the prevention of such an attack includes using S-ARP instead of ARP, which solves security-related issues for ARP but has problems with scalability.

A common way to help with prevention is the application of encryption. Using cryptographic protocols among which TLS (Transport Layer Security) and previously SSL which is now deprecated that offer proper data encryption is a great way to prevent these attacks.

Another method of prevention is the implementation of the DNS (Domain Name System) extension named DNSSEC (Domain Name System Security Extensions). This extension adds security to the lack of mechanisms in DNS to authenticate data and originators, thus helping with MITM DNS Spoofing attempts and DNS cache poisoning. The way DNSSEC does this is by adding authentication on the origin of the data.

A quite effective way of preventing a MITM attack is by using Virtual Private Networks (VPN). In the MITM context, a VPN hides the user’s communication route and encrypts their network traffic as well as hides the IP address. This concealment makes it very difficult for an attacker to trace the IP address and in turn initiate a proper attack.



Regarding prevention methods relating to Rogue DHCP Server MITM attack, a good prevention method is using DHCP Snooping.

A very big reason why prevention is so incredibly important when considering MITM attacks is that the detection of a MITM attack is incredibly difficult. If one is not actively searching for a Man-In-The-Middle attack, it can go unnoticed for quite some time which in effect will allow enough time for the attacker to do what it requires before proper measures are taken. What can be done in these cases is tamper detection, which practically checks the time and latency in an occurring communication. Increased latency may reveal possible occurring attack if records show that such a communication should not occur for the measured time.

**Conclusions**

The increase in the number of users who use the internet and also the increase of the services that are offered online makes this topic really important. Many of these services use user’s personal data, and they do not always offer security and protection. Security problems can be caused by user carelessness but in many times they are caused by the network protocols. There are many network security threats but this paper was focused on Man-in-the-Middle (MITM) attacks. Firstly, this paper analysed what MITM attacks are, and then it explained the different types on how these attacks can be implemented. The most commonly used attack is ARP Spoofing, but this paper also examined DNS Spoofing and DHCP Spoofing. For every type of attack, this paper also analysed the best practices that offer protection. It is important to note that online security cannot be achieved only by securing the network but it should be combined with the cautiousness and carefulness of the network user.

**Limitations**

Practical implementation of these attacks in real-world scenarios and combine them with other types of attacks like DOS, sniffing and phishing could be a challenge.

We don’t know if new technologies like 5G are protected by MITM attacks.

**References**

Conti, Mauro & Dragoni, Nicola & Lesyk, Viktor. (2016). A Survey of Man in the Middle Attacks. *IEEE Communications Surveys & Tutorials.* *18*. 1-1. 10.1109/COMST.2016.2548426.

Gade, Nikhita Reddy & Reddy, Ugander. (2019). A Study of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.

James Forshaw , ATTACKING NETWORK PROTOCOLS A Hacker’s Guide to Capture, Analysis, and Exploitation , William Pollock , 2018 , pg. 95-103

PROWELL, Stacy, Rob Kraus, Mike Borkin. Seven Deadliest Network Attacks (Seven Deadliest Attacks), *Syngress*, 2019.

S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC," *The Second International Conference on Availability, Reliability and Security (ARES'07), Vienna*, 2007, pp. 335- 342, doi: 10.1109/ARES.2007.139.

**Research Paper 5**

**Prevention of Man-in-the-Middle Attack on Internet Communication Using Blockchain Technology.**

**Problem Addressed/Objectives Stated**

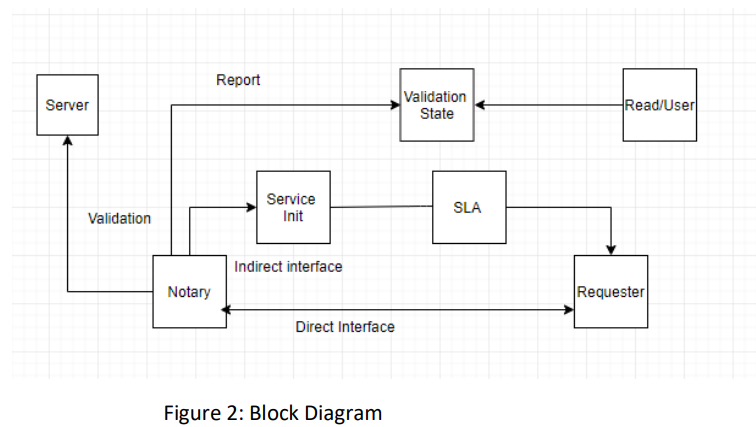
The paper tries to put light on the working of HTTPS and explains how Man-in-the-Middle attack is carried out on HTTPS.

TLS protocol is a cryptographic algorithm which provides complete security to the data transmitted over the network. However, it should be noted that, TLS is not responsible for securing the data in the end systems. It is mostly used for browsing web securely.

All though the TLS systems provides security to the data in transit, the trustworthiness of these systems is heavily dependent on Certificate Authority (CA) systems. There have been many incidences in the past wherein it became possible to perform the Man-in-the-Middle Attack. These attacks have been reported from across the globe. This is because of the weak certificates which are easy to forge and make the server believe that those certificates are valid ones and thus establish the connection. The Man-in-the-Middle attack on HTTPS is on the rise. Thus this paper defines the problem statement as follows “Internet Communication is vulnerable to Man-in-the-Middle attack”.

**Proposed Methodology**

Thus in this paper, they have taken into account the issue of compromising TLS using Man-in-the-Middle attack and present a system called Persistent and Accountable Domain Validation Extended (PADVAE) to prevent the issue of Man-in-the-Middle Attack on HTTPS. The system is based on previous research conducted by Szalachowski, P. (2018). Szalachowski, P.(2018) attempts to improve the existing notary based systems. Notary based systems were introduced in HTTPS earlier, but it had been discovered that there are some issues with the notary based systems like not having enough accountability and the system also introduces privacy issues in the working of HTTPS security.Thus, to implement a more secured and more accountable notary systems, Szalachowski, P. (2018) brings in blockchain technologies into recognition. The Ethereum technology was used in the implementation. They have proposed to use Nebulas blockchain technology. The nebulas blockchain was developed in 2018 and is the advanced version of ethereum blockchain. The nebulas blockchain works on some of the drawbacks of ethereum blockchain and like issues with Smart Contracts and PoW which are the important parts of blockchain development and its application in the HTTPS security.

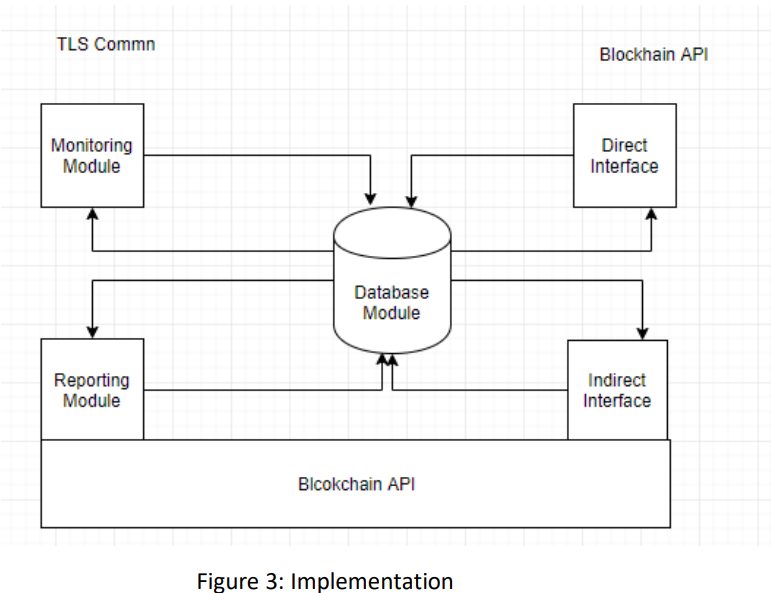


This system is mainly divided into three categories:

• Server It uses the TLS connection to render its service

• Notary It works as a third party auditor. It has to keep checking the servers and verifying their public keys.

• Requester It is more interested to check public keys of the servers. It can operate the server or and make the PADVAE service work from the notary.



Above diagram illustrates implementation. They have followed the following the steps to implement the project:

1. Blockchain Implementation

2. Database Module

3. Direct Interface

4. Monitoring Module

5. Reporting Module

6. Indirect Interface

**Conclusions**

Thus as seen from the above findings, the PADVAE has been implemented and it is able to detect the man-in-the-middle attack. There are a few shortcomings in the implementation which needs to be addressed. Although it strives to keep the notaries transparent, auditable and available, a lot work can still be done on this system as discussed in the previous sections.

**Limitations**

One of the drawback is that there are no enough limitations to test the system. As the Nebulas platform is a new blockchain, there are relatively very limited to test the performance of this blockchain.

TLS 1.3 is an emerging technology. It has been released in Feb 2018 and Szalachowski, P. believes that the upgrade to TLS 1.3 sooner is not something we should expect. Szalachowski, P. states that the TLS 1.3 is different from earlier versions of TLS 1.3 which might affect TLS 1.3, thus it can affect this system.

**References**

Clark, J. (2013). SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements*. IEEE*.

Conti, M. (2016). A Survey of Man In The Middle Attacks. *IEEE, 18*(3)

GitHub. (2019). nebulasio/nebPay. [online] Available at: https://github.com/nebulasio/nebPay [Accessed 10 Aug. 2019].

Internet Society. (2019). What is TLS & How Does it Work? | *ISOC Internet Society.* [online] Available at: https://www.internetsociety.org/deploy360/tls/basics/ [Accessed 5 Aug. 2019]. Ibm.com. (2019).

Karaarslan, E. and Adiguzel, E. (2018). Blockchain Based DNS and PKI Solutions. *IEEE Communications Standards Magazine, 2*(3), pp.52-57.

Nebulas Technical White Paper. (2018).

Szalachowski, P. (2018). Blockchain-based TLS Notary Service.