EasyChair Preprint

№ 9538

System Penetration: Concepts, Attack Methods, and Defense Strategies

Mohammad Tabrez Quasim, Ahmed Naser Al Hawi and Mohammad Meraj

January 3, 2023

System Penetration: Concepts, Attack Methods, and Defense Strategies

Mohammad Tabrez Quasim, Ahmed Nasser Al Hawi, Mohammad Meraj
University of Bisha, Saudi Arabia
King Saud University , Saudi Arabia

ABSTRACT

Penetration testing has become an integral part of a comprehensive security program. Pen tests are conducted by ethical hackers to mimic the strategies and actions of the attacker. This complicated task is creative, and it needs you to understand your task completely.

All security problems detected are then presented to the customer together with an assessment of their impact on the system and in the corporate business scenario, also providing a technical solution for abilities mitigation. More specifically, different penetration tests using a private network, devices, and virtualized systems and tools. We predominately used tools within the Kali Linux suite. The attacks we performed included: smartphone penetration testing, hacking the phone's Bluetooth, traffic sniffing, hacking WPA Protected Wife, Man-in-the-Middle attack, spying (accessing a PC microphone), hacking the phone's Bluetooth, and hacking remote PC via IP and open ports using an advanced port scanner.

This paper investigates about different penetration testing tools in kali Linux, how to deploy it and how to make use of it to perform different types of attacks which includes methodologies and also defense strategies. Technically, we will perform different penetration tests with virtualized systems, tools and using private networks. The attacks that are performed were: Man in the middle attack and traffic spoofing and sniffing using both terminal and by Ettercap and driftnet, Bluetooth hacking, spying a webcam.

Keywords : System Penetration, Network Security , Hacking , Penetration Testing

INTRODUCTION

Penetration testing is a simulation of an attack to verify the security of a system or environment to be analyzed. This test can be performed through physical means utilizing hardware, or through social engineering. The objective of this test is to examine, under extreme circumstances, the behavior of systems, networks, or personnel devices, in order to identify their weaknesses and vulnerabilities. In terms of tools, there exist penetration testing tools which simply analyze a system, as well as ones which actually attack the system to find vulnerabilities. One may assume that penetration testing is essentially port scanning, which is not the case. To give an analogy, if a network or host system is a house, port scanning would be looking with binoculars at the doors and windows to find potential entry points. A step above that would be vulnerability assessment/management, which in this case would be sending a home inspector to the house who has a focus on security; and inspects different aspects of the house and gives critiques and suggestions as to things that could be improved upon the security analysis. Penetration testing in this scenario would be getting someone to actually try to break into the house to truly find the security faults and weak points of the house. Penetration Testing can be automated with software applications, or it can be performed manually. Either way the process includes gathering information about the target system before the test (reconnaissance), and identifying possible entry [1].

points, attempting to break in (either virtually or for real), and reporting back the findings. The main objective of penetration testing is to determine the security weaknesses. A penetration test can also be used to: 1) test an organization's security policy compliance; 2) test employee security awareness; and 3) test an organization's ability to respond to security incidents.

There are four typical types of penetration testing: external testing, internal testing, blind testing, and double blind testing. An external test targets a company's externally visible servers or devices, such as domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective in this case is to find out if an outside attacker can gain illegitimate access and what level of access can he get. An internal test simulates an inside attack behind the firewall by an authorized user with standard access privileges. A blind test simulates the actions and procedures of a real attacker by strictly limiting the information

given to the person or team that is performing the test beforehand. In double blind testing, it takes the blind test even further, in that only a few individuals within the organization would be aware that a test is being conducted. There are many different tools that can be used for penetration testing. Several are available on the market that one can download and use for free. Many of them are even able to be customized; known as Open Source tools. For example, the testing tool Kali Linux has its own built-in penetration tools, however, you can download and install additional tools to it. Most of these programs are being developed for Linux, with only a handful are being devil for Windows or Mac.

There are also several penetration testing software that one can purchase. Some of them cost as little of 10 dollars for their license, and others may cost thousands of dollars. Examples of these tools include:

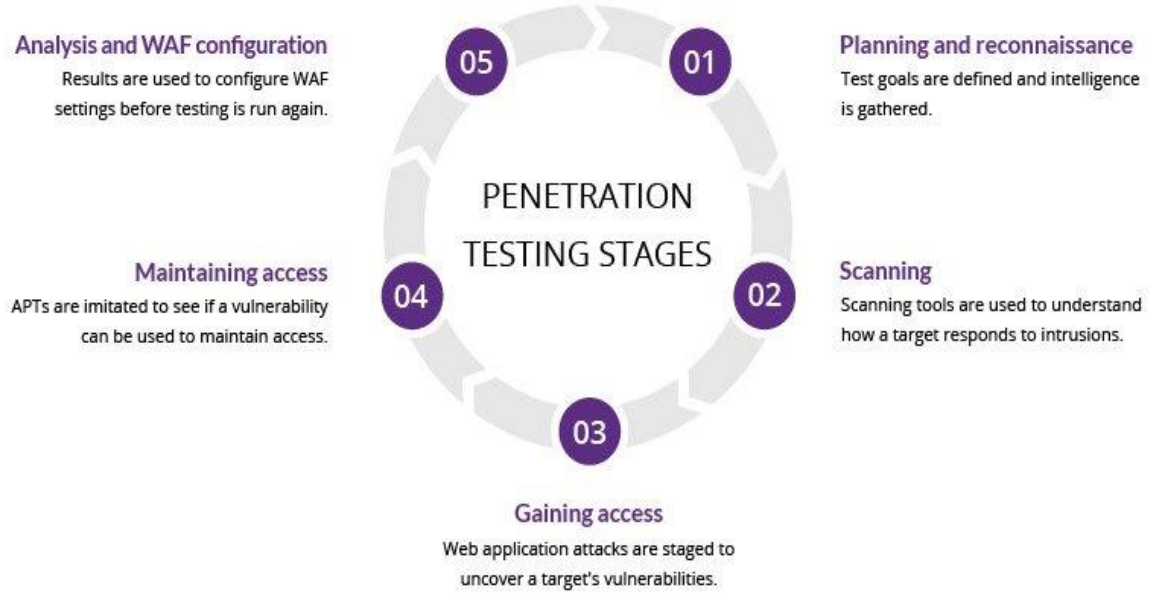
- Kali Linux – An Linux-based OS Linux-based suite of penetration tools.
- Metasploit – An advanced Framework used for pen testing that contains command-line and GUI interfaces.
- Wireshark – A protocol analyzer with a GUI.
- w3af – A web application attack and audit framework.
- John The Ripper – A password cracker [2].

Fig.1 penetration attack steps

1. Context and Preliminary Investigation

2.1 Penetration testing stages

The pen testing process can be broken down into five stages.



2.1.1 Planning and reconnaissance

The first stage involves:

- Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.
- Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2.1.2 Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

- **Static analysis** – Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.
- **Dynamic analysis** – Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application's performance.

2.1.3 Gaining Access

This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these

vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

2.1.4 Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization's most sensitive data.

2.1.5 Analysis

The results of the penetration test are then compiled into a report detailing:

- Specific vulnerabilities that were exploited
- Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

2.1.6 Penetration testing methods

- **External testing**

External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

- **Internal testing**

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

- **Blind testing**

In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

- **Double-blind testing**

In a double-blind test, security personnel has no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

- **Targeted testing**

In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

3 Literature survey

V. Santhi et al., presented the Penetration Testing which helps us to secure a computer system, network or web applications that allows you to gain high security issues which also helps to find vulnerabilities that an attacker could exploit. This paper investigates about different penetration testing tools in kali Linux, how to deploy it and how to make use of it to perform different types of attacks which includes methodologies and also defense strategies. Technically, we performed different penetration tests with virtualized systems, tools and using private networks. The attacks that are performed were: Man in the middle attack and traffic sniffing using both terminal and by Ettercap and driftnet, Bluetooth hacking, and spying on a webcam. The results and implementation is discussed and summarized. This paper also gives a detail methodology of how to perform these attacks [1].

Ibrahim Ali et al., presented in this paper investigate different aspects of penetration testing including tools, attack methodologies, and defense strategies. More specifically, we performed different penetration tests using a private network, devices, and virtualized systems and tools. We predominately used tools within the Kali Linux suite. The attacks we performed included: smartphone penetration testing, hacking phones' Bluetooth, traffic sniffing, hacking WPA Protected Wifi, Man-in-the-Middle attack, spying (accessing a PC microphone), hackingphones's Bluetooth, and hacking remote PC via IP and open ports using advanced port scanner. The results are then summarized and discussed [2-5].

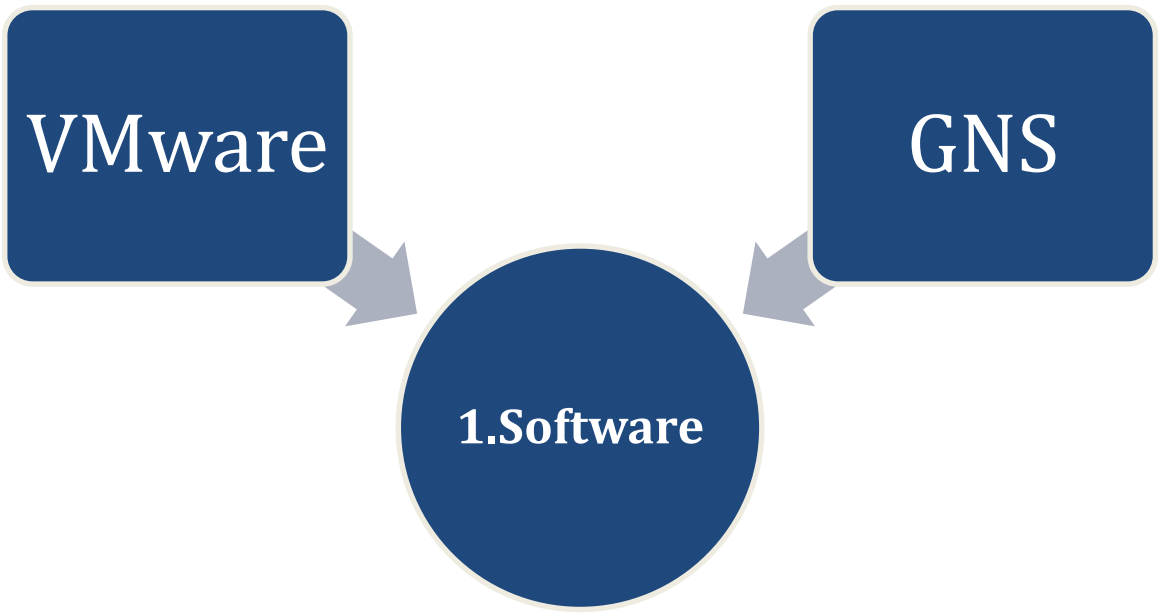
Chung-Kuan Chen et al. present Internet of Things (IoT) devices and services that are now integral to most daily activities [3]. However, the IoT brings not only added convenience but, by connecting more and more objects to the Internet, new security threats.1 Many applications in IoT ecosystems, from smart homes to customized healthcare, contain sensitive personal information that can becotatargets of network attacks. Unfortunately, ensuring the security of IoT objects is not straightforward for three major reasons. First, the IoT's heterogeneous nature makes it vulnerable to many kinds of attacks. Second, heavyweight protection mechanisms are infeasible for resource-constrained IoT devices. Third, many IoT objects are deployed only once and thereafter are rarely maintained or updated[5 -20]

Dewan Md. Farid, et al. [4]explained A variety of intrusion detection systems (IDS) have been employed for protecting computers and networks from malicious network-based or host-based attacks by using traditional statistical methods to new data mining approaches last decades. However, today's commercially available intrusion detection systems are signature-based that are not capable of detecting unknown attacks. In this paper, we present a new learning algoritanomaly-based based network intrusion detection system using a decision tree algorithm that distinguishes attacks from normal behaviors and identifies different types of intrusions. Experimental results on the KDD99 benchmark network intrusion detection dataset demonstrate that the proposed learning algorithm achieved 98% detection rate (DR) in comparison with other existing methods [20-40].

Authors discussed Intrusion Detection Systems (IDS) [5] have become a necessity in computer security systems because of the increase in unauthorized accesses and attacks. Intrusion Detection is a major component in computer security systems that can be classified as Host-based Intrusion Detection System (HIDS), which protects a certain host ,or system and Network-based Intrusion detection system (NIDS), which protects a network of hosts and systems. This paper addresses Probes attacks or reconnaissance attacks, which try to collect any possible relevant information in the network. Network probe attacks have two types: Host Sweep and Port Scan attacks. Host Sweep attacks determine the hosts that exist in the network, while port scan attacks determine the available services that exist in the network. This paper uses an intelligent system to maximize the recognition rate of network attacks by embedding the temporal behavior of the attacks into a TDNN neural network structure. The proposed system consists of five modules: packet capture engine, preprocessor, pattern recognition, classification, and monitoring and alert module. We have tested the system in a real environment where it has shown good capability in detecting attacks. In addition, the system has been tested using DARPA 1998 dataset with 100% recognition rate. In fact, our system can recognize attacks in a constant time [40-50].

4 Analysis

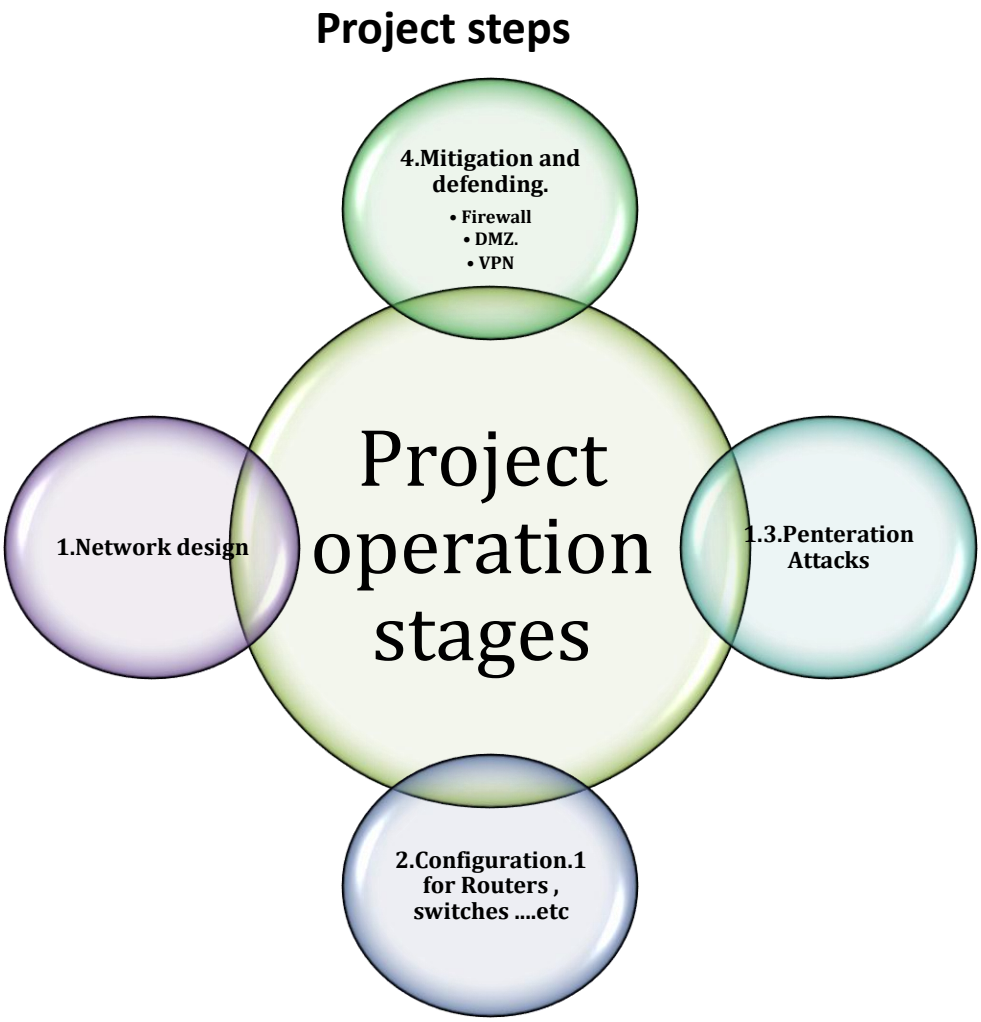
4.1 Software



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 ended-services “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[50-54].

4.2 Project phases

1. Network Design.
2. Configurations.
3. Penetration attacks.
4. Mitigation and defending.



5. Design

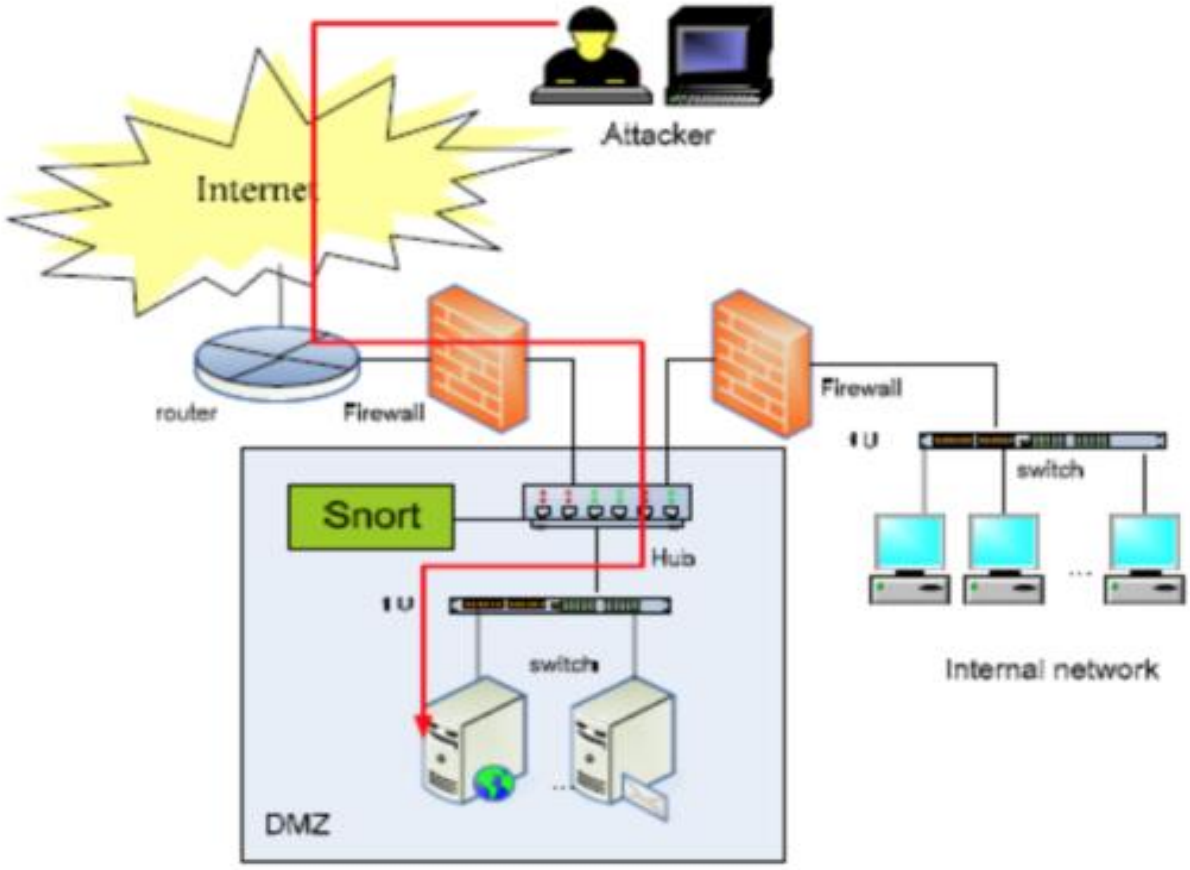


Fig.2 Network block diagram

4 References

1. Santhi, V., Dr K. Raja Kumar, and BLV Vinay Kumar. "Penetration Testing using Linux Tools: Attacks and Defense Strategies." *pub. in International Journal of Engineering Research & Technology (IJERT)* 5.12 (2016).
2. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.
3. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.
4. Rahman, Chowdhury Mofizur, et al. "Attacks classification in adaptive intrusion detection using decision tree." (2010).
5. Al-Jarrah, O., & Arafat, A. (2015). Network intrusion detection system using neural network classification of attack behavior. Journal of Advances in Information Technology Vol, 6(1).
6. 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
7. 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
8. 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
9. 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.
10. 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
11. 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
12. 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
13. 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

14. Khan, M. A., Quasim, M. T., Algarni, F., & Alharthi, A. (Eds.). (2020). Decentralised Internet of Things: A blockchain perspective (Vol. 71). Springer Nature.
15. 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
16. 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
17. 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
18. 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
19. 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
20. 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.
21. 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.
22. 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.
23. 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.
24. 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
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), 2020, pp. 599-604, doi: 10.1109/ICSTCEE49637.2020.9276922.

26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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
32. 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
33. 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).
34. 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)
35. 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,
36. M.T.Quasim , An Efficient approach for concurrency control in distributed database system, Indian Streams Research Journal, 2013(Volume-3, Issue-9)
37. 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.
38. 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

39. 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.
40. 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.
41. 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.
42. 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.
43. 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.
44. 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
45. Ebrahim, N. S., & Quasim, M. T. (2021). EMCSS: efficient multi-channel and time-slot scheduling. Wireless Networks, 27(4), 2879-2890.
46. 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
47. 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.
48. 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.
49. Quasim, M. T. (2021). Challenges and applications of internet of things (IoT) in Saudi Arabia.
50. 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
51. Johri, Prashant, Adarsh Anand, Juri Vain, Jagvinder Singh, and Mohammad Tabrez Quasim, eds. System Assurances: Modeling and Management. Elsevier, 2022.
52. 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 .
53. AA Radwan , M.T.Quasim, "Toward semantic representation of middleware services", Smart Computing, 2021, pp. 3-10

54. 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.
55. 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.