EasyChair Preprint

№ 10096

Techniques for Detecting and Preventing IP Sniffing Amplification Attacks

Mohammad Tabrez Quasim and Mohammed Amer Alasiri

May 12, 2023

Techniques for Detecting and Preventing IP Sniffing Amplification Attacks

Mohammad Tabrez Quasim, Mohammed Amer Alasiri

University of Bisha, Saudi Arabia

ABSTRACT

Sniffing attack in context of network security, corresponds to theft or interception of data by capturing the network traffic using a packet sniffer (an application aimed at capturing network packets). When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer. Using a sniffer application, an attacker can analyze the network and gain information to eventually cause the network to crash or to become corrupted, or read the communications happening across the network.

Sniffing attacks can be compared to tapping of phone wires and get to know about the conversation, and for this reason, it is also referred as wiretapping applied to computer networks. Using sniffing tools, attackers can sniff sensitive information from a network, including Email traffic (SMTP, POP, IMAP traffic), Web traffic (HTTP), FTP traffic (Telnet authentication, FTP Passwords, SMB, NFS) and many more. The packet sniffer usually sniffs the network data without making any modifications in the network's packets. Packet sniffers can just watch, display, and log the traffic, and this information can be accessed by the attacker.

To prevent networks from sniffing attacks, organizations and individual users should keep away from applications that are using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted. If required, VPN (Virtual Private Networks) can be used to provide secure access to users. Our project will discuss this issue by discussing Techniques for Detecting and Preventing IP Sniffing amplification Attacks.

1. INTRODUCTION

Sniffing in general terms refers to investigate something covertly in order to find confidential information. From an information security perspective, sniffing refers to tapping the traffic or routing the traffic to a target where it can be captured, analyzed, and monitored. Sniffing is usually performed to analyze network usage, troubleshooting network issues, monitoring the session for development and testing purposes. Since we have understood what basically sniffing is, let's move on to know how it can be used to perform attacks.

By the end of this, you will be able to understand what is Sniffing attack and its role in extracting meaningful insights from the complex and large sets of data all around us. To get in-depth knowledge of Ethical Hacking, you can enroll for a live ethical hacking course by OnlineITGuru with 24/7 support and lifetime access.

Remember back in some movies, law agencies, and criminals used to bug the telephone lines in order to hear the calls that a person receives in order to get some information. This is a perfect example of sniffing attacks. This technology can be used to test the telephone lines and determine the quality of the call but criminals used it for their own illegitimate purpose. In the world of internet, sniffing can be performed using an application, hardware devices at both the network and host level. Any network packet having information in plain text can be intercepted and read by the attackers. This information can be usernames, passwords, secret codes, banking details, or any information which is of value to the attacker. This attack is just the technical equivalent of a physical spy.

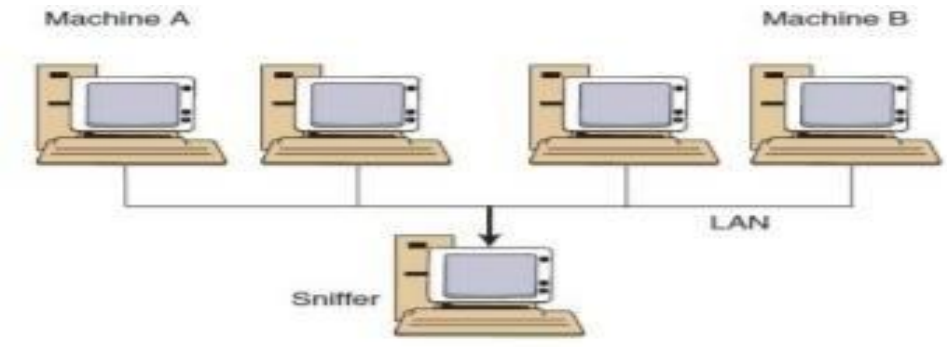


Fig.1 Sniffing attack

2. Context and Preliminary Investigation

Normally, a computer only looks at packets addressed to it and ignores the rest of the traffic on the network. But when a packet sniffer is set up on a computer, the sniffer's network interface is set to promiscuous mode. This means that it is looking at everything that comes through. Packets that contain targeted data are copied onto the hard disk as they pass through. These copies can then be analyzed carefully for specific information or patterns. Once the pattern is recognized the encryption key becomes known to the sniffer and the cipher text can be decrypted. Thus, inspite of cryptographic encryptions, the fact that the pattern from all the collected packets was recognized can lead to data theft (both ethical and unethical).

Packet sniffing can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. However, it is largely an internal threat in most organizations. In sniffing, a malicious third party may be able to eavesdrop as well as manipulate sensitive data during communication between machines in a LAN. Packet sniffing tools, which are powerful software’s, can prove to be devastating hacking tools. Even worse, these are freely available on the Internet. Some examples include Dsniff and ScoopLM. Businesses are switching ageing hubs with new switches. However, packet sniffing in a switched environment, though more challenging than in a non-switched environment, is also possible. To combat this problem, our paper proposes to use the concept of fake packets along with the existing ciphers.

3. Literature survey

P.Anu presented Generally Malicious users that make use of different attacks at different levels to steal different level of data. Some of the sniffing attacks that can be used in different levels of networking/transmission are Media Access Control (MAC) Flooding, Dynamic Host Configuration Protocol (DHCP) Attacks, DHCP Starvation Attack, Rogue DHCP Server Attack, Address Resolution Protocol (ARP) Spoofing, MAC spoofing and Domain Name Server (DNS) Poisoning. In this paper, a comparative study has been done with the above mentioned sniffing attacks and the level of recovery that can be done with each sniffing attack. Sniffer is not only used for hacking purpose but also it is used for network traffic analysis, packet/traffic monitoring, troubleshooting and other useful purposes. Packet sniffers can be used in intrusion detection. There exist some tools also that can be used for intrusion detection. Packet sniffing is a technique through which an intrusion can be created and through which an intrusion can be detected [2-7].

Ibrahim Ali et al., presented analysis tools of data traffic is becoming an important factor to increase an overall system and network security by avoiding external attackers and monitoring abuse of the IT assets by employees in the workplace. The techniques that used for collecting and converting data to a readable format are called packet sniffing. Packet Sniffer is a tool that used to capture packets in binary format, converts that binary data into a readable data format and log of that captured data for analyzing and monitoring, displaying different used applications, cleartext user names, passwords, and other vulnerabilities. this paper may be considered as an insight for the new researchers to guide them to an overview, essentials, and understanding of the packet sniffing techniques and their working [7-20].

Pallavi Asrodia introduced a tool which is developed to remove deficiency of existing tool. By using this packet sniffer we can capture traffic as well as we analyzed capture traffic. We can generate reports on the basis of analyzed traffic. Many protocol like TCP, IP, UDP etc. are implemented and filtering on basis of protocol is also done. Alerts generated on the occurring of suspected activities [20-30].

Praful Saxena presented Packet sniffing is important in network monitoring to watch network activities which help network administrators to find out weakness of network. This paper focuses

on sniffing network traffic working in different environment. Working of Network sniffing tool Wireshark .By using this packet sniffer we can capture traffic as well as we analyzed capture traffic. We can generate reports on the basis of analyzed traffic. Many protocol like TCP, IP, UDP etc. are implemented and filtering on basis of protocol is also done. Alerts generated on the occurring of suspected activities [30-35].

B. Prabadevi Presented ARP sniffing causes poisoning of ARP cache or spoofing. Through ARP sniffing, the attacker tries to know the (IP, MAC) pair of victim's system available in ARP table or ARP request-reply packet passed over the network and either exploits victim's resources or creates a situation to deny victim's services for its legitimate users. This in-turn causes MITM, DoS or DDoS attacks. The major cause for these attacks is lack of effective authentication mechanisms with ARP or RARP protocols used for address resolution. This paper provides the working principle of ARP protocol and a method to mitigate the attacks caused by ARP cache poisoning. The proposed framework compares the IP-MAC pair in the ARP and Ethernet headers and if any fake entry is suspected, the information is updated in the fake list and a message is sent to the gateway or router to alert it from cache poisoning attacks [36-40].

Pallavi Asrodia introduced the development and popularization of network Technology, the management, maintenance and monitoring of network is Important to keep the network smooth and improve Economic efficiency. For this purpose packet sniffer is used. Packet sniffing is important in network monitoring to troubleshoot and to log network activities which will benefit both the network Software engineers and network administrators There are various packet sniffers are available in market by which we can perform packet sniffing. This paper focuses on the basics of packet sniffer; it's working Principle and various packets sniffing tools their working and their capabilities for network monitoring and analysis [41-50].

Anubhi explained a comprehensive review of sniffing attacks, its type, sniffing tools and techniques, online adaptation problem, Scatter net scheme based on sniff mode, sniff project, Wi-Fi sniffing program and other related techniques. Numerous research papers explored for this purpose. Reviewing process also focused on security measures which are applied during the flow of information between client and server. To explore the gap in present area, overcome issues related to sniffing attacks are also discussed in the research paper [51-60].

4. Analysis

4.1 Sniffing Motives:

- Getting username a passwords
- Stealing bank-related/transaction-related information
- Spying on email and chat messages
- Identity theft

4.2 Types of Sniffing

There are two types of sniffing- active and passive. As the name suggests, active involves some activity or interaction by the attacker in order to gain information. In passive the attacker is just hiding dormant and getting the information. Let's discuss passive sniffing first.

4.2.1 Passive Sniffing:

This kind of sniffing occurs at the hub. A hub is a device that received the traffic on one port and then retransmits that traffic on all other ports. It does not take into account that the traffic is not meant for other destinations. In this case, if a sniffer device is placed at the hub then all the network traffic can be directly captured by the sniffer. The sniffer can sit there undetected for a long time and spy on the network. Since hubs are not used these days much, this kind of attack will be an old-school trick to perform. Hubs are being replaced by switches and that is where active sniffing comes into the picture.

4.2.2 Active Sniffing:

In a nutshell, a switch learns a CAM table that has the mac addresses of the destinations. Basis this table the switch is able to decide what network packet is to be sent where. Inactive sniffing, the sniffer will flood the switch with bogus requests so that the CAM table gets full. Once the CAM is full the switch will act as a switch and send the network traffic to all ports. Now, this is legitimate traffic that gets distributed to all the ports. This way the attacker can sniff the traffic from the switch.

4.2.3 Types of sniffing attacks

- **MAC flooding:**

Flooding the switch with MAC addresses so that the CAM table is overflowed and sniffing can be done.

- **DNS Cache Poisoning:**

Altering the DNS cache records so that it redirects the request to a malicious website where the attacker can capture the traffic. The malicious website may be a genuine-looking website which has been set up by the attacker so that the victims trust the website. The user may enter the login details and they are sniffed right away.

- **Evil Twin Attack:**

The attacker uses malicious software to change the DNS of the victim. The attacker has a twin DNS set up already (evil twin), which will respond to the requests. This can be easily used to sniff the traffic and reroute it to the website that the attacker wishes.

- **MAC Spoofing:**

The attacker can gather the MAC address(s) that are being connected to the switch. The sniffing device is set with the same MAC address so that the messages that are intended for the original machine are delivered to the sniffer machine since it has the same MAC address set.

4.3 Top Sniffing tools

- **Wireshark:**

An opensource packet capturer and analyzer. It supports Windows, Linux, etc. and is a GUI based tool (alternate to Tcpdump). It used pcap to monitor and capture the packets from the network interface. The packets can be filtered basis IP, protocol, and many other parameters. The packets can be grouped or marked basis relevance. Each packet can be selected and dissected as per need.

- **dSniff:**

It is used for network analysis and password sniffing from various network protocols. It can analyze a variety of protocols (FTP, Telnet, POP, rLogin, Microsoft SMB, SNMP, IMAP, etc) for getting the information.

Microsoft network monitor: As the name suggests it is used for capturing and analyzing the network. It is used for troubleshooting the network. Some of the features of the software are

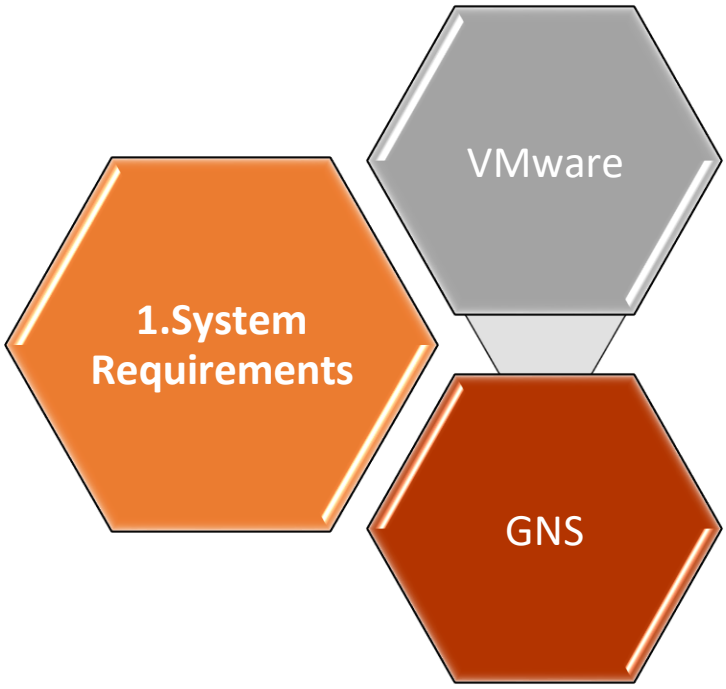
Grouping, a Large pool of protocol support(300+), Wireless monitor mode, reassembly of fragmented messages etc.

- **Debookee:**

It is a paid tool that can be used to monitor and analyze the network. It is able to intercept and analyze the traffic from devices that are in that subnet, irrespective of the device type (Laptop, devices, TV, etc). It offers various modules:

- **Network analysis module:** scan for connected devices, Intercept traffic in a subnet, TCP port scanner, Network analysis and monitoring of HTTP, DNS, TCP, DHCP protocols, Analyse VoIP calls, etc.
- **WiFi monitoring module:** Details of access points in the radio range, wireless client details, wifi statistics, etc.
- **SSL/TLS decryption module:** Support for monitoring and analyzing secured protocols.

4.4 System Requirements



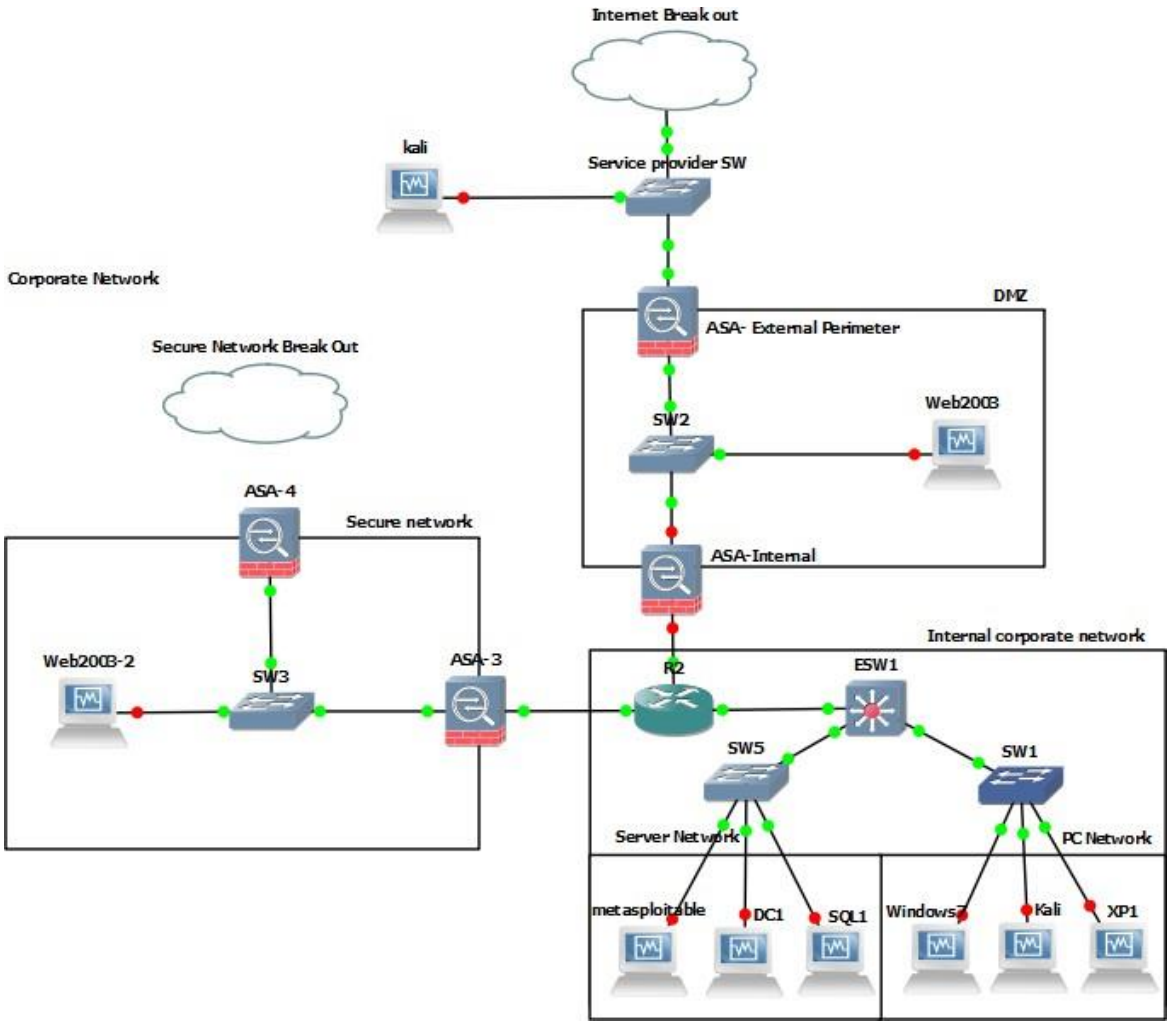
By GNS-3 the network is completely designed and with all its details on the GNS 3 program used to design networks, in addition to that, complete settings for the routers used to connect branches, as well as the switch devices used to connect devices and resources within the network, as well as the address settings used to connect the network so on this project we will use this an option to

perform our project, also VMware to create all end user devices “server, IDS/IPS, kali Linux” , and we will use GNS-3 to create our network topology “routers, switches, firewall”, then we will add the end devices into the GNS-3 network topology.

4.5 Practical Project phases

1. Network Design.
2. Configurations.
3. IP Sniffing attacks.
4. Prevention and mitigations.

5 Design


Internet Break out
kali
Service provider SW
Corporate Network
DMZ
ASA- External Perimeter
Secure Network Break Out
Web2003
SW2
ASA-4
Secure network
ASA-Internal
Internal corporate network
Web2003-2
SW3
ASA-3
R2
ESW1
SW5
SW1
Server Network
PC Network
metasploitable
DC1
SQL1
Windows7
Kali
XP1

6 References

1. Mishra[1], Vineet, et al. "Combating Packet Sniffing."
2. Anu, P., and S. Vimala. "A survey on sniffing attacks on computer networks." *2017 International Conference on Intelligent Computing and Control (I2C2)*. IEEE, 2017.
3. Diyeb, Ibrahim Ali Ibrahim, Anwar Saif, and Nagi Ali Al-Shaibany. "Ethical network surveillance using packet sniffing tools: A comparative study." *International Journal of Computer Network and Information Security* 11.7 (2018): 12.
5. Asrodia, Pallavi, and Vishal Sharma. "Network monitoring and analysis by packet sniffing method." *International Journal of Engineering Trends and Technology (IJETT)* 4.5 (2013): 2133-2135.
6. Saxena, Praful, and Sandeep Kumar Sharma. "Analysis of network traffic by using packet sniffing tool: Wireshark." *Int. J. Adv. Res. Ideas Innov. Technol* 3.6 (2017): 804-808.
7. Prabadevi, B., and N. Jeyanthi. "A framework to mitigate ARP sniffing attacks by cache poisoning." *International Journal of Advanced Intelligence Paradigms* 10.1-2 (2018): 146-159.
8. Asrodia, Pallavi, and Hemlata Patel. "Analysis of various packet sniffing tools for network monitoring and analysis." *International Journal of Electrical, Electronics and Computer Engineering* 1.1 (2012): 55-58.
9. Kulshrestha, Anubhi, and Sanjay Kumar Dubey. "A literature reviewon sniffing attacks in computernetwork." *International Journal of Advanced Engineering Research and Science (IJAERS)* 1.2 (2014).
10. Quasim, M.T. Resource Management and Task Scheduling for IoT using Mobile Edge Computing. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-09087-7
11. M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020. DOI: 10.1109/ACCESS.2020.2980739
12. M. T. Quasim, M. A. Khan, M. Abdullah, M. Meraj, S. P. Singh and P. Johri, "Internet of Things for Smart Healthcare: A Hardware Perspective," 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), Hadhramout, Yemen, 2019, pp. 1-5. DOI: 10.1109/ICOICE48418.2019.9035175
13. M. A. Khan, M. T. Quasim, F. Algarni and A. Alharthi, "Internet of Things: On the Opportunities, Applications and Open Challenges in Saudi Arabia," 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), 2020, pp. 1-5, doi: 10.1109/AECT47998.2020.9194213.
14. Aileni R.M., Suciu G. (2020) IoMT: A Blockchain Perspective. In: Khan M., Quasim M.,

Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-030-38677-1_9

15. Khan M.A., Algarni F., Quasim M.T. (2020) Decentralised Internet of Things. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-030-38677-1_1
16. Bhardwaj R., Datta D. (2020) Consensus Algorithm. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, Cham. https://doi.org/10.1007/978-3-030-38677-1_5
17. Quasim M.T., Khan M.A., Algarni F., Alshahrani M.M. (2021) Fundamentals of Smart Cities. In: Khan M.A., Algarni F., Quasim M.T. (eds) Smart Cities: A Data Analytics Perspective. Lecture Notes in Intelligent Transportation and Infrastructure. Springer, Cham. https://doi.org/10.1007/978-3-030-60922-1_1
18. Khan, M. A., Quasim, M. T., Algarni, F., & Alharthi, A. (Eds.). (2020). Decentralised Internet of Things: A blockchain perspective (Vol. 71). Springer Nature.
19. Mohammad Ayoub Khan, Mohammad Tabrez Quasim , et.al, Decentralised IoT, Decenetralised IoT: A Blockchain perspective, Springer, Studies in BigData, 2020, DOI: https://doi.org/10.1007/978-3-030-38677-1
20. Quasim M.T., Khan M.A., Algarni F., Alharthy A., Alshmrani G.M.M. (2020) Blockchain Frameworks. In: Khan M., Quasim M., Algarni F., Alharthi A. (eds) Decentralised Internet of Things. Studies in Big Data, vol 71. Springer, DOI: https://doi.org/10.1007/978-3-030-38677-1
21. M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020. DOI: 10.1109/ACCESS.2020.2980739
22. M. T. Quasim, M. A. Khan, M. Abdullah, M. Meraj, S. P. Singh and P. Johri, "Internet of Things for Smart Healthcare: A Hardware Perspective," 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), Hadhramout, Yemen, 2019, pp. 1-5. DOI: 10.1109/ICOICE48418.2019.9035175
23. Sivaram, M., Rathee, G., Rastogi, R. et al. A resilient and secure two-stage ITA and blockchain mechanism in mobile crowd sourcing. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-01800-x
24. M. T. Quasim, A. A. E. Radwan, G. M. M. Alshmrani and M. Meraj, "A Blockchain Framework for Secure Electronic Health Records in Healthcare Industry," 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, 2020, pp. 605-609, doi: 10.1109/ICSTCEE49637.2020.9277193.
25. M. Meraj, S. P. Singh, P. Johri and M. T. Quasim, "An investigation on infectious disease patterns using Internet of Things (IoT)," 2020 International Conference on Smart Technologies

in Computing, Electrical and Electronics (ICSTCEE), Bengaluru, 2020, pp. 599-604, doi: 10.1109/ICSTCEE49637.2020.9276922.

26. M. Tabrez Quasim, F. Algarni, A. Abd Elhamid Radwan and G. M. M. Alshmrani, "A Blockchain based Secured Healthcare Framework," 2020 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 2020, pp. 386-391, doi: 10.1109/ComPE49325.2020.9200024.
27. M. A. Khan, M. T. Quasim, F. Algarni and A. Alharthi, "Internet of Things: On the Opportunities, Applications and Open Challenges in Saudi Arabia," 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), Al Madinah Al Munawwarah, Saudi Arabia, 2020, pp. 1-5, doi: 10.1109/AECT47998.2020.9194213.
28. Khan, M. A, Algarni F, Quasim M.T,(2021). Smart Cities: A Data Analytics Perspective. https://doi.org/10.1007/978-3-030-60922-1. . 978-3-030-60921-4
29. M. Meraj, S. P. Singh, P. Johri and M. T. Quasim, "An investigation on infectious disease patterns using Internet of Things (IoT)," 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), 2020, pp. 599-604, doi: 10.1109/ICSTCEE49637.2020.9276922.
30. H. Alqarni, W. Alnahari and M. T. Quasim, "Internet of Things (IoT) Security Requirements: Issues Related to Sensors," 2021 National Computing Colleges Conference (NCCC), 2021, pp. 1-6, doi: 10.1109/NCCC49330.2021.9428857.
31. M. Meraj, S. A. M. Alvi, M. T. Quasim and S. W. Haidar, "A Critical Review of Detection and Prediction of Infectious Disease using IOT Sensors," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), 2021, pp. 679-684, doi: 10.1109/ICESC51422.2021.9532992.
32. W. Alnahari and M. T. Quasim, "Privacy Concerns, IoT Devices and Attacks in Smart Cities," 2021 International Congress of Advanced Technology and Engineering (ICOTEN), 2021, pp. 1-5, doi: 10.1109/ICOTEN52080.2021.9493559.
33. Meraj, M., Singh, S. P., Johri, P., & Quasim, M. T. (2021, April). Detection and Prediction of Infectious Diseases Using IoT Sensors: A Review. In Smart Computing: Proceedings of the 1st International Conference on Smart Machine Intelligence and Real-Time Computing (SmartCom 2020), 26-27 June 2020, Pauri, Garhwal, Uttarakhand, India (p. 56). CRC Press.
34. W. Alnahari and M. T. Quasim, "Authentication of IoT Device and IoT Server Using Security Key," 2021 International Congress of Advanced Technology and Engineering (ICOTEN), 2021, pp. 1-9, doi: 10.1109/ICOTEN52080.2021.9493492.
35. Mohammad Tabrez Quasim, et.al 5V'S OF BIG DATA VIA CLOUD COMPUTING: USES AND IMPORTANCE, Sci.int(Lahore),vol.31(3),PP.367-371,2019
36. Dr. Md. Tabrez Quasim and Mohammad. Meraj, Big Data Security and Privacy: A Short

Review, International Journal of Mechanical Engineering and Technology, 8(4), 2017, pp. 408-412. http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=8&IType=4

37. M.T. Quasim ,et.al . Artificial Intelligence as a Business Forecasting and Error Handling Tool. COMPUSOFT, An international journal of advanced computer technology, 4 (2), February-2015 (Volume-IV, Issue-II).
38. M.T. Quasim ,Security Issues in Distributed Database System Model , COMPUSOFT, An international journal of advanced computer technology, 2 (12), December-2013 (Volume-II, Issue-XII)
39. MA Ali, MT Quasim, MA Farah, et .al," CSTNPD: A Database for Cancer Specific Toxic Natural Products" , Indian Journal of Science and Technology, Vol 12(10), DOI: 10.17485/ijst/2019/v12i10/141396, March 20192019,
40. M.T.Quasim , An Efficient approach for concurrency control in distributed database system, Indian Streams Research Journal, 2013(Volume-3, Issue-9)
41. S. S. Kshatri, D. Singh, B. Narain, S. Bhatia, M. T. Quasim and G. R. Sinha, "An Empirical Analysis of Machine Learning Algorithms for Crime Prediction Using Stacked Generalization: An Ensemble Approach," in IEEE Access, vol. 9, pp. 67488-67500, 2021, doi: 10.1109/ACCESS.2021.3075140.
42. MT Quasim, A Shaikh, M Shuaib, A Sulaiman, S Alam, and Y Asiri, "Smart Healthcare Management Evaluation using Fuzzy Decision Making Method,"Apr. 2021, doi: 10.21203/RS.3.RS-424702/V1
43. Quasim, M. T., Alhuwaimel, S., Shaikh, A., Asiri, Y., Rajab, K. et al. (2021). An Improved Machine Learning Technique with Effective Heart Disease Prediction System. CMC-Computers, Materials & Continua, 69(3), 4169–4181.
44. Perumal, S., Tabassum, M., Narayana, G., Ponnan, S., Chakraborty, C. et al. (2021). ANN Based Novel Approach to Detect Node Failure in Wireless Sensor Network. CMC-Computers, Materials & Continua, 69(2), 1447–1462.
45. R. Farkh, H. Marouani, K. A. Jaloud, S. Alhuwaimel, M. T. Quasim et al., "Intelligent autonomous-robot control for medical applications," Computers, Materials & Continua, vol. 68, no.2, pp. 2189–2203, 2021.
46. R. Farkh, M. T. Quasim, K. Al jaloud, S. Alhuwaimel and S. T. Siddiqui, "Computer vision-control-based cnn-pid for mobile robot," Computers, Materials & Continua, vol. 68, no.1, pp. 1065–1079, 2021.
47. Meraj, M., Singh, S. P., Johri, P., & Quasim, M. T. (2021). An Analysis of Malaria Prediction through ML-Algorithms in Python and IoT Adoptability. Annals of the Romanian Society for Cell Biology, 25(6), 14098-14107.
48. Quasim, M.T., Alkhammash, E.H., Khan, M.A. et al. Emotion-based music recommendation

and classification using machine learning with IoT Framework. Soft Comput 25, 12249–12260 (2021). https://doi.org/10.1007/s00500-021-05898-9

49. Ebrahim, N. S., & Quasim, M. T. (2021). EMCSS: efficient multi-channel and time-slot scheduling. Wireless Networks, 27(4), 2879-2890.
50. Quasim, M.T., Alkhammash, E.H., Khan, M.A. et al. Emotion-based music recommendation and classification using machine learning with IoT Framework. Soft Comput 25, 12249–12260 (2021). https://doi.org/10.1007/s00500-021-05898-9
51. B.M.M. AlShahrani, Mohammad Tabrez Quasim, "Classification of Cyber-Attack using Adaboost Regression Classifier and Securing the Network", Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 10, pp. 1215-1223, 2021.
52. Mohammad Tabrez Quasim, Adel Sulaiman, Asadullah Shaikh, Mohammed Younus, " Blockchain in churn prediction based telecommunication system on climatic weather application, Sustainable Computing: Informatics and Systems" , Volume 35,2022,100705,ISSN 2210-5379, https://doi.org/10.1016/j.suscom.2022.100705.
53. Quasim, M. T. (2021). Challenges and applications of internet of things (IoT) in Saudi Arabia.
54. Meraj, M., Singh, S.P., Johri, P., Quasim, M.T.: Detection and Prediction of Infectious Diseases Using IoT Sensors: A Review (2021). arXiv:2101.02029
55. Johri, Prashant, Adarsh Anand, Juri Vain, Jagvinder Singh, and Mohammad Tabrez Quasim, eds. System Assurances: Modeling and Management. Elsevier, 2022.
56. A, Suliman and M.T.Quasim," The efficiency of a virtual lab in studying a digital logic design course using Logisim", Smart Computing , 2021, pp.18-26 .
57. AA Radwan , M.T.Quasim, "Toward semantic representation of middleware services", Smart Computing, 2021, pp. 3-10
58. Bhatia, Surbhi, Rajendra Kumar Bharti, Mohammad Tabrez Quasim, Mohammad Ayoub Khan, Meghna Chhabra, Swati Chandna, Shadab Alam, Vipin Jain, Pawan Kumar Bharti, and Beg Raj. "LSM Luggage Trolleys: Intelligent Shopping Mall Luggage Trolleys." U.S. Patent Application 17/164,845, filed June 17, 2021.
59. R. Farkh, S. Alhuwaimel, S. Alzahrani, K. Al Jaloud and M. T. Quasim, "Deep learning control for autonomous robot," Computers, Materials & Continua, vol. 72, no.2, pp. 2811–2824, 2022.
60. A. Alqazzaz, M. T. Quasim, M. M. Alshahrani, I. Alrashdi and M. A. Khan, "A deep learning model to analyse social-cyber psychological problems in youth," *Computer Systems Science and Engineering*, vol. 46, no.1, pp. 551–562, 2023.