Controlling and Protecting Wide Broadband Networks Using ACS Server Against Attacks

Waleed Mughram Saad Alamri Alamri and
Mohammad Tabrez Quasim

December 19, 2024

Controlling and protecting Wide broadband networks using ACS server against attacks

Waleed Mughram saad alamri, Mohammad Tabrez Quasim
College of Computing and Information Technology, University of Bisha, Bisha,67714, Saudi Arabia

ABSTRACT

Networks emerged to meet the need for communication across distances and the exchange of services, enabled by advances in science and technology. They allow organizations to share resources, such as linking company branches into a unified system or connecting multiple devices to a single printer. This fosters a shared work environment and centralized management for geographically dispersed operations.

Networks are classified by geographical scope into local (LANs), metropolitan (MANs), and wide (WANs) networks. LANs, limited to a few kilometers, offer high data speeds (10–1,000 Mbps) using technologies like coaxial cables, twisted pairs, or optical fibers. WANs span vast distances, connecting numerous devices and enabling data exchange across regions.

Access control is crucial for information system security. It prevents unauthorized access, defines user permissions, and protects system resources, ensuring safe and secure operation while blocking illegal intrusions.

1. INTRODUCTION

Server is a computer with high-capacity components, its main task is to manage the information resources available on the network such as computers, printers, phones, etc.

The server has multiple uses that differ according to the types of programs that were previously installed to determine the server working environment, so you must first determine which server is needed to provide the appropriate programs for it[1-10].

1.1 Why Use Cisco ACS?

- Cisco ACS servers can be used as a clearinghouse for user authentication.
- By allowing all your network devices to use the ACS server, an admin can avoid having to create the same user account on each individual router and switch
- One convenient feature of the ACS is that the users do not have do not have to be configured locally on the server

    - ACS servers have the ability to use and review an external database o An example of this type of external database is the Microsoft Active Directory

1.2 On What Platform Does ACS Run?

- There are multiple platforms that an ACS server can run on.
    - Newer versions of the ACS server can be installed on top of previous older versions of it
- The most common option is to install the ACS server in a Vmware environment like ESXi server o This will mean that the ACS server will run as a virtual machine.

1.3 Protocols Used Between the ACS and the Router

- The communication between an ACS server and its client uses two main protocols: TACACS+ and RADIUS.
    - TACACS+: Terminal Access Control Access Control Server
        - TACACS+ is proprietary to Cisco
        - If the ACS server uses this protocol, all AAA packets are encrypted before being sent o RADIUS: Remote Authentication Dial-In User Service
        - Open standard alternative to TACACS+
        - Only encrypts passwords, not the entire packet

1.4 Protocol Choices Between the ACS Server and the Router

- TACACS+ is more granular than RADIUS
    - If an administrator wants to tell the router to check authorization for each individual command before allowing the user to put that command and only give the administrator a select few of commands.
    - RADIUS does not allow for command-by-command authorization
- RADIUS can be used in a scenario in which end users just want their packets to go through a network device where authentication and authorization are required.
- A router can be configured to use both RADIUS and TACACS+ simultaneously [10-20].

The following table compares the two protocols:

	TACACS+	**RADIUS**

Functionality	Separates AAA functions into distinct elements. Authentication is separate from authorization and both are separate from accounting	Combines many of the functions of authentication and authorization together. Has detailed accounting capability when accounting is configured for use.
Standard	Cisco proprietary, but very well known.	Open standard, and supported by nearly all vendors' AAA implementation.
L4 Protocol	TCP	UDP
Confidentiality	***ALL*** packets are encrypted between the ACS server and the router (aka the client)	Only the password is encrypted with regard to packets sent back and forth between the ACS server and the router.
Granular command by command authorization	This is supported, and the rules are defined on the ACS server about which commands are allowed or disallowed.	No explicit command authorization checking rules can be implemented.
Accounting	Provides accounting support.	Provide accounting support, and generally acknowledged as providing more detailed or extensive accounting capability than TACACS+.

2. Context and Preliminary Investigation

2.1 Most important types of hosting servers:

1. Dedicated Server

An integrated unit that works to serve one company or one person, and it is considered one of the most expensive and best types of servers, and institutions, companies and major sites work in it in order to achieve the greatest degree of safety and privacy[21-30] .

2.Virtual Privet Server

Vps, which means dividing the server into more than one virtual server, and each VPS server is sold separately. Therefore, all users will share the capabilities of the server from (storage unit - RAM - data processor.. That is why a virtual server was named for its privileges as a full server .

3. Application Server

It provides a suitable working environment for running applications and games, and there are different types of it for the diversity of applications and the diversity of programming languages such as applications made through Java or PHP, and therefore you must choose an application server compatible with the programming language[31-40] .

4. Web Server

A device that contains software files for websites, so that it receives and processes requests coming from the network (through users' browsers., and provides pages with website content, and the service provided in this type of server is called web hosting .

5. Email Server

A device responsible for receiving and sending e-mails to and from the same domain or any other domain, as well as through which e-mail files are stored .

6. File Transfer Server - FTP Server

It is a server device used for the exchange of computer files through the network and often the Internet, so that it is possible to specify the permissions to access the files and control the users' access to the files on the server [41-50].

7. Database Server

It is a server machine that contains a database management program, and provides database service to other servers or computers connected to a network .

8. DNS Server

It is a server machine that is responsible for translating domain names into two IP addresses and vice versa, and has uses in local networks (LAN. and the Internet .

2.2 THE PROPOSED SERVER-ACS SERVER

The ACS "Cisco Access Control Security" is a server from Cisco that is used to control WANs or large-scale networks, allowing some specific users of it to access these networks .

It is the latest types of servers that have provided:

1. A lot of security and flexibility in dealing between networks and each other .

2. As well as protection from cyber attacks that threaten its work .

3. It provides and supports AAA feature

- It is a feature found in the latest types of Routers and some types of the latest switches, and its main function is to give permissions to access the network in addition to specifying the permissions for everyone who accesses the router .
- Protecting network devices, specifically the router, from any penetration of unauthorized users.
- After connecting the router, two virtual machines will be created, one VM machines, one will be placed on it, a copy of the ACS, which is the server through which the site networks will be controlled, but not by configuration or the usual traditional commands, but by a GUI dedicated to remote control of the devices.

3. Literature survey

R.Molva describes an access control mechanism that enforces at the network level an access control decision that is taken at the application level. The mechanism is based on the precomputation of encrypted counters called tickets. An access enforcement device verifies the existence of a valid ticket in each packet that is subject to access control and kills unauthorized packets. Tickets are not computed as a function of the user data. Due to the timing constraints of shared media LANs the presence of a valid ticket in a packet proves that the operation implied by the user data has been authorized. The access control mechanism is elaborated for Internet protocols over Ethernet and we discuss its properties for internetworking and multicasting *[4].*

David presented RBAC systems define a number of roles and assign each role a set of permissions. Each user is then assigned to one or more roles, and inherits the permissions assigned to the roles (for more on RBAC, see the “Role-Based Access Control Models” sidebar). X.509 supports RBAC by defining role specification ACs that hold the permissions granted to each role, and role assignment ACs that assign various roles to the users. RBAC can significantly simplify access control management for large numbers of users because it allocates permissions to roles rather than individuals, and there are typically far fewer roles than users [5].

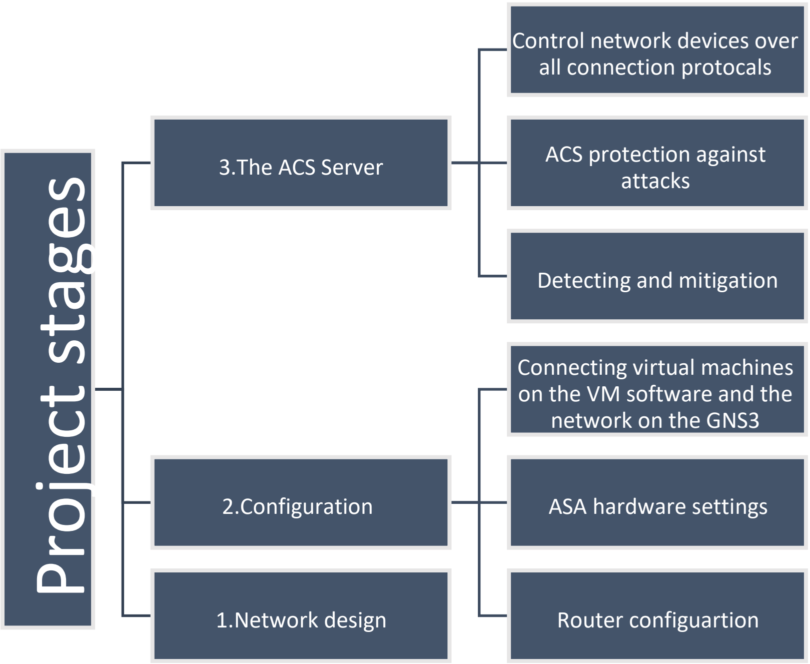
SHI Jiaoli et al. introduced Binding access policies to data, Ciphertext-policy attribute-based encryption (CP-ABE) enables data access control to be independent from a certain application and lets users face data directly. It is regarded as one of the most suitable access control methods in cloud storage system and gets the attention of extensive researches. In those researches, Hierarchical cryptography architecture (HCA) is often applied to improve the efficiency of the system. There exist two open issues: illegal leakage of symmetric keys and low efficiency of revocation of an attribute of a user. We propose an Access control scheme under Hierarchical cryptography architecture (ACS-HCA). In this scheme, key derivation mechanism and forward derivation function are used to avoid the leakage of symmetric keys, All-orNothing transform is used to prevent the illegal reuse of symmetric keys, and attribute revocation is realized without reissuing other users' private keys. Analyses and simulations demonstrate that our scheme sustains less encrypting cost on each owner and less decrypting cost on each user, but gain high efficiency in revocation of an attribute of a user [50-54]].

4. Analysis

Project phases

1. Designing.
2. Implementation.
3. Testing.

Project steps


Project stages
3.The ACS Server
Control network devices over all connection protocals
ACS protection against attacks
Detecting and mitigation
2.Configuration
Connecting virtual machines on the VM software and the network on the GNS3
ASA hardware settings
1.Network design
Router configuartion

Software:

- GNS3.
- VMWARE.

4.1 Designing phase:

In this stage, the shape of the network, how to design it, the types of the router devices used in the network and the switch devices to connect the network devices used by computers, as well as network sources such as printers and .... etc.

Also, at this stage, a general conception of how the ACS server is used, how to manage and control it, as well as a general conception of the addresses used within the network, in addition to creating a structural vision of the network expected to be designed.

4.2 Implementation phase:

In this stage, 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.

Also, at this stage, the virtual machines will be added to the VM ware program, which is the program used to create virtual machines from the Windows system used to manage the ACS server or even the ACS server itself, and link the virtual network cards used to connect the virtual machines created on the VM program and link them to the network designed on the GNS3 program. And finally, creating authenticated network users to give them access to the network, or 4.3

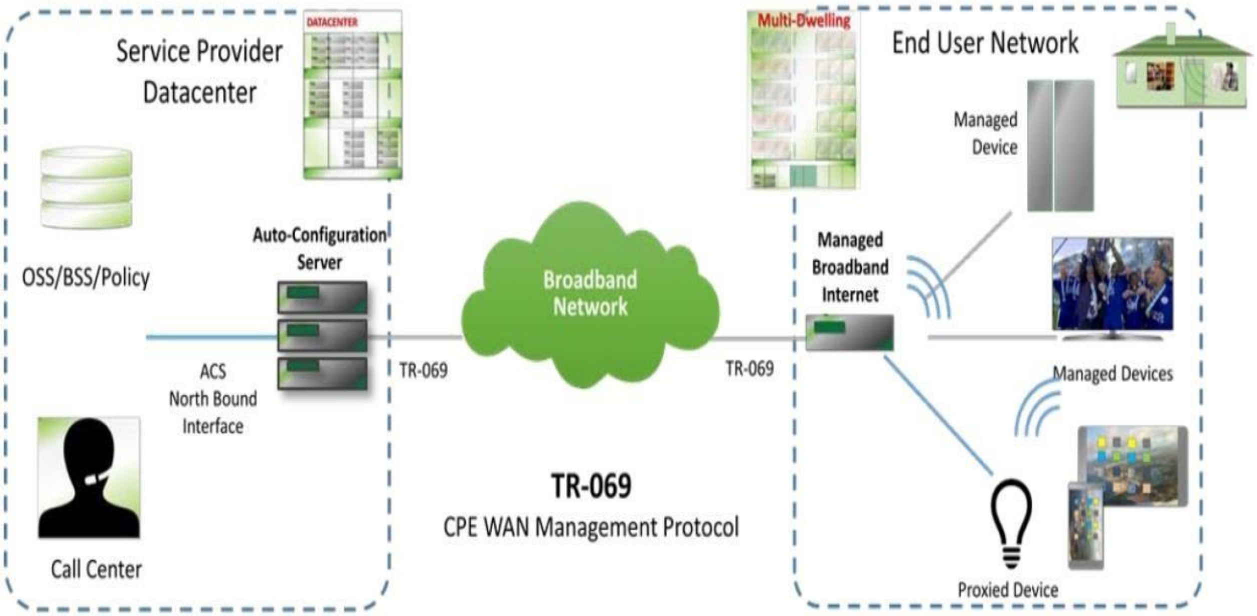
4.3 Testing phase:

In the testing phase, the connection to all the designed branches within the network will be tested and investigated, and their connection between them and some will also be investigated, the ACS will be operated and its connection to all parts of the network will be investigated, and then the network management stage will come through the server.

The network will be managed first through the Cisco Configuration Professional program, which is used to manage Cisco devices from servers and use the graphical interface features to fully control the network devices[55-60].

Then, secondly, controlling the server through the HTTPs browser and managing the services and features provided by this server[60-65] .

5. Design



Network block diagram

6. References

[1]. 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.

[2]. 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).

[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.

[4]. Molva, Refik, and Erich Rütsche. "Application access control at network level." Proceedings of the 2nd ACM Conference on Computer and Communications Security. 1994.

[5]. Chadwick, David, Alexander Otenko, and Edward Ball. "Role-based access control with X. 509 attribute certificates." IEEE Internet Computing 7.2 (2003): 62-69.

[6]. Shi, Jiaoli, et al. "ACS-HCA: An access control scheme under hierarchical cryptography architecture." Chinese Journal of Electronics 28.1 (2019): 52-61.

[7] Mohammad Ayoub Khan, Mohammad Tabrez Quasim , et.al, Decentralised IoT, Decenetralised IoT: A Blockchain perspective, Springer, Studies in BigData, 2020, DOI: https://doi.org/10.1007/978-3030-38677-1

[8] 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

[9] 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

[10] 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

[11] 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

[12]Jaafar Alghazo, Geetanjali Rathee, Sharmidev Gupta, Mohammad Tabrez Quasim, Sivaram Murugan, Ghazanfar Latif, and Vigneswaran Dhasarathan. A Secure Multimedia Processing through Blockchain in Smart Healthcare Systems. ACM Trans. Multimedia Comput. Commun. Appl. 0, ja. DOI: https://doi.org/10.1145/3396852

[13] 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.

[14] 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.

[15] 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.

[16] Khan, M. A., Quasim, M. T., Algarni, F., & Alharthi, A. (2020). Decentralised Internet of Things: A blockchain perspective. https://doi.org/10.1007/978-3-030-38677-1. ISBN: 978-3-030-38676-4.

[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/10.1007/978-3-03060922-1_1

[18] 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

[19] 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.

[20] 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.

[12] 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

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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

[27] 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.

[28] 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.

[29] Quasim, M. T. (2021). Challenges and applications of internet of things (IoT) in Saudi Arabia.

[30] 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

[31] Johri, Prashant, Adarsh Anand, Juri Vain, Jagvinder Singh, and Mohammad Tabrez Quasim, eds. System Assurances: Modeling and Management. Elsevier, 2022.

[32] 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 .

[33] AA Radwan , M.T.Quasim, “Toward semantic representation of middleware services”, Smart Computing, 2021, pp. 3-10

[34] 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.

[35] Narayana, T. Lakshmi, C. Venkatesh, Ajmeera Kiran, Adarsh Kumar, Surbhi Bhatia Khan, Ahlam Almusharraf, and Mohammad Tabrez Quasim. "Advances in real time smart monitoring of environmental parameters using IoT and sensors." Heliyon 10, no. 7 (2024).

[36] Quasim, Mohammad Tabrez, Khair ul Nisa, Mohammad Zunnun Khan, Mohammad Shahid Husain, Shadab Alam, Mohammed Shuaib, Mohammad Meraj, and Monir Abdullah. "An internet of things enabled machine learning model for Energy Theft Prevention System (ETPS) in Smart Cities." Journal of Cloud Computing 12, no. 1 (2023): 158.

[37] Quasim, Mohammad Tabrez, Mohammad Mufareh Mobarak, Khair Ul Nisa, Mohammad Meraj, and Mohammad Zunnun Khan. "Blockchain-based Secure health records in the healthcare industry." In 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), pp. 545-549. IEEE, 2023.

[38] 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

[39] 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

[40] 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).

[41] 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)

[42] 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,

[43] M.T.Quasim , An Efficient approach for concurrency control in distributed datase system, Indian Streams Research Journal, 2013(Volume-3, Issue-9)

[44] Khan, Mohammad Zunnun, Mohd Shoaib, Mohd Shahid Husain, Khair Ul Nisa, and Mohammad Tabrez Quasim. "Enhanced mechanism to prioritize the cloud data privacy factors using AHP and TOPSIS: a hybrid approach." Journal of Cloud Computing 13, no. 1 (2024): 42.

[45] 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.

[46] 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

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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.

[52] 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

[53] 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.

[54] 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.

[55] Ebrahim, N. S., & Quasim, M. T. (2021). EMCSS: efficient multi-channel and time-slot scheduling. Wireless Networks, 27(4), 2879-2890.

[56] Syed, Ahsan Saud Qadri, C. Atheeq, Layak Ali, and Mohammad Tabrez Quasim. "A Chaotic Mapbased Approach to Reduce Black Hole Attacks and Authentication Computational Time in MANETs." Engineering, Technology & Applied Science Research 14, no. 3 (2024): 13909-13915.

[57] Prakash, P. Suman, P. Kiran Rao, E. Suresh Babu, Surabhi Batia Khan, Ahlam Almusharraf, and Mohammad Tabrez Quasim. "Decoupled SculptorGAN Framework for 3D Reconstruction and Enhanced Segmentation of Kidney Tumors in CT Images." IEEE Access (2024).

[58] Masoodi, Faheem, Mohammad Quasim, Syed Bukhari, Sarvottam Dixit, and Shadab Alam, eds. Applications of Machine Learning and Deep Learning on Biological Data. CRC Press, 2023.

[59] Alghamdi, Abdullah, Asadullah Shaikh, Mohammad Tabrez Quasim, Mesfer Alrizq, Surbhi Bhatia, Mana Saleh Al Reshan, and Shadab Alam. "Emotion recognition and notification system." U.S. Patent Application 17/809,428, filed October 20, 2022.

[60] Sulaiman, Adel, Abdullah Alghamdi, Hani Alshahrani, Sultan Alyami, Mana Saleh Al Reshan, Yousef Asiri, Mohammad Alsulami, Asadullah Shaikh, Samar M. Alqhtani, and Mohammad Tabrez Quasim. "Ai based system for warning and managing operations of vehicles at higher speeds." U.S. Patent Application 18/081,836, filed April 20, 2023.

[61] Alshahrani, Hani, Yousef Asiri, Adel Sulaiman, Mohammed Hamdi, Asadullah Shaikh, and Mohammad Tabrez Quasim. "Artificial intelligent based system for customer recommendation and notification and its process thereof." U.S. Patent Application 18/067,169, filed April 20, 2023.

[62] Quasim, Mohammad Tabrez, and Mohammed Amer Alasiri. Techniques for Detecting and Preventing IP Sniffing Amplification Attacks. No. 10096. EasyChair, 2023.

[63] Quasim, Mohammad Tabrez, Ahmed Nasser Al Hawi, and Mohammad Meraj. System Penetration: Concepts, Attack Methods, and Defense Strategies. No. 9538. EasyChair, 2023.

[64] Quasim, Mohammad Tabrez, and Ahmed Nasser Al Hawi. Mechanisms of System Penetration: Concepts, Attack Methods, and Defense Strategies. No. 9197. EasyChair, 2022.

[65] M. Khalifa, M. A. Khan, M. T. Quasim, M. Z. Khan and K. Ul Nisha, "Reliable IPS model for eLCMS Service and Files Protection," 2024 9th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Athens, Greece, 2024, pp. 25-29, doi: 10.1109/SEEDA-CECNSM63478.2024.00014.