A Model to Investigate the Security Challenges and Vulnerabilities of Cloud Computing Services in Wireless Networks

Desta Dana Data
destadanedata@wsu.edu.et
Assistant Professor in Information Technology,
Department of Information Technology, School of Informatics, Wolaita Sodo University, Ethiopia

Abstract

The study provides the identification of vulnerabilities in the security issues by Wireless Network. To achieve it the research focus on packet flow analysis, end to end data communication, and the security challenges (Cybercrime, insider threat, attackers, hactivist, malware and Ransomware). To solve this I have used the systematic literature review mechanisms and demonstrative tool namely Wireshark network analyzer. The practical demonstration identifies the packet flow, packet length time, data flow statistics, end- to- end packet flow, reached and lost packets in the network and input/output packet statics graphs. Then, I have developed the proposed model that used to secure the Wireless network solution and prevention vulnerabilities of the network security challenges. And applying the model that used to investigate the security challenges and vulnerabilities of cloud computing services is used to fulfill the network security goals in Wireless network. Finally the research provides the model that investigate the security challenges and vulnerabilities of cloud computing services in wireless networks

Keywords
Cloud Computing, Cyber security, Network Security, Security challenges, Wireless Network

1. Introduction

1.1 Background of Study

The increased use of technology for improved teaching and enhanced learning is going to be the future of education at all levels. Most of the colleges and universities, because of low enrolment in their onsite classes, now offer courses and in some cases the entire degree program through distance education or in online format as well as use various other teaching and learning models.[1].

A wireless network is a computer network that uses wireless data connections between network nodes. Examples of wireless networks include cell phone networks, wireless local area networks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks.

Cloud computing is one of information communication technology application that allow the users to access software applications, hardware, storage, computing processes directly from the web. It offers two paradigms in computing; SaaS and PaaS. The application of cloud computing namely: social medias, Productivity management, Marketing, Communication, educations, healthcare, and others. The model provides the systematic methods to protect the security challenges in the Wireless network. To do this I have use the End to end packet flow communication, identifying the nnetwork challenges which includes cybercrime, insider attacks, attackers, hactivist, malwares and ransomware [1].

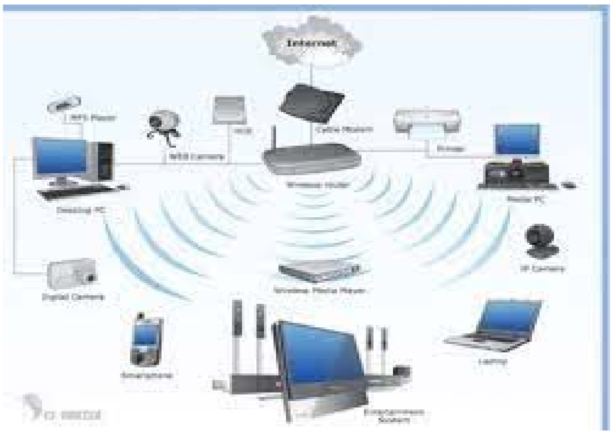


Fig.1. wireless network and cloud services:[2]

Cyber security is the protection of Internet-connected systems, including hardware, software, and data from cyber-attacks. It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data. Whereas security issues related with the protection which includes systems security, network security and application and information security. In this study we will investigate the key challenges of the cloud computing security, vulnerabilities of the cloud computing services and forwarding the suitable solution for the wireless network by proposing the models.

Manuscript received October 5, 2023
Manuscript revised October 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.10.14

1.2 Motivation of the study:

In the 21st century the world is under risks of cyber security problems in different countries are complying in case of the crimes. In the last Year 2020, The FDRE Government of Ethiopia Published and launched the working regulation to combat and fight the challenges and crimes of the cybercrimes.

Different Activists attacker's and malware are strongly working the bounder less fight between different sovereign states and societies. The country's privately owned critical infrastructure banks, telecommunications networks, the power grid, and so on—is vulnerable to catastrophic cyber-attacks. The existing academic literature does not adequately grapple with this problem, however, because it conceives of cyber-security in unduly narrow terms: most scholars understand cyber-attacks as a problem of either the criminal law or the law of armed conflict. Cyber-security scholarship need not run in such established channels.[3],[4],[5],[6].

There are many challenges and problems in the security of wireless networking

- ✓ Ransomware,
- ✓ malwares
- ✓ Cyber Criminals
- ✓ Hacktivists
- ✓ Attackers
- ✓ Insider Threat

To solve those challenges in wireless security issues, I have proposed the two objectives in this research works

1. To investigate the vulnerabilities level of the t hreat in Wireless Network by Wireshark tool
2. To develop model that used to identify, measur e and detect security problems.

1.3 Research Questions

i. What are the major cloud computing security p roblems in Wireless Network?

ii. What is the suitable models to detect the securi ty challenges cloud services?

2. Literature Review

2.1 Vulnerabilities of IEEE 802.11i Wir eless LAN CCMP Protocol

IEEE has recently incorporated CCMP protocol to provide robust security to IEEE 802.11 wireless LANs. It is found that CCMP has been designed with a weak nonce construction and transmission mechanism, which leads to the exposure of initial counter value. This weak construction of nonce renders the protocol vulnerable to attacks by intruders. This paper presents how the initial counter can be pre-computed by the intruder. This vulnerability of counter block value leads to pre-computation attack on the counter mode encryption of CCMP. The failure of the counter mode will result in the collapse of the whole security mechanism of 802.11 WLAN.[7]

Offering real-time data security for petabytes of data is important for Cloud Computing. A recent survey on cloud security states that the security of users' data has the highest priority as well as concern. We believe this can only be able to achieve with an approach that is systematic, adoptable and well-structured. Therefore, this paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. The paper explains the overview, rationale and components in the CCAF to protect data security. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. [8],[9]

Since there Data Center has 10 PetaBytes of data, there is a huge task to provide real-time protection and quarantine. We use Business Process Modeling Notation (BPMN) to simulate how data is in use. The use of BPMN simulation allows us to evaluate the chosen security performances before actual implementation. Results show that the time to take control of security breach can take between 50 and 125 hours. This means that additional security is required to ensure all data is well-protected in the crucial 125 hours. This paper has also demonstrated that CCAF multi-layered security can protect data in real-time and it has three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and 3) convergent encryption. To validate CCAF, this paper has undertaken two sets of ethical-hacking experiments involved with penetration testing with 10,000 trojans and viruses. CCAF can be more effective when combined with BPMN simulation to evaluate security process and penetrating testing results.[10], [11], [4]

2.2 DATA SECURITY BASED ON LAN USIN G DISTRIBUTED FIREWALL

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. In most of the systems, the network security is achieved by firewall and acts as a filter for unauthorized traffic. But there are some problems with these traditional firewalls like they rely on the notation of restricted topology and controlled entry points to function. Restricting the network topology, difficulty in filtering of certain protocols, end-to-end encryption problem and few more problems lead to the evolution of Distributed Firewalls. It secures the network by protecting critical network endpoints, exactly where hackers want to penetrate. This paper is a survey paper, dealing with the general concepts such distributed firewalls, its requirements and implications and introduce, its suitability to common threats on the Internet, as well as give a short discussion on contemporary implementations.

A distributed firewall gives complete security to the network.[4],[12] Based on the reviewed literature of both two papers indicate that the researchers' tried to investigate on the vulnerabilities of security to IEEE 802.11security issues and the second paper also tried the study on security LAN using distributed firewall. Therefore, this study provide the investigations model on Wireless Network which used to identifies the level of vulnerabilities and provide the solution.

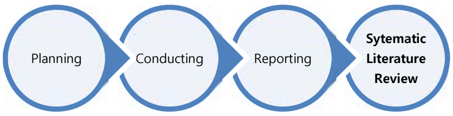
3. Methodology and Research Tools:

3.1 Systematic Literature Review (SLR)

Systematic Literature Review (SLR) will be one of the main research methodologies for this research. This is primarily to summarize the existing information and knowledge on current cloud computing security threats. This is essentially to create a bridge to reflect on how the effectiveness of current cloud architecture security techniques. Systematic literature review is a methodology that identify, evaluate and interpret all available research that is relevant to the particular research question or topic. Systematic literature review can provide a fair evaluation on research topic as it synthesis existing work in the field of cloud computing in a just manner.

The difference between systematic literature review and traditional literature review are:

- ✓ Systematic Literature Review directly addresses the specified research questions by utilizing a review pr otocol
- ✓ Systematic literature review creates a search strategy that targets and detects all of the relevant literature a s possible
- ✓ Systematic literature review would require criteria o f inclusion and exclusion to assess the viability of ea ch primary study. The systematic literature review will be conducted in three main phases.



- ✓ **Planning the systematic literature review**
  - Developing review protocol
- ✓ **Conducting the review**
  - Selecting primary study, extracting da ta and assessing quality of data
- ✓ **Reporting the review**
  - Reporting the whole review holisticall y and documenting the systematic liter ature review process

3.2 Wireshark Demonstration tool

It is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. [13],[14], [15] Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

Wireshark has a rich feature set which includes the following:

- ✓ Deep inspection of hundreds of protocols, with more being added all the time
- ✓ Live capture and offline analysis
- ✓ Standard three-pane packet browser

- ✓ Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- ✓ Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- ✓ The most powerful display filters in the industry
- ✓ Rich VoIP analysis
- ✓ Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- ✓ Capture files compressed with gzip can be decompressed on the fly
- ✓ Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- ✓ Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- ✓ Coloring rules can be applied to the packet list for quick, intuitive analysis
- ✓ Output can be exported to XML, PostScript®, CSV, or plain text

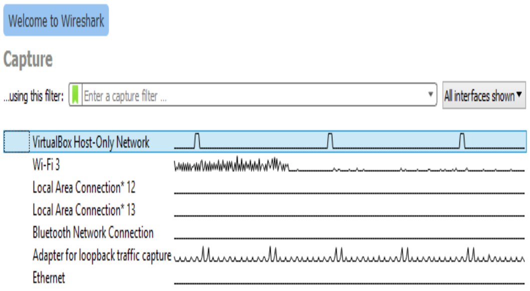

Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown ▾
VirtualBox Host-Only Network
Wi-Fi 3
Local Area Connection* 12
Local Area Connection* 13
Bluetooth Network Connection
Adapter for loopback traffic capture
Ethernet

Fig-2- Wireshark Interface

3.3 Proposed model of Cloud security on Wirel ess Networking

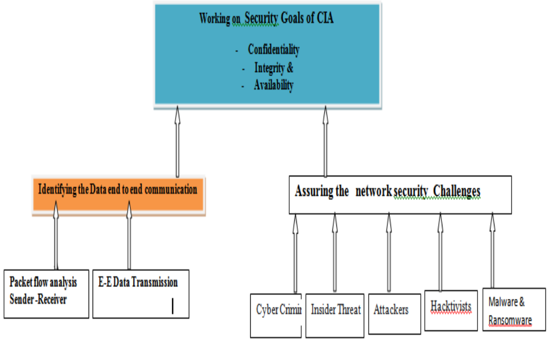

Working on Security Goals of CIA
- Confidentiality
- Integrity &
- Availability
Identifying the Data end to end communication
Assuring the network security Challenges
Packet flow analysis Sender-Receiver
E-E Data Transmission
Cyber Crimi
Insider Threat
Attackers
Hacktivists
Malware & Ransomware

Fig-3- Proposed Model of cloud security on Wireless Network

3.3.1 Network Security challenges

- ✓ Mis-configuration proliferation:- Perhaps the least glamorous of all security threats, mis-configuration continues to hold a top spot as a serious network security threat.
- ✓ Many organizations focus their firewall management activities on permitting access. That often leads to too many users being granted levels of permissions that are too high. This is a dangerous mistake. In order to make the firewall a more effective security device in the network, risk must be evaluated with the same weight as access.
- ✓ Automation plays a critical role in reducing privileged access abuse by reducing the accidental errors that lead to mis-configurations and increasing security agility

- ✓ **Tool interoperability shortcomings** is the problem isn't too many tools. The problem is too many tools that that don't share data seamlessly.
- ✓ A network is not a single zone. It's a system of software-defined networks, micro-segmentation, and network rules and assets that create exponential complexity. Security analytics platforms make data more accessible to more people so it can be consumed and analyzed efficiently.
- ✓ Visibility changes from moment to moment as new devices and endpoints join and leave the network. Typically, there is no way to tell if the network is secure or compliant at any given point in time – at best, security professionals can look back over historical data to tell if the network had been secure at some point in the past.
- ✓ **Controls that are out of step with infrastructure changes** Security teams are not able to keep up with ever-increasing volumes of vulnerabilities that need to be patched, new applications that need to be tested and deployed, emerging threats that need to be mitigated and, of course, access requests that must be granted, returned for further authentication, or denied.[16], [17]

3.3.2 End to end data flow communication

TCP is a transport level protocol of the Internet that provides reliable, end-to-end communication between two processes. The requesting process, often known as the client, requests services from the server process. Both client and server processes are accessible on their respective machines by their TCP port numbers assigned to them. Many standard application layer services have *well-known* TCP port numbers assigned by a central authority.. [18]

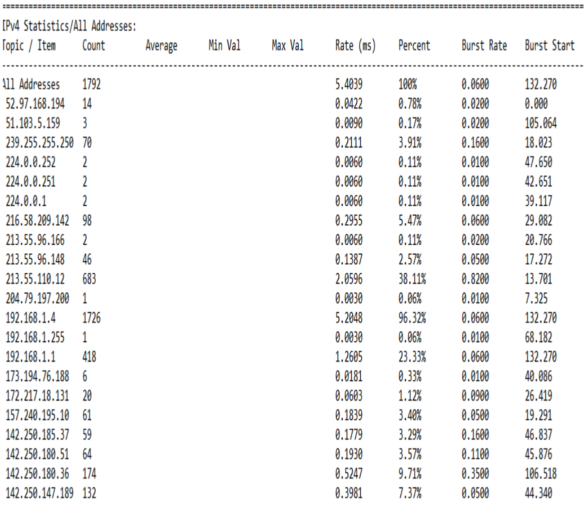
3.3.3 Working on Security Key Goals

The primary goal of network security are Confidentiality, Integrity, and Availability. These three pillars of Network Security are often represented as **CIA triangle**.[19], [20],[21]

- ✓ **Confidentiality**:- The function of confidentiality is to protect precious business data from unauthorized persons. Confidentiality part of network security makes sure that the data is available only to the intended and authorized persons.
- ✓
- ✓ **Integrity**: - This goal means maintaining and assuring the accuracy and consistency of data. The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.
- ✓ **Availability**:- The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the legitimate users, whenever they require it.

4. Demonstration and Results

4.1 The packet flow in WIFI3 on Wireshark



```
=================================================================================================================
IPv4 Statistics/All Addresses:
Topic / Item      Count         Average       Min Val       Max Val       Rate (ms)     Percent       Burst Rate    Burst Start
-----------------------------------------------------------------------------------------------------------------

All Addresses     1792                                                    5.4039        100%          0.0600        132.270
 52.97.168.194    14                                                      0.0422        0.78%         0.0200        0.000
 51.103.5.159     3                                                       0.0090        0.17%         0.0200        105.064
 239.255.255.250  70                                                      0.2111        3.91%         0.1600        18.023
 224.0.0.252      2                                                       0.0060        0.11%         0.0100        47.650
 224.0.0.251      2                                                       0.0060        0.11%         0.0100        42.651
 224.0.0.1        2                                                       0.0060        0.11%         0.0100        39.117
 216.58.209.142   98                                                      0.2955        5.47%         0.0600        29.082
 213.55.96.166    2                                                       0.0060        0.11%         0.0200        20.766
 213.55.96.148    46                                                      0.1387        2.57%         0.0500        17.272
 213.55.110.12    683                                                     2.0596        38.11%        0.8200        13.701
 204.79.197.200   1                                                       0.0030        0.06%         0.0100        7.325
 192.168.1.4      1726                                                    5.2048        96.32%        0.0600        132.270
 192.168.1.255    1                                                       0.0030        0.06%         0.0100        68.182
 192.168.1.1      418                                                     1.2605        23.33%        0.0600        132.270
 173.194.76.188   6                                                       0.0181        0.33%         0.0100        40.086
 172.217.18.131   20                                                      0.0603        1.12%         0.0900        26.419
 157.240.195.10   61                                                      0.1839        3.40%         0.0500        19.291
 142.250.185.37   59                                                      0.1779        3.29%         0.1600        46.837
 142.250.180.51   64                                                      0.1930        3.57%         0.1100        45.876
 142.250.180.36   174                                                     0.5247        9.71%         0.3500        106.518
 142.250.147.189  132                                                     0.3981        7.37%         0.0500        44.340
```

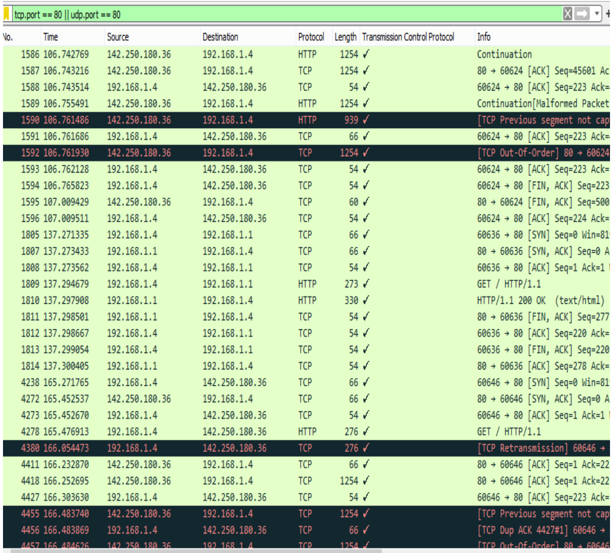
Fig-4- Statistics of Packet by IPv4

- ✓ The packet Burst is equivalent to the maximum number of packets sent per interval of time
- ✓ The Burst start means the time when the maximum number of packets sent occurred

Wireshark calculates the maximum number of packets sent per interval of time. The user is able to adjust the interval of time in 1 millisecond intervals.: The demonstration shows burst count for item rather rate if it's selected, the statistics will show the count of events within the burst window instead of a burst rate. Burst rate is calculated as the number of packets within the burst window divided by the burst window length.

- ✓ Burst rate resolution = sets the duration of the time interval into which packets are grouped when calculating the burst rate.
- ✓ Burst rate window size = sets the duration of the sliding window during which the burst rate is measured
- ✓ Burst rate resolution = Burst rate window size

4.2 TCP/IP Packet sending over the internet



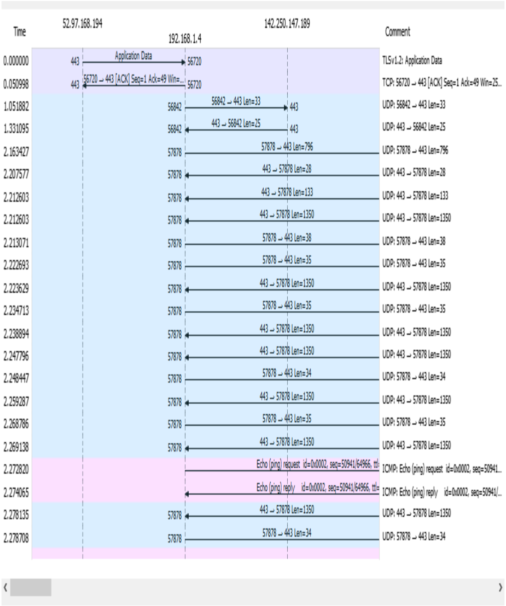
tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Transmission Control Protocol	Info
1586	106.742769	142.250.180.36	192.168.1.4	HTTP	1254	✓	Continuation
1587	106.743216	142.250.180.36	192.168.1.4	TCP	1254	✓	80 → 60624 [ACK] Seq=45601 Ac
1588	106.743514	192.168.1.4	142.250.180.36	TCP	54	✓	60624 → 80 [ACK] Seq=223 Ack=
1589	106.755491	142.250.180.36	192.168.1.4	HTTP	1254	✓	Continuation[Malformed Packet
1590	106.761486	142.250.180.36	192.168.1.4	HTTP	939	✓	[TCP Previous segment not cap
1591	106.761686	192.168.1.4	142.250.180.36	TCP	66	✓	60624 → 80 [ACK] Seq=223 Ack=
1592	106.761930	142.250.180.36	192.168.1.4	TCP	1254	✓	[TCP Out-Of-Order] 80 → 60624
1593	106.762128	192.168.1.4	142.250.180.36	TCP	54	✓	60624 → 80 [ACK] Seq=223 Ack=
1594	106.765823	192.168.1.4	142.250.180.36	TCP	54	✓	60624 → 80 [FIN, ACK] Seq=223
1595	107.009429	142.250.180.36	192.168.1.4	TCP	60	✓	80 → 60624 [FIN, ACK] Seq=500
1596	107.009511	192.168.1.4	142.250.180.36	TCP	54	✓	60624 → 80 [ACK] Seq=224 Ack=
1805	137.271335	192.168.1.4	192.168.1.1	TCP	66	✓	60636 → 80 [SYN] Seq=0 Win=81
1807	137.273433	192.168.1.1	192.168.1.4	TCP	66	✓	80 → 60636 [SYN, ACK] Seq=0 A
1808	137.273562	192.168.1.4	192.168.1.1	TCP	54	✓	60636 → 80 [ACK] Seq=1 Ack=1
1809	137.294679	192.168.1.4	192.168.1.1	HTTP	273	✓	GET / HTTP/1.1
1810	137.297908	192.168.1.1	192.168.1.4	HTTP	330	✓	HTTP/1.1 200 OK (text/html)
1811	137.298501	192.168.1.1	192.168.1.4	TCP	54	✓	80 → 60636 [FIN, ACK] Seq=277
1812	137.298667	192.168.1.4	192.168.1.1	TCP	54	✓	60636 → 80 [ACK] Seq=220 Ack=
1813	137.299054	192.168.1.4	192.168.1.1	TCP	54	✓	60636 → 80 [FIN, ACK] Seq=220
1814	137.300405	192.168.1.1	192.168.1.4	TCP	54	✓	80 → 60636 [ACK] Seq=278 Ack=
4238	165.271765	192.168.1.4	142.250.180.36	TCP	66	✓	60646 → 80 [SYN] Seq=0 Win=81
4272	165.452537	142.250.180.36	192.168.1.4	TCP	66	✓	80 → 60646 [SYN, ACK] Seq=0 A
4273	165.452670	192.168.1.4	142.250.180.36	TCP	54	✓	60646 → 80 [ACK] Seq=1 Ack=1
4278	165.476913	192.168.1.4	142.250.180.36	HTTP	276	✓	GET / HTTP/1.1
4380	166.054473	192.168.1.4	142.250.180.36	TCP	276	✓	[TCP Retransmission] 60646 →
4411	166.232870	142.250.180.36	192.168.1.4	TCP	66	✓	80 → 60646 [ACK] Seq=1 Ack=22
4418	166.252695	142.250.180.36	192.168.1.4	TCP	1254	✓	80 → 60646 [ACK] Seq=1 Ack=22
4427	166.303630	192.168.1.4	142.250.180.36	TCP	54	✓	60646 → 80 [ACK] Seq=223 Ack=
4455	166.483740	142.250.180.36	192.168.1.4	TCP	1254	✓	[TCP Previous segment not cap
4456	166.483869	192.168.1.4	142.250.180.36	TCP	66	✓	[TCP Dup ACK 4427#1] 60646 →
4457	166.484626	142.250.180.36	192.168.1.4	TCP	1254	✓	[TCP Out-Of-Order] 80 → 60646

Fig-5- TCP/IP streaming

The Transmission Control Protocol (TCP) is one of the main protocols of the Internet protocol suite. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. The scenario is tested by using wireshark simulator as mentioned on Figure Fig-5-

4.3 The Packet flow graphs by Wireshark

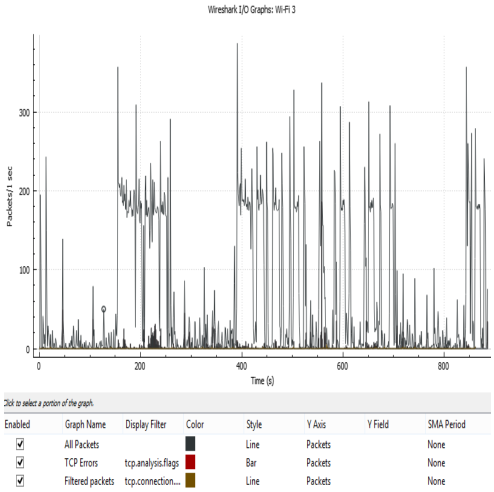


Time	Comment
0.000000	TLSv1.2: Application Data
0.050998	TCP: 56720 → 443 [ACK] Seq=1 Ack=49 Win=25...
1.051882	UDP: 56842 → 443 Len=33
1.331095	UDP: 443 → 56842 Len=25
2.163427	UDP: 57878 → 443 Len=796
2.207577	UDP: 443 → 57878 Len=28
2.212603	UDP: 443 → 57878 Len=133
2.212603	UDP: 443 → 57878 Len=1350
2.213071	UDP: 57878 → 443 Len=38
2.222693	UDP: 57878 → 443 Len=35
2.223629	UDP: 443 → 57878 Len=1350
2.234713	UDP: 57878 → 443 Len=35
2.238894	UDP: 443 → 57878 Len=1350
2.247796	UDP: 443 → 57878 Len=1350
2.248447	UDP: 57878 → 443 Len=34
2.259287	UDP: 443 → 57878 Len=1350
2.268786	UDP: 57878 → 443 Len=35
2.269138	UDP: 443 → 57878 Len=1350
2.272820	ICMP: Echo (ping) request id=0x0002, seq=50941...
2.274065	ICMP: Echo (ping) reply id=0x0002, seq=50941/...
2.278135	UDP: 443 → 57878 Len=1350
2.278708	UDP: 57878 → 443 Len=34

Fig-6- The Packet flow graphs by Wireshark

The Flow Graph window shows connections between hosts. It displays the packet time, direction, ports and comments for each captured connection. You can filter all connections by ICMP Flows, ICMPv6 Flows, UIM Flows and TCP Flows

4.4 I/O Network


Wireshark I/O Graphs: Wi-Fi 3
Packets/1 sec
300
200
100
0
0
200
400
600
800
Time (s)
Click to select a portion of the graph.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
☑	All Packets		■	Line	Packets		None
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None
☑	Filtered packets	tcp.connection....	■	Line	Packets		None

Fig-7- Wireshark IO Graphs

Wireshark IO Graphs will show you the overall traffic seen in a capture file which is usually measured in rate per second in bytes or packets (which you can always change if you prefer bits/bytes per second). In default the x-axis is the tick interval per second, and y-axis is the packets per tick (per second)

5. Conclusion

The study concluded by providing the identification and vulnerabilities of the security issues in the Wireless Fidelity(WiFi) i.e. Wireless Network. To find the challenges I have used the systematic literature review mechanisms and demonstrative tool namely Wirehark network analyzer. The tool identifies the packet flow, packet length time, data flow statistics, end- to- end the packet flow, reached and lost packets in the network and input/output packet statics graphs. Then, developed the proposed model that used to secure the Wireless network solution and prevention vulnerabilities of the network security challenges.Finally applying the model that used to investigate the security challenges and vulnerabilities of cloud computing services is the solution for the wireless network security issues

References

[1] M. Al-Zoube, S. Abou El-Seoud, and M. F. Wyne, “Cloud computing based e-learning system,” *Int. J. Distance Educ. Technol. IJDET*, vol. 8, no. 2, pp. 58–71, 2010.

[2] M. J. Kavis, *Architecting the cloud: design decisions for cloud computing service models (SaaS, PaaS, and IaaS).* John Wiley & Sons, 2014.

[3] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, 2013.

[4] J. V. Gaud and M. M. Bartere, “Data Security Based on LAN Using Distributed Firewall,” *Int. J. Comput. Sci. Mob. Comput.*, 2014.

[5] L. Hansen and H. Nissenbaum, “Digital disaster, cyber security, and the Copenhagen School,” *Int. Stud. Q.*, vol. 53, no. 4, pp. 1155–1175, 2009.

[6] N. A. Sales, “Regulating cyber-security,” *Nw UL Rev*, vol. 107, p. 1503, 2012.

[7] M. Junaid, M. Mufti, and M. U. Ilyas, “Vulnerabilities of IEEE 802.11 i wireless LAN CCMP protocol,” *Trans. Eng. Comput. Technol.*, vol. 11, pp. 228–233, 2006.

[8] J. W. Branch, N. L. Petroni, L. Van Doorn, and D. Safford, “Autonomic 802.11 wireless LAN security auditing,” *IEEE Secur. Priv.*, vol. 2, no. 3, pp. 56–65, 2004.

[9] S. Miehlke *et al.*, “Efficacy and safety of budesonide, vs mesalazine or placebo, as induction therapy for lymphocytic colitis,” *Gastroenterology*, vol. 155, no. 6, pp. 1795–1804, 2018.

[10] J.-C. Chen, M.-C. Jiang, and Y. Liu, “Wireless LAN security and IEEE 802.11 i,” *IEEE Wirel. Commun.*, vol. 12, no. 1, pp. 27–36, 2005.

[11] D. E. Denning and P. J. Denning, “Data security,” *ACM Comput. Surv. CSUR*, vol. 11, no. 3, pp. 227–249, 1979.

[12] J. V. Gaud and M. B. Mahip, “Data security based on LAN using distributed firewalls,” *Int. J. Comput. Sci. Mob. Comput.*, 2014.

[13] U. Lamping and E. Warnicke, “Wireshark user’s guide,” *Interface*, vol. 4, no. 6, p. 1, 2004.

[14] P. Zhang and K. Xia, “Custom Protocol Analysis Based on Wireshark”.

[15] B. P. Miller, “Vulnerability assessment of open source wireshark and chrome browser,” WISCONSIN UNIV MADISON, 2013.

[16] “3.3.1. Network Security challenges - Barbaadachiisaa Google.” https://www.google.com/search? (accessed Sep. 08, 2021).

[17] “Network Security Challenges & Threats | Vital IT Security Issues.” https://www.firemon.com/network-security-threats-challenges/ (accessed Sep. 08, 2021).

[18] “End to End Communication - an overview | ScienceDirect Topics.” https://www.sciencedirect.com/topics/computer-science/end-to-end-communication (accessed Sep. 08, 2021).

[19] “Network Security â Overview.” https://www.tutorialspoint.com/network_security/network_security_overview.htm (accessed Sep. 08, 2021).

[20] C. H. Sandeep, V. Thirupathi, P. Pramod kumar, and S. Naresh kumar, “Goals and Model of Network Security,”

Int. J. Adv. Sci. Technol., vol. 28, no. 20, pp. 593–599, 2019.

[21] I. A. Sumra, H. B. Hasbullah, and J. B. AbManan, "Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey," in *Vehicular Ad-Hoc Networks for Smart Cities*, Springer, 2015, pp. 51–61.