A MODEL TO INVESTIGATE THE SECURITY CHALLENGES AND VULNERABILITIES OF CLOUD COMPUTING SERVICES IN WIRELESS NETWORKS

By

Desta Dana Data*

Assistant Professor in Information Technology,

Department of Information Technology, School of Informatics, Wolaita Sodo University,

Ethiopia, P.O. Box 138

Email: destadanedata@wsu.edu.et

Abstract:

This study identifying networks security challenges and vulnerabilities of cloud computing services by using wireless networks. To achieve this, I have used various methods that includes reviewed different related works on network challenges in wired or wireless network by using Systematic literature review(SLR), analysis packet flow by using network analyzer tool, data from practical demonstration identifies the packet flow, packet length time, data flow statistics, end-to-end packet flow, reached or lost packets in the network, and input or output packet statistics graphs, and SPSS tool to interpret the data that imported from Wireshark analyzer by .CSV file.

Then, finally the study identifies the data end-to-end data communication streams, and the security challenges (Cybercrime, insider threat, attackers, hacktivists, malware, and Ransomware). Lastly, I have developed the proposed model that is used to secure the Wireless network solution and prevent vulnerabilities of the network security challenges and, applying the developed model to identify and investigate the security challenges and vulnerabilities of cloud computing services I the wireless network.

Keywords:-*Cloud Computing, Cyber security, Network Security, Security challenges, Wireless Network,*

1. Introduction

An 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.(Al-Zoube et al., 2010a)

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 network challenges which includes cybercrime, insider attacks, attackers, hactivist, malwares and Ransomware.

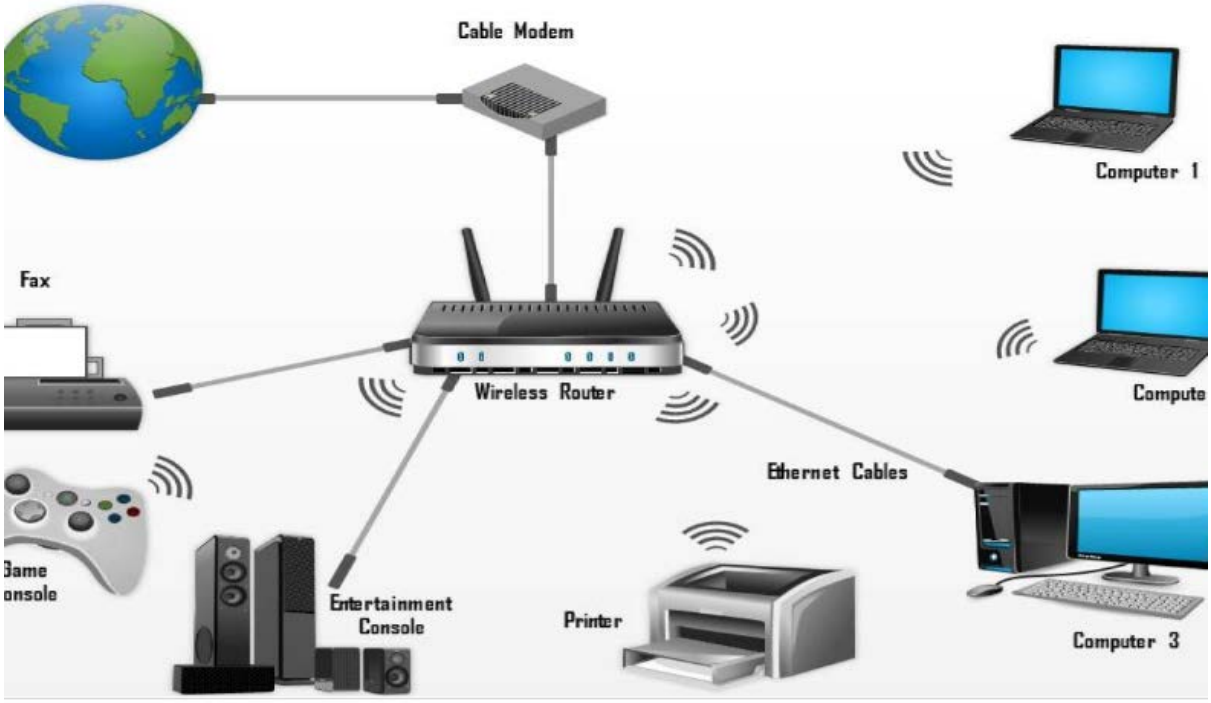

Fig.1. wireless network and cloud services:(Kavis, 2014)

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 issue related with the protection which includes systems security, network

security and application and information security. In this study, I have investigated 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.

In the 21st century the world is under risks of cyber security problems in different countries are complying in case of the crimes.

In 2020GC. FDRE Government of Ethiopia Published and launched the working regulation to combat and fight the challenges and crimes of the cybercrimes.[22] Different Activists attackers and malware are strongly working the bounder less fight between different sovereign states and societies.

The country's privately owned critical infrastructure like 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 scholars need not run in such established channels.(Von Solms & Van Niekerk, 2013),(Gaud & Bartere, 2014),(Hansen & Nissenbaum, 2009),(Sales, 2012).

There are many challenges and problems in the security of wireless networking includes Ransomware, malwares, cyber Criminals, Hacktivists, attackers and insider threat

1.1. Research Questions

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

ii. What is the suitable model to detect the security challenges cloud services?

1.2. Related Studies

1.2a. Vulnerabilities of IEEE 802.11i Wireless 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 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.(Junaid et al., 2006)

CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. (Branch et al., 2004),(Miehlke et al., 2018)

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.(Chen et al., 2005), (Denning & Denning, 1979), (Gaud & Bartere, 2014)

1.2b. DATA SECURITY BASED ON LAN USING 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.(Gaud & Bartere, 2014),(Gaud & Mahip, 2014)

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 provides the investigations model on Wireless Network which used to identifies the level of vulnerabilities and provide the solution.

1.2c. Application of SNORT and Wireshark in Network Traffic Analysis

The researcher study focus on a Network Intrusion Detection System properties of SNORT which is used for intrusion detection by making use of predefined rules and alerting the user

by directing alert messages. The SNORT tool creates log file that entails data packets along with their alert messages. The recorded log file is then exported to Wireshark so as to examine the captured data packets. This Wireshark tool generates each detail about the packets of the log file. It provides minute details about frames, internet protocols, Ethernet, protocol hierarchy etc. An I/O graph outlined the flow of the packet which demonstrations the total traffic which is further measured in either bytes or packets per second. The researcher focused on the intrusion Detection systems by using Wireshark simulator. (Jain & Anubha, 2021)

1.2d. Technical Challenges in Vehicular Ad hoc Networks (VANET) (Raw et al., 2013)

I. Network Management: Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can't use structures like tree because these structures can't be set up and maintained as rapidly as the topology changed.

II. Congestion and collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

III. Environmental Impact: VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.

IV. MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based Mac for VANET.

V. Security: As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied.

2. Objectives

To conduct my research work, I have proposed three main objectives for this work

1. To investigate the vulnerabilities of the threat in Wireless Network by Wireshark tool
2. Analyze the data by using SPSS software
3. To develop model that used to identify, measure and detect security problems.

3. Methodology

3.1. Statistical Package for the Social Sciences (SPSS)

Statistical Package for the Social Sciences (SPSS) is used by various kinds of researchers for complex statistical data. It used after retrieving data by Wireshark Network analyzer; I have use to identify the statistical data analyzer tools. So, SPSS is the tools use in this project to identify more frequently displayed numeric data in the Wireshark.

3.2. Systematic Literature Review (SLR)

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.

SLR is a methodology that identifies, 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.

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

- ✓ SLR directly addresses the specified research questions by utilizing a review protocol
- ✓ SLR creates a search strategy that targets and detects all of the relevant literature as possible
- ✓ SLR would require criteria of inclusion and exclusion to assess the viability of each primary study. The systematic literature review will be conducted in three main phases

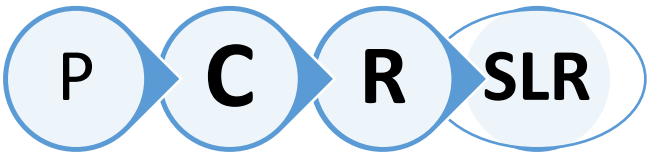

Fig.2: Systematic literature review(SLR) Steps

- ✓ **P(Planning) the systematic literature review**- Developing review protocol
- ✓ **C(Conducting) the review**- Selecting primary study, extracting data and assessing quality of data
- ✓ **R(Reporting) the review**- Reporting the whole review holistically and documenting the systematic literature review process

3.3. Wireshark Demonstration tool

The world most 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. (Lamping & Warnicke, 2004),(Zhang & Xia, n.d.), [15]

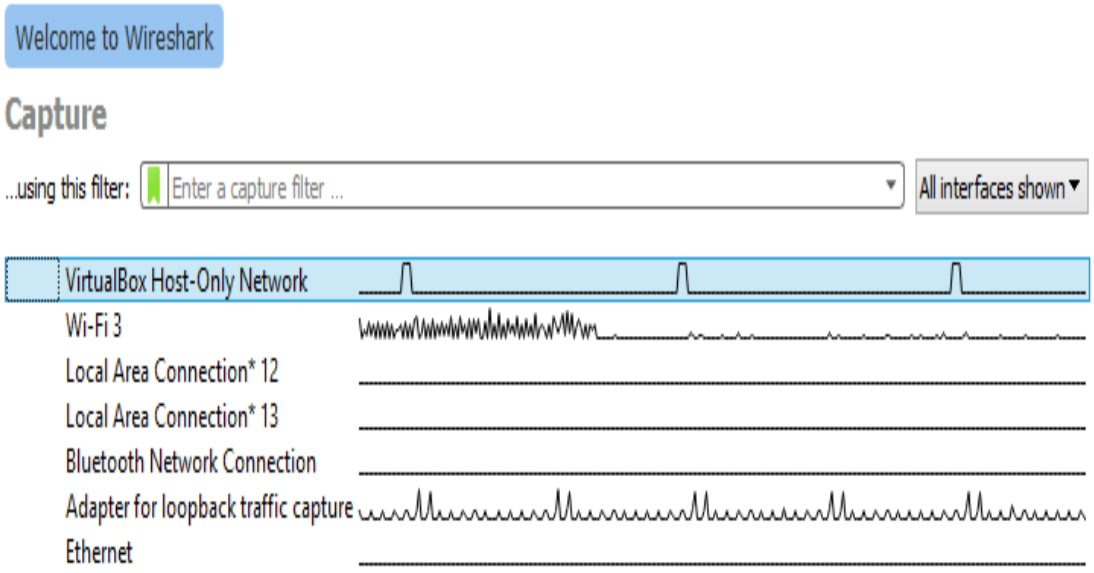

Fig-3- Wireshark Interface

3.4. Proposed model of Cloud security on Wireless Networking

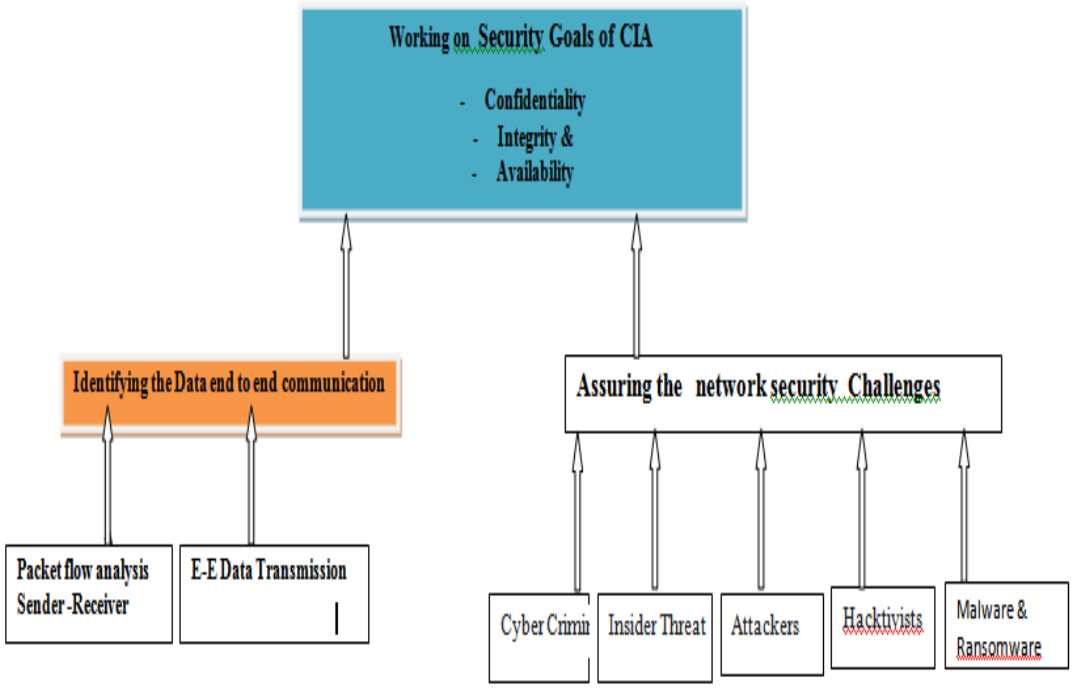

Fig-4- Proposed Model of cloud security on Wireless Network

3.4a. Network Security challenges

People are focus on 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 invalid configuration and increasing security.

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. (Maxa et al., 2017) , (Ren et al., 2012)

3.4b. 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 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.

3.4c. Working on Security Key Goals

The primary goal of network security are Confidentiality, Integrity, and Availability. These three pillars of Network Security goals **CIA** described in below, (Lundgren & Möller, 2019), (Sumra et al., 2015a) (Sandeep et al., 2019),(Sumra et al., 2015b), (Nweke, 2017)

I. **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.

II. **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.

III. **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. Results an Discussion

By using Wireshark network analyzer I have demonstrated the network packet flow on WIFI Network of 2MBPS bandwidth, and SPSS tool to analyze details in statistically. The results are clearly mentioned under below by using different figures and interpretations.

4.1. Packet Flow Statistics by Wireshark analyzer

In the diagram below (Fig.5) the packet burst rate and burst start described. In the study burst rate the maximum number of packets sent per interval of time and burst start the time when the maximum number of packets sent occurred. (Ota et al., 1994), (Trabelsi & Zeidan, 2012)

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-5- Statistics of Packet flow by IPv4(Wireshark anlyzer result)

4.2. The packet flow in Analysis By Using SPSS

A packet Burst is equivalent to the maximum number of packets sent per interval of time and 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 and 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.

✓ BRR(Burst rate resolution) = sets the duration of the time interval into which packets are grouped when calculating the burst rate.

✓ BRW(Burst rate window size) = sets the duration of the sliding window during which the burst rate is measured

BRR= BRW----------(1)

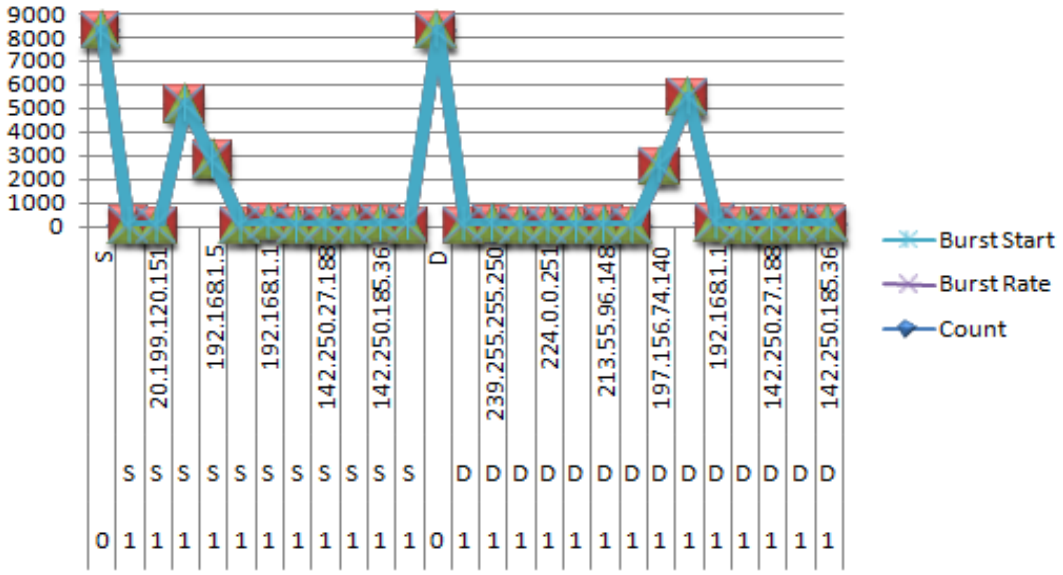

Fig-6- Packet Burst/end-to-end flow/ by using SPSS data

From Above Charts the S (Source) and D (Destination) The package flow in the given IP intervals from both sides. The packet that sent received has counted on the left corners of the diagram in above. In the diagram on above the maximum packet count is 9000 and the minimum is 0 in the specified IPv4s. In short, the burst rate is the time intervals that a packet initiated from senders and arrived on receivers as well as the confirmation or acknowledgement messages come from receiver and arrived to source.

The initial messages created are 0 hop and the next receiver got the sent messages at 1 hop.

4.3. TCP/IP Packet sending over the internet

Packet flow can be defined as a traffic stream between a source (IP and port) and a destination (IP and port) over a specific protocol. When a user tries to connect their system to a network, connections are created to facilitate the transfer. Several connections can result in several flows. In fig.7 below the packet source that means initiated and started and the packet which sent or destinations well noticed by using Wireshark analyzer. In the TCP port 80 each packet clearly sent and received the information of ACK(acknowledgment) color is green, the packet that sent, but not reached or the response ACK not received is red/black color in the diagram below.

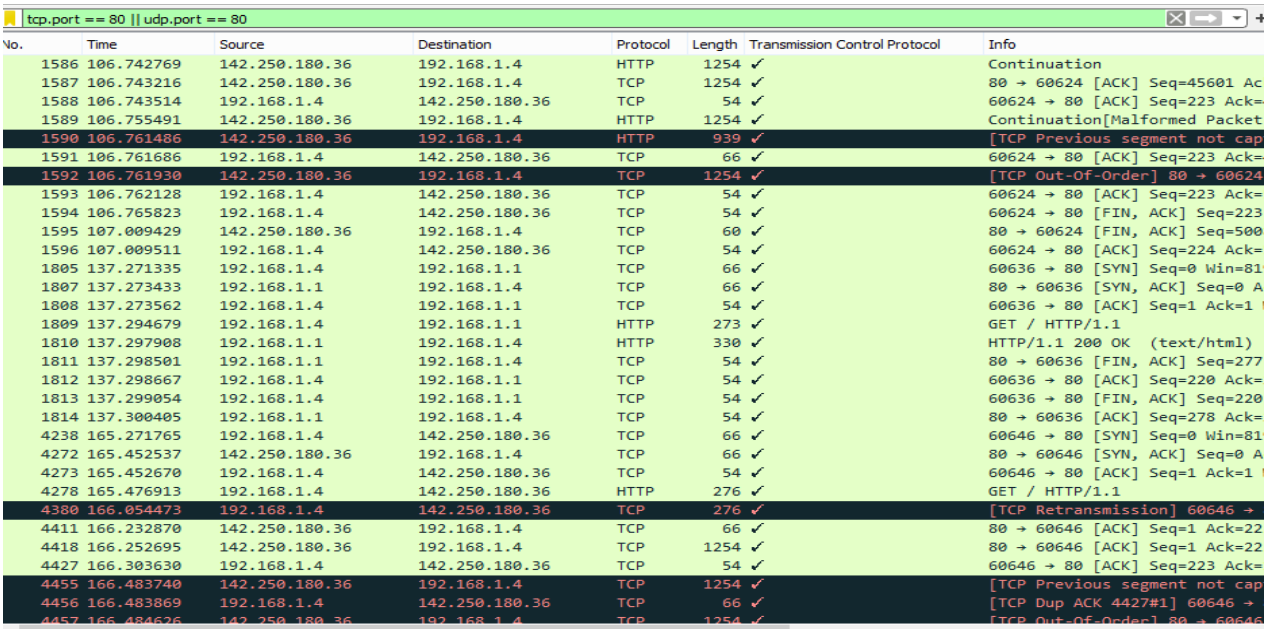

Fig-7- TCP/IP streaming from Wireshark analyzer tool

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. TCP/IP packet streams through network gateways and TCP/IP is considered to be a long stream of data that is transmitted from one end of the connection to the other end, and another long stream of data flowing in the opposite direction.(Samain et al., 2017), (Oliver-Balsalobre et al., 2017)

4.4. The Packet flow graph

In Fig-8- below network packets sent and received analyzed by Wireshark network analyzer data is collected and analyzed by using SPSS tool.(Kim et al., 2006) The data exported by

.CSV file formats and imported into the systems. The diagram represented by using X-Y formats of packet BPS (bandwidth Per Seconds) and length of time intervals simultaneously.

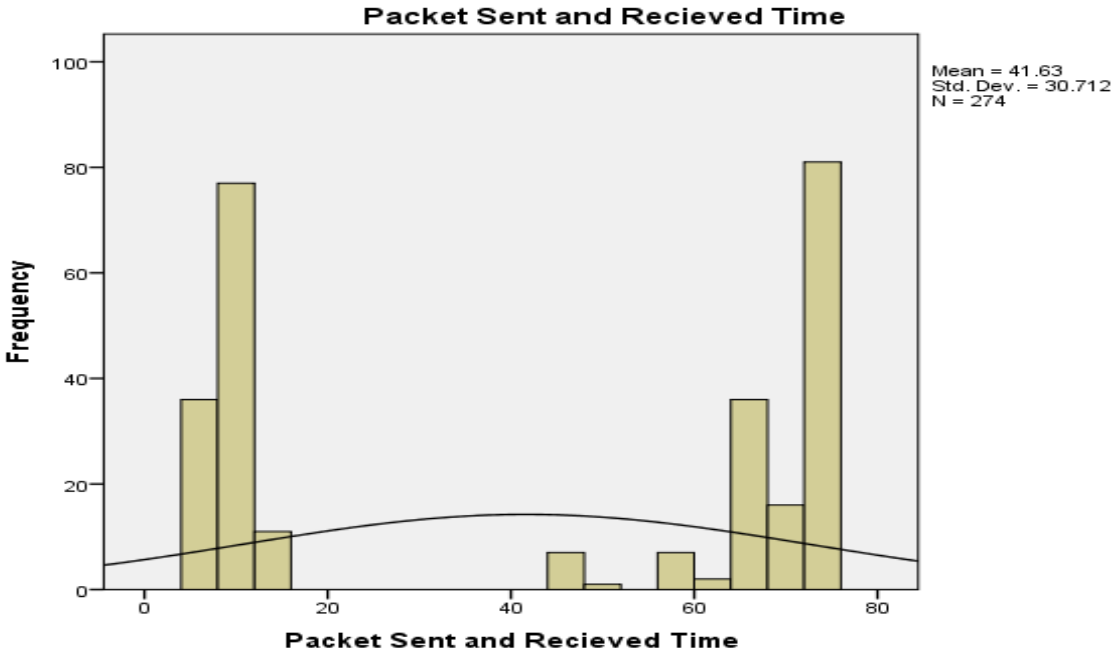

Fig-8- The Packet flow on Source that Sent and Received [SPSS Results]

4.5. Packet streaming

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. In Fig. 8. Below The packet can screen by filtering different protocols that mentioned on the diagram.(Sanders, 2017)

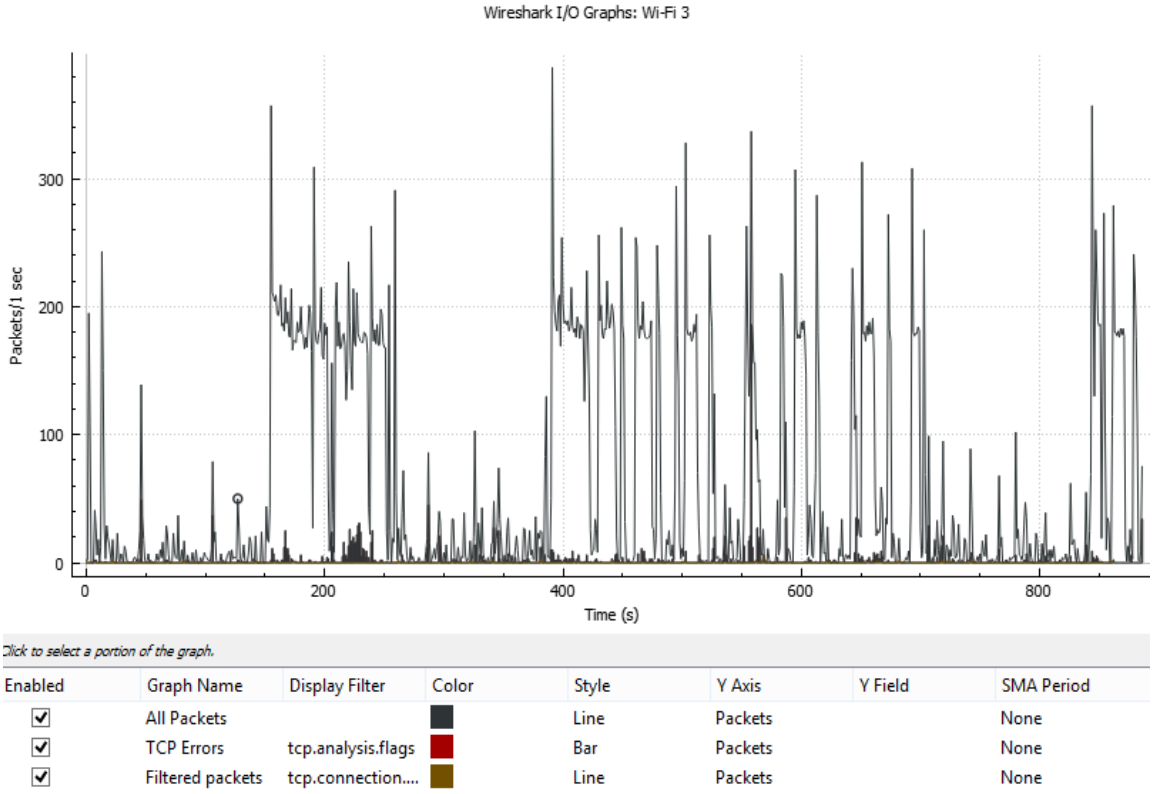

Fig-9- Incoming and Outgoing packets

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)(Majidha Fathima , Santhiyakumari, 2021)

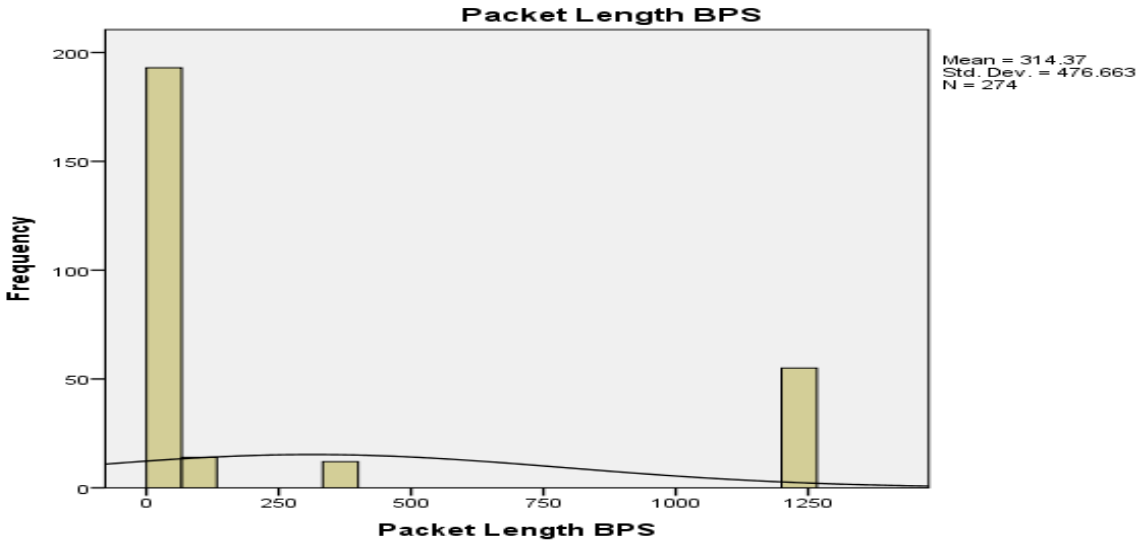

Fig-10- The average Packet flow in Bit per Second (BPS) by Using SPSS result

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 the Wireshark network analyzer. The tools identify 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, developed the proposed model that was used to secure the Wireless network solution and prevent 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

6. References

Al-Zoube, M., Abou El-Seoud, S., & Wyne, M. F. (2010a). Cloud computing based e-learning system. *International Journal of Distance Education Technologies (IJDET)*, *8*(2), 58–71.

DOI:- https://doi.org/10.4018/jdet.2010040105

Branch, J. W., Petroni, N. L., Van Doorn, L., & Safford, D. (2004). Autonomic 802.11 wireless LAN security auditing. *IEEE Security & Privacy*, *2*(3), 56–65.

DOI: http://doi.org/10.1109/MSP.2004.4

Chen, J.-C., Jiang, M.-C., & Liu, Y. (2005). Wireless LAN security and IEEE 802.11 i. *IEEE Wireless Communications*, *12*(1), 27–36.

DOI- https://doi.org/10.1145/356778.356782

Denning, D. E., & Denning, P. J. (1979). Data security. *ACM Computing Surveys (CSUR)*, *11*(3), 227–249. DOI:- http://doi.org/10.1007/978-3-642-22540-6_10

Gaud, J. V., & Bartere, M. M. (2014). Data Security Based on LAN Using Distributed Firewall. *International Journal of Computer Science and Mobile Computing*.

DOI:- http://doi.org/10.47760/ijcsmc

Gaud, J. V., & Mahip, M. B. (2014). Data security based on LAN using distributed firewalls. *International Journal of Computer Science and Mobile Computing*.

DOI:- http://doi.org/10.47760/ijcsmc

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

DOI:- http://doi.org/10.1111/j.1468-2478.2009.00572.x

Jain, G. & Anubha. (2021). Application of SNORT and Wireshark in Network Traffic Analysis. *IOP Conference Series: Materials Science and Engineering*, *1119*(1), 012007.

DOI:- https://doi.org/10.1088/1757-899X/1119/1/012007

Junaid, M., Mufti, M., & Ilyas, M. U. (2006). Vulnerabilities of IEEE 802.11 i wireless LAN CCMP protocol. *Transactions on Engineering, Computing and Technology*, *11*, 228–233.

DOI:- doi.org/10.5281/zenodo.1333294

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

Kim, Y., Lau, W. C., Chuah, M. C., & Chao, H. J. (2006). PacketScore: A statistics-based packet filtering scheme against distributed denial-of-service attacks. *IEEE Transactions on Dependable and Secure Computing*, *3*(2), 141–155.

DOI: https://doi.org/10.1109/TDSC.2006.25

Lamping, U., & Warnicke, E. (2004). Wireshark user's guide. *Interface*, *4*(6), 1.

Lundgren, B., & Möller, N. (2019). Defining information security. *Science and Engineering Ethics*, *25*(2), 419–441. DOI: https://doi.org/10.1007/s11948-017-9992-1

Majidha Fathima, K. M., & Santhiyakumari, N. (2021). A Survey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap. *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, 1136–1141.

DOI:- https://doi.org/10.1109/ICAIS50930.2021.9395852

Miehlke, S., Aust, D., Mihaly, E., Armerding, P., Böhm, G., Bonderup, O., Fernández-Bañares, F., Kupcinskas, J., Munck, L. K., & Rehbehn, K.-U. (2018). Efficacy and

safety of budesonide, vs mesalazine or placebo, as induction therapy for lymphocytic colitis. *Gastroenterology*, *155*(6), 1795–1804.

Nweke, L. O. (2017). Using the CIA and AAA models to explain cybersecurity activities. *PM World Journal*, *6*, 1–2.

Ota, Y., Swartz, R. G., Archer, V. D., Korotky, S. K., Banu, M., & Dunlop, A. E. (1994). High-speed, burst-mode, packet-capable optical receiver and instantaneous clock recovery for optical bus operation. *Journal of Lightwave Technology*, *12*(2), 325–331.

Raw, R. S., Kumar, M., & Singh, N. (2013). Security challenges, issues and their solutions for VANET. *International Journal of Network Security & Its Applications*, *5*(5), 95.

DOI:- https://doi.org/10.5121/IJNSA.2013.5508

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing*, *16*(1), 69–73.

DOI:- https://doi.org/10.1109/MIC.2012.14

Sales, N. A. (2012). Regulating cyber-security. *Nw. UL Rev.*, *107*, 1503.

Samain, J., Carofiglio, G., Muscariello, L., Papalini, M., Sardara, M., Tortelli, M., & Rossi, D. (2017). Dynamic adaptive video streaming: Towards a systematic comparison of ICN and TCP/IP. *IEEE Transactions on Multimedia*, *19*(10), 2166–2181.

Sandeep, C. H., Thirupathi, V., Pramod kumar, P., & Naresh kumar, S. (2019). Goals and Model of Network Security. *International Journal of Advanced Science and Technology*, *28*(20), 593–599.

Sanders, C. (2017). *Practical Packet Analysis, 3E: Using Wireshark to Solve Real-World Network Problems*. No Starch Press.

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

Trabelsi, Z., & Zeidan, S. (2012). Multilevel early packet filtering technique based on traffic statistics and splay trees for firewall performance improvement. *2012 IEEE International Conference on Communications (ICC)*, 1074–1078.

DOI: https://doi.org/10.1109/ICC.2012.6364218

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

DOI:- https://doi.org/10.1016/j.cose.2013.04.004

Zhang, P., & Xia, K. (n.d.). *Custom Protocol Analysis Based on Wireshark*.

Conflict of interest:

I declared **this research on date January 29, 2022 GC**. The research entitled "A MODEL TO INVESTIGATE THE SECURITY CHALLENGES AND VULNERABILITIES OF CLOUD COMPUTING SERVICES IN WIRELESS NETWORKS" I have no conflict of interest. And this research is sole published by Desta Dana Data

Author: Information

- ✓ Name: DESTA DANA DATA
- ✓ Graduated on B.Sc. and M.Sc. in Information Technology from Jimma University and Wolaita Sodo University respectively in Ethiopia
- ✓ Thesis Work: Modelling Network Optimization to improve QoS in LAN
- ✓ Academic Rank: Assistant Professor in Information Technology, Wolaita Sodo University
- ✓ ORCID: https://orcid.org/0000-0001-8111-8462