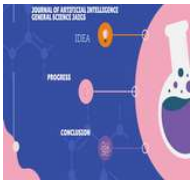
ISSN: 3006-4023(Online), Vol. 2, Issue 1
Journal of Artificial Intelligence General Science (JAIGS)



Security Challenges of Vehicular Cloud Computing

Jaydeep Thakker

Abstract

In the realm of Industry 4.0, the utilization of artificial intelligence (AI) and machine learning for anomaly detection faces challenges due to significant computational demands and associated environmental consequences. This study aims to tackle the need for high-performance machine learning models while promoting environmental sustainability, contributing to the emerging concept of 'Green AI.' We meticulously assessed a wide range of machine learning algorithms, combined with various Multilayer Perceptron (MLP) configurations. Our evaluation encompassed a comprehensive set of performance metrics, including Accuracy, Area Under the Curve (AUC), Recall, Precision, F1 Score, Kappa Statistic, Matthews Correlation Coefficient (MCC), and F1 Macro. Concurrently, we evaluated the environmental footprint of these models by considering factors such as time duration, CO2 emissions, and energy consumption during training, cross-validation, and inference phases.

While traditional machine learning algorithms like Decision Trees and Random Forests exhibited robust efficiency and performance, optimized MLP configurations yielded superior results, albeit with a proportional increase in resource consumption. To address the trade-offs between model performance and environmental impact, we employed a multi-objective optimization approach based on Pareto optimality principles. The insights gleaned emphasize the importance of striking a balance between model performance, complexity, and environmental considerations, offering valuable guidance for future endeavors in developing environmentally conscious machine learning models for industrial applications.

Keywords: Anomaly Detection, Green AI, Trustworthy AI, Machine Learning, Artificial Intelligence, Industrial Environments, Comparative Study, Environmental Impact.

Article Information:
Article history: Received:01/02/2024Accepted: 05/02/2024Online: 10/03/2024Published: 10/03/2024
Corresponding author: Jaydeep Thakker email: jaydeep2005@gmail.com

Introduction

By constantly connecting resources and gathering data, a vehicle cloud may be instantly constructed. Vehicles can access the cloud and receive get all of the necessary resources and apps they want when they need them. The VCC may be quite advantageous for vehicles, especially less expensive ones. For instance, in bad wealth automobiles without pricey radar cruise systems may request vehicle collision detection service. It is obvious that security and privacy concerns must be resolved if the VCC concept is to be widely adopted and have a substantial social impact.[1] Unlike traditional wireless networks, VANETs, or cloud computing, VCC has significant potential security and privacy issues. The number of vehicles rises in direct proportion to the enormous growth of the human population. According to statistics, there are already 1 billion automobiles on the road, and that number will double by 2050. Along with travel conveniences, this influx of vehicles creates other problems, such traffic congestion, roadside accidents, pollution, and more. To address these issues, the Intelligent Transport System (ITS) is a successful endeavor. To reach the goal of intelligent driving, these linked cars have embedded systems such as the onboard unit (OBU), electronic control unit, application unit, and head unit. Vehicle (V2V) communication models are used in ITS to enable vehicle-to-vehicle communication and the sharing of useful information. Vehicles can interact with linked Road Side Unit (RSU) systems on the side of the road via Vehicle- to- Infrastructure (V2I) communication.[2] It's also known as (Vehicle- to- Network)V2N . Through the use of computer equipment, like laptops or mobile phones, cars and pedestrians may interact while they are both on the road (V2P communication).[3]

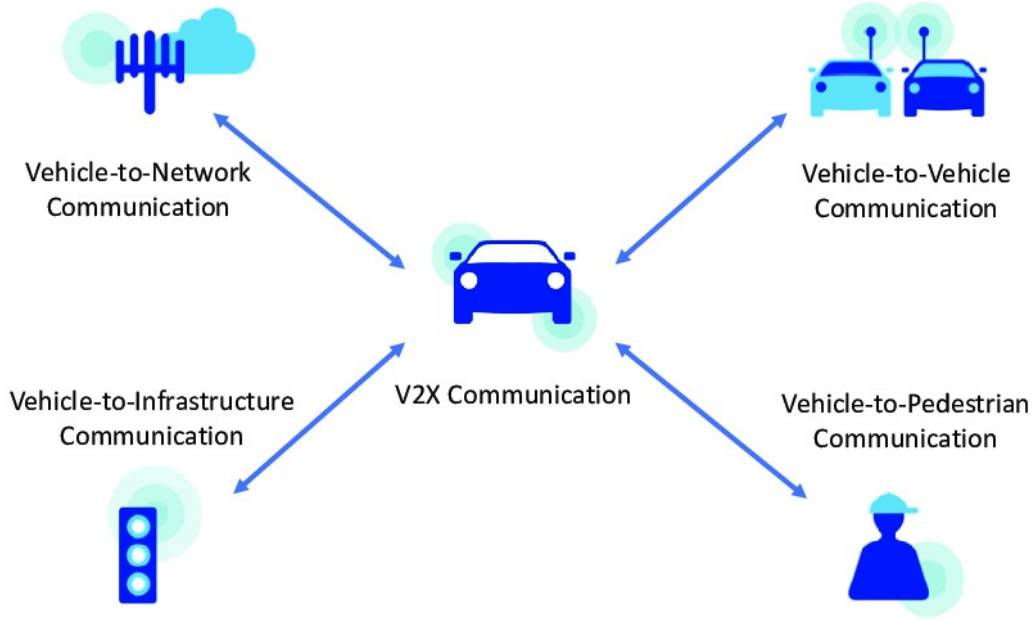


Figure.1 Vehicle Communication Model

To establish the above connections, a vehicular ad-hoc network (VANET) is created. VANET is a wireless connection architecture for offering automobile safety and also non-safety services. Dedicated Short Range Communication (DSRC), the most popular V2X interaction technology, enables communication between cars and other connected devices in VANET. Additionally, Long Term Evolution (LTE), also known as V2X-LTE, has attracted a lot of attention in the V2X communication community. Additionally, 5G technologies are finding a place in the V2X communication paradigm.[4] Vehicular Cloud Computing (VCC) is a brand-new hybrid system that aims to take advantage of the computing power of VANET devices in order to provide consumers with useful

services on a pay-as-you-go basis. In order to create a cloud of shared resources with plenty of computing resources, VCC works in conjunction with VANET elements like RSU or cars within a defined range (almost 300 meters). To handle constraints and overloaded service expectations, VCC strives to manage onboard computers, storage resources, sensor equipment, and communication facilities. The most important applications offered by VCC are traffic management, data outsourcing, outsourced computing, access control, data sharing, and additional value-added services, including entertainment, traffic safety, autonomous driving, and road management. Due to its unique characteristics, such as the cloud's multi-tenancy, quick services, high vehicle movement, and short range of linked devices, the security of VCC is the largest problem in the VCC tale.[5] We will discuss security needs and potential threats will be discussed in the following section.

Vcc Security Assessment

Security requirements and a hypothetical assault against VCC are presented in this section. VCC has additional security difficulties in addition to the inherent security constraints of cloud computing. The primary feature of VCC that sets it apart from CC is the dynamic switching of the available computer resources. Furthermore, VCC cars are unreliable since they enter a shared resource pool for a brief time before leaving.[6] One car never has a neighbor who remains for a long time, and each vehicle has a neighbor who frequently changes, which makes it difficult to build confidence. The resources that offer computational services to other resources may also be used by possible malicious vehicles due to VCC. These features add further difficulties to the security problems with cloud computing.

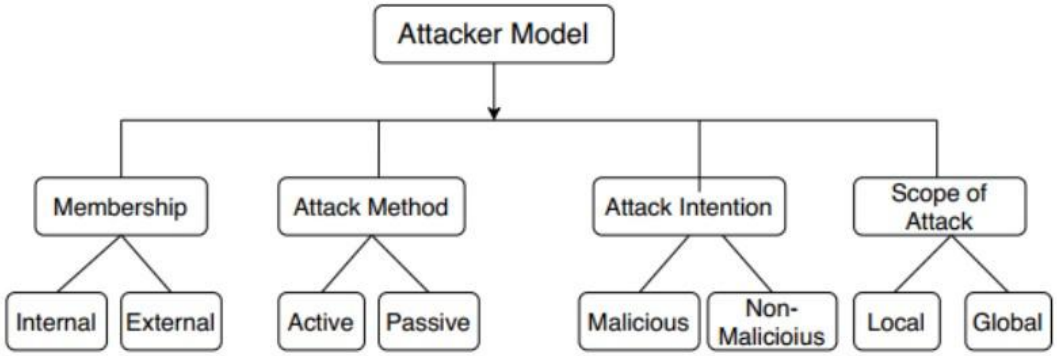


Figure.2 Vehicular cloud computing Attack Model

Internal intruders have given VCC members permission to access and make use of VCC resources legally. External intruders attack by maliciously gaining access to VCC even if they are not permitted to do so. They could physically harm RSUs or other stationary infrastructure, for instance. Messages, signals, and other sources can all be promptly attacked by an active assault, such as by inserting a bogus message. The security of data stored in the cloud is threatened by active attackers. Important papers, saved data, more private information, and executable code can all be included in this material. Passive attackers use the information for future use, as opposed to active attackers who actively modify data. They might function in a wireless network as an eavesdropper.[7]

Comparison of malicious and non-malicious attackers

Despite their gain, the malevolent attacker has harmful objectives. This type of attacker has the ability to introduce malware into the system, causing disruption or even system failure. A greedy attacker who intends to attack the system personally is another name for a non-malicious attacker. They may, for instance, inform people about the emergency system and reduce traffic.[8] Different types of attackers have different ranges of attack. Limited automobiles are affected by the neighborhood attacker. They may, for instance, set up listening posts for a select group of VCC organizations or adjacent automobiles. The global attacker, in comparison, has a larger domain and the ability to command additional VCC units, allowing them to access a wider variety of data in the vehicular cloud network.[9] According to the aforementioned concept, a Global Passive Attacker (GPA), whether internal or external, may cause the most damage by listening in on global broadcast information and violating location privacy

for their targeted range of vehicles. GPA can build its listening post by utilizing already-existing infrastructures like RSU.

Requirement for Security and Possible Attacks

An important requirement of VCC is authenticity, which separates harmful from genuine organizations from the harmful ones.The VCC system ought to be able to identify genuine VCC entities. Message authentication and user authentication are two further categories of authentication needs. On the basis of a predetermined set of regulations, it should be assured that only authorized VCC entities have access to excellent VCC service. To specify which VCC entity may access particular VCC services, there needs to be some sort of Service Level Agreement (SLA).[10] The process of sending communications across VCC entities on time in order to prevent service disruption is covered by the availability requirement. Availability may be achieved with a low-cost cryptographic approach to guarantee that communications get to their destination in the required amount of time without being tempered. Information security is a necessity for sending data to a target entity in its original form. Since most messages in the VCC environment are visible to everyone, data confidentiality is not given primary importance. It is mostly required for some private communications between two parties. Data transit between two entities should be independently verified to look for any signs of data manipulation, deletion, or change.

CONCLUSION

This study provides a comprehensive review of vehicular cloud computing networks, including a discussion of the key ideas and security concerns. A new hybrid technology that combines cloud computing and intelligent transportation systems is called vehicular cloud computing. Cloud computing for vehicles requires close attention in the area of security. We discussed the security issues and difficulties posed by a unique approach to VANETs by moving VANETs to the clouds. We started by outlining the security and privacy issues that networks using vehicular cloud computing must deal with, as well as some potential security fixes. Although some of the solutions can make use of the current security methods, there are several particular difficulties. On the same cloud server, attackers can physically assemble. High mobility and erratic interaction are fundamental characteristics of vehicles. Intelligent transportation systems must be implemented in a methodical and synthetic approach because of the extensive effort being done on security and privacy in VC. Vehicular cloud computing networks can only offer reliable and workable security and privacy solutions with coordinated efforts and tight collaboration among several institutions, including law enforcement, the government, the automotive car industry, and academia.

References

[1]. Kommaraju, V., Gunasekaran, K., Li, K., Bansal, T., McCallum, A., Williams, I., & Istrate, A. M. (2020). Unsupervised pre-training for biomedical question answering. arXiv preprint arXiv:2009.12952.

[2]. Bansal, T., Gunasekaran, K., Wang, T., Munkhdalai, T., & McCallum, A. (2021). Diverse distributions of self-supervised tasks for meta-learning in NLP. arXiv preprint arXiv:2111.01322.

[3]. Gunasekaran, K., Tiwari, K., & Acharya, R. (2023, June). Utilizing deep learning for automated tuning of database management systems. In 2023 International Conference on Communications, Computing and Artificial Intelligence (CCCAI) (pp. 75-81). IEEE.

[4]. Gunasekaran, K. P. (2023, May). Ultra sharp: Study of single image super resolution using residual dense network. In 2023 IEEE 3rd International Conference on Computer Communication and Artificial Intelligence (CCAI) (pp. 261-266). IEEE.

[5]. Gillespie, A., Yirsaw, A., Gunasekaran, K. P., Smith, T. P., Bickhart, D. M., Turley, M., ... & Baldwin, C. L. (2021). Characterization of the domestic goat γδ T cell receptor gene loci and gene usage. Immunogenetics, 73, 187-201.

[6]. Yirsaw, A. W., Gillespie, A., Zhang, F., Smith, T. P., Bickhart, D. M., Gunasekaran, K. P.,

... & Baldwin, C. L. (2022). Defining the caprine γδ T cell WC1 multigenic array and evaluation of its expressed sequences and gene structure conservation among goat breeds and relative to cattle. Immunogenetics, 74(3), 347-365.
[7]. Gunasekaran, K. P., Babrich, B. C., Shirodkar, S., & Hwang, H. (2023, August). Text2Time: Transformer-based Article Time Period Prediction. In 2023 IEEE 6th International Conference on Pattern Recognition and Artificial Intelligence (PRAI) (pp. 449-455). IEEE.
[8]. Gunasekaran, K., & Jaiman, N. (2023, August). Now you see me: Robust approach to partial occlusions. In 2023 IEEE 4th International Conference on Pattern Recognition and Machine Learning (PRML) (pp. 168-175). IEEE.
[9]. Gillespie, A., Yirsaw, A., Kim, S., Wilson, K., McLaughlin, J., Madigan, M., ... & Baldwin, C. L. (2021). Gene characterization and expression of the γδ T cell co-receptor WC1 in sheep. Developmental & Comparative Immunology, 116, 103911.
[10]. Gunasekaran, K. P. (2023). Leveraging object detection for the identification of lung cancer. arXiv preprint arXiv:2305.15813.
[11]. Zhu, M., Zhang, Y., Gong, Y., Xing, K., Yan, X., & Song, J. (2024). Ensemble Methodology: Innovations in Credit Default Prediction Using LightGBM, XGBoost, and LocalEnsemble. arXiv preprint arXiv:2402.17979.
[12]. Yafei, X., Wu, Y., Song, J., Gong, Y., & Lianga, P. (2024). Generative AI in Industrial Revolution: A Comprehensive Research on Transformations, Challenges, and Future Directions. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 3(2), 11-20.
[13]. Xu, J., Wang, H., Zhong, Y., Qin, L., & Cheng, Q. (2024). Predict and Optimize Financial Services Risk Using AI-driven Technology. Academic Journal of Science and Technology, 10(1), 299-304.
[14]. Li, Z., Huang, Y., Zhu, M., Zhang, J., Chang, J., & Liu, H. (2024). Feature manipulation for ddpm based change detection. arXiv preprint arXiv:2403.15943.
[15]. Li, Z., Huang, Y., Zhu, M., Zhang, J., Chang, J., & Liu, H. (2024). Feature manipulation for ddpm based change detection. arXiv preprint arXiv:2403.15943.
[16]. Li, Z., Zhu, H., Liu, H., Song, J., & Cheng, Q. (2024). Comprehensive evaluation of Mal-API-2019 dataset by machine learning in malware detection. arXiv preprint arXiv:2403.02232.

[17]. Tomar, M., &Periyasamy, V. (2023). The Role of Reference Data in Financial Data Analysis: Challenges and Opportunities. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 1(1), 90-99.
DOI: https://doi.org/10.60087/jklst.vol1.n1.p99

[18]. Chentha, A. K., Sreeja, T. M., Hanno, R., Purushotham, S. M. A., &Gandrapu, B. B. (2013). A Review of the Association between Obesity and Depression. Int J Biol Med Res, 4(3), 3520-3522.

[19]. Gadde, S. S., &Kalli, V. D. R. (2020). Descriptive analysis of machine learning and its application in healthcare. *Int J Comp Sci Trends Technol*, *8*(2), 189-196.

[20]. Atacho, C. N. P. (2023). A Community-Based Approach to Flood Vulnerability Assessment: The Case of El Cardón Sector. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 434-482.

DOI:https://doi.org/10.60087/jklst.vol2.n2.p482

[21]. jimmy, fnu. (2023). Understanding Ransomware Attacks: Trends and Prevention Strategies. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(1), 180-210. https://doi.org/10.60087/jklst.vol2.n1.p214

[21]. Bayani, S. V., Prakash, S., &Malaiyappan, J. N. A. (2023). Unifying Assurance A Framework for Ensuring Cloud Compliance in AIML Deployment. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 457-472.DOI: https://doi.org/10.60087/jklst.vol2.n3.p472

[23]. Bayani, S. V., Prakash, S., &Shanmugam, L. (2023). Data Guardianship: Safeguarding Compliance in AI/ML Cloud Ecosystems. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(3), 436-456.
DOI: https://doi.org/10.60087/jklst.vol2.n3.p456

[24]. Karamthulla, M. J., Malaiyappan, J. N. A., & Prakash, S. (2023). AI-powered Self-healing Systems for Fault Tolerant Platform Engineering: Case Studies and Challenges. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 327-338. DOI: https://doi.org/10.60087/jklst.vol2.n2.p338

[25]. Prakash, S., Venkatasubbu, S., &Konidena, B. K. (2023). Unlocking Insights: AI/ML Applications in Regulatory Reporting for US Banks. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *1*(1), 177-184.DOI: https://doi.org/10.60087/jklst.vol1.n1.p184

[26]. Prakash, S., Venkatasubbu, S., &Konidena, B. K. (2023). From Burden to Advantage: Leveraging AI/ML for Regulatory Reporting in US Banking. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *1*(1), 167-176. DOI: https://doi.org/10.60087/jklst.vol1.n1.p176

[27]. Prakash, S., Venkatasubbu, S., &Konidena, B. K. (2022). Streamlining Regulatory Reporting in US Banking: A Deep Dive into AI/ML Solutions. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *1*(1), 148-166.DOI: https://doi.org/10.60087/jklst.vol1.n1.p166

[28]. Tomar, M., &Jeyaraman, J. (2023). Reference Data Management: A Cornerstone of Financial Data Integrity. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(1), 137-144.DOI: https://doi.org/10.60087/jklst.vol2.n1.p144

[29]. Tomar, M., &Periyasamy, V. (2023). The Role of Reference Data in Financial Data Analysis: Challenges and Opportunities. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 1(1), 90-99.
DOI: https://doi.org/10.60087/jklst.vol1.n1.p99

[30]. Tomar, M., &Periyasamy, V. (2023). Leveraging Advanced Analytics for Reference Data

Analysis in Finance. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(1), 128-136.
DOI: https://doi.org/10.60087/jklst.vol2.n1.p136

[31]. Sharma, K. K., Tomar, M., &Tadimarri, A. (2023). Unlocking Sales Potential: How AI Revolutionizes Marketing Strategies. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 231-250.
DOI: https://doi.org/10.60087/jklst.vol2.n2.p250

[32]. Sharma, K. K., Tomar, M., &Tadimarri, A. (2023). Optimizing Sales Funnel Efficiency: Deep Learning Techniques for Lead Scoring. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 261-274.
DOI: https://doi.org/10.60087/jklst.vol2.n2.p274

[33]. Shanmugam, L., Tillu, R., &Tomar, M. (2023). Federated Learning Architecture: Design, Implementation, and Challenges in Distributed AI Systems. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 371-384.
DOI: https://doi.org/10.60087/jklst.vol2.n2.p384

[34]. Sharma, K. K., Tomar, M., &Tadimarri, A. (2023). AI-driven Marketing: Transforming Sales Processes for Success in the Digital Age. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *2*(2), 250-260.
DOI: https://doi.org/10.60087/jklst.vol2.n2.p260

[35]. Gadde, S. S., &Kalli, V. D. (2021). The Resemblance of Library and Information Science with Medical Science. International Journal for Research in Applied Science & Engineering Technology, 11(9), 323-327.

[36]. Gadde, S. S., &Kalli, V. D. R. (2020). Technology Engineering for Medical Devices-A Lean Manufacturing Plant Viewpoint. Technology, 9(4).

[37]. Gadde, S. S., &Kalli, V. D. R. (2020). Medical Device Qualification Use. International Journal of Advanced Research in Computer and Communication Engineering, 9(4), 50-55.

[38]. Gadde, S. S., &Kalli, V. D. R. (2020). Artificial Intelligence To Detect Heart Rate Variability. *International Journal of Engineering Trends and Applications*, *7*(3), 6-10.

[39]. Chentha, A. K., Sreeja, T. M., Hanno, R., Purushotham, S. M. A., &Gandrapu, B. B. (2013). A Review of the Association between Obesity and Depression. *Int J Biol Med Res*, *4*(3), 3520-3522.

[40]. Tao, Y. (2022). Algorithm-architecture co-design for domain-specific accelerators in communication and artificial intelligence (Doctoral dissertation). https://deepblue.lib.umich.edu/handle/2027.42/172593

[41]. Tao, Y., Cho, S. G., & Zhang, Z. (2020). A configurable successive-cancellation list polar decoder using split-tree architecture. IEEE Journal of Solid-State Circuits, 56(2), 612-623.
DOI: https://doi.org/10.1109/JSSC.2020.3005763

[42]. Tao, Y., & Choi, C. (2022, May). High-Throughput Split-Tree Architecture for Nonbinary SCL Polar Decoder. In 2022 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 2057-2061). IEEE.
DOI: https://doi.org/10.1109/ISCAS48785.2022.9937445

[43]. Tao, Y. (2022). Algorithm-architecture co-design for domain-specific accelerators in communication and artificial intelligence (Doctoral dissertation).
https://deepblue.lib.umich.edu/handle/2027.42/172593

[44]. Mahalingam, H., VelupillaiMeikandan, P., Thenmozhi, K., Moria, K. M., Lakshmi, C., Chidambaram, N., &Amirtharajan, R. (2023). Neural attractor-based adaptive key generator with DNA-coded security and privacy framework for multimedia data in cloud environments. Mathematics, 11(8), 1769.
https://doi.org/10.3390/math11081769

[45]. Padmapriya, V. M., Thenmozhi, K., Praveenkumar, P., &Amirtharajan, R. (2020). ECC joins first time with SC-FDMA for Mission “security”. Multimedia Tools and Applications, 79(25), 17945-17967.
DOI https://doi.org/10.1007/s11042-020-08610-5

[46]. Padmapriya, V. M. (2018). Image transmission in 4g lte using dwt based sc-fdma system. Biomedical & Pharmacology Journal, 11(3), 1633.
DOI :https://dx.doi.org/10.13005/bpj/1531

[47]. Padmapriya, V. M., Priyanka, M., Shruthy, K. S., Shanmukh, S., Thenmozhi, K., &Amirtharajan, R. (2019, March). Chaos aided audio secure communication over SC-FDMA system. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-5). IEEE.
https://doi.org/10.1109/ViTECoN.2019.8899413

[48]. Padmapriya, V. M., Thenmozhi, K., Praveenkumar, P., &Amirtharajan, R. (2022). Misconstrued voice on SC-FDMA for secured comprehension-a cooperative influence of DWT and ECC. Multimedia Tools and Applications, 81(5), 7201-7217.
DOI https://doi.org/10.1007/s11042-022-11996-z

[49]. Padmapriya, V. M., Sowmya, B., Sumanjali, M., &Jayapalan, A. (2019, March). Chaotic Encryption based secure Transmission. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN) (pp. 1-5). IEEE.
DOI https://doi.org/10.1109/ViTECoN.2019.8899588

[50]. Sowmya, B., Padmapriya, V. M., Sivaraman, R., Rengarajan, A., Rajagopalan, S., &Upadhyay, H. N. (2021). Design and Implementation of Chao-Cryptic Architecture on FPGA

for Secure Audio Communication. In Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2020, Volume 3 (pp. 135-144). Springer Singapore https://link.springer.com/chapter/10.1007/978-981-15-9774-9_13

[51]. Padmapriya, V. M., Thenmozhi, K., Avila, J., Amirtharajan, R., &Praveenkumar, P. (2020). Real Time Authenticated Spectrum Access and Encrypted Image Transmission via Cloud Enabled Fusion centre. Wireless Personal Communications, 115, 2127-2148. DOI https://doi.org/10.1007/s11277-020-07674-8
[52].Thakur, A., & Thakur, G. K. (2024). Developing GANs for Synthetic Medical Imaging Data: Enhancing Training and Research. Int. J. Adv. Multidiscip. Res, 11(1), 70-82. DOI: http://dx.doi.org/10.22192/ijamr.2024.11.01.009
[53]. Shuford, J. (2023). Contribution of Artificial Intelligence in Improving Accessibility for Individuals with Disabilities. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(2), 421-433.DOI: https://doi.org/10.60087/jklst.vol2.n2.p433

[54]. Schwartz, E. A., Bravo, J. P., Ahsan, M., Macias, L. A., McCafferty, C. L., Dangerfield, T. L., ...& Taylor, D. W. (2024). RNA targeting and cleavage by the type III-Dv CRISPR effector complex. Nature Communications, 15(1), 3324. https://www.nature.com/articles/s41467-024-47506-y#Abs1

[55]. Saha, A., Ahsan, M., Arantes, P. R., Schmitz, M., Chanez, C., Jinek, M., & Palermo, G. (2024). An alpha-helical lid guides the target DNA toward catalysis in CRISPR-Cas12a. Nature Communications, 15(1), 1473.https://www.nature.com/articles/s41467-024-45762-6

[56]. Nierzwicki, Ł., Ahsan, M., & Palermo, G. (2023). The electronic structure of genome editors from the first principles. Electronic Structure, 5(1), 014003.DOI https://doi.org/10.1088/2516-1075/acb410

[57]. Bali, S. D., Ahsan, M., &Revanasiddappa, P. D. (2023). Structural Insights into the Antiparallel G-Quadruplex in the Presence of K+ and Mg2+ Ions. The Journal of Physical Chemistry B, 127(7), 1499-1512.https://doi.org/10.1021/acs.jpcb.2c05128
[58]. Ahsan, M., Pindi, C., &Senapati, S. (2022). Mechanism of darunavir binding to monomeric HIV-1 protease: A step forward in the rational design of dimerization inhibitors. Physical Chemistry Chemical Physics, 24(11), 7107-7120.https://doi.org/10.1039/D2CP00024E

[59]. Ahsan, M., Pindi, C., &Senapati, S. (2021). Hydrogen bonding catalysis by water in epoxide ring opening reaction. Journal of Molecular Graphics and Modelling, 105, 107894.https://doi.org/10.1016/j.jmgm.2021.107894

[60]. Ahsan, M., Pindi, C., &Senapati, S. (2020). Electrostatics plays a crucial role in HIV-1 protease substrate binding, drugs fail to take advantage. Biochemistry, 59(36), 3316-3331. https://doi.org/10.1021/acs.biochem.0c00341

[61]. Pindi, C., Chirasani, V. R., Rahman, M. H., Ahsan, M., Revanasiddappa, P. D., &Senapati, S. (2020). Molecular basis of differential stability and temperature sensitivity of ZIKA versus

dengue virus protein shells. Scientific Reports, 10(1), 8411.https://doi.org/10.1038/s41598-020-65288-3
[62]. Ahsan, M., &Senapati, S. (2019). Water plays a cocatalytic role in epoxide ring opening reaction in aspartate proteases: a QM/MM study. *The Journal of Physical Chemistry B*, *123*(38), 7955-7964.
https://doi.org/10.1021/acs.jpcb.9b04575
[63]. Dixit, S. M., Ahsan, M., &Senapati, S. (2019). Steering the lipid transfer to unravel the mechanism of cholesteryl ester transfer protein inhibition. Biochemistry, 58(36), 3789-3801.
https://doi.org/10.1021/acs.biochem.9b00301

[64]. Hasan, M. R., Gazi, M. S., & Gurung, N. (2024). Explainable AI in Credit Card Fraud Detection: Interpretable Models and Transparent Decision-making for Enhanced Trust and Compliance in the USA. *Journal of Computer Science and Technology Studies*, *6*(2), 01-12.

[65]. Gazi, M. S., Hasan, M. R., Gurung, N., & Mitra, A. (2024). Ethical Considerations in AI-driven Dynamic Pricing in the USA: Balancing Profit Maximization with Consumer Fairness and Transparency. *Journal of Economics, Finance and Accounting Studies*, *6*(2), 100-111.

[66]. Sarkar, M., Puja, A. R., & Chowdhury, F. R. (2024). Optimizing Marketing Strategies with RFM Method and K-Means Clustering-Based AI Customer Segmentation Analysis. *Journal of Business and Management Studies*, *6*(2), 54-60.

[67]. Jones, K., Spaeth, J., Rykowski, A., Manjunath, N., Vudutala, S. K., Malladi, R., & Mishra, A. (2020). U.S. Patent No. 10,659,295. Washington, DC: U.S. Patent and Trademark Office.

[68]. Malladi, R., Bukkapattanam, A., Wigley, C., Aggarwal, N., & Vudutala, S. K. (2021). U.S. Patent No. 11,087,020. Washington, DC: U.S. Patent and Trademark Office.

[69]. Jones, K., Pitchaimani, S., Viswanathan, S., Shah, M., Malladi, R., Allidina, A., ... & Brannon, J. B. (2023). U.S. Patent No. 11,797,528. Washington, DC: U.S. Patent and Trademark Office.