INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 86-92

DETECTION OF CYBER-ATTACK IN A NETWORK USING ADVANCED MACHINE LEARNING TECHNIQUES

Dr. M. Venkateswara Rao[1], B. Ramya[2], A. Kiranmayi[3], Ch. Bhavya Sri[4], G. Deepthi[5]

[1]Professor & HoD, Dept. of AI & ML, NRI Institute of Technology, Pothavarappadu, Vijayawada, AP, India.

[2,3,4,5]UG Scholar, Department of CSE, NRI Institute of Technology, Pothavarappadu, Vijayawada, AP, India.

ABSTRACT

In contemporary society, reliance on cyberspace permeates every facet of daily life, leading to an increase in cybercrimes and threats. While novel innovations offer significant advantages to individuals, organizations, and governments, they also introduce vulnerabilities. Critical issues such as safeguarding important data, securing stored information platforms, and ensuring data availability have emerged. Among these concerns, cyber terrorism stands out as a paramount challenge. The proliferation of cyber threats poses significant risks to both individuals and institutions, potentially jeopardizing public and national security. Consequently, the development of Intrusion Detection Systems (IDS) has become imperative to mitigate cyber-attacks. In this study, we employ support vector machine (SVM) algorithms for port scan detection using the latest CICIDS2017 dataset, achieving precision rates of 97.80% and 69.79% respectively.

Keywords: Data Preprocessing, Cyber Attack, SVM, ANN, CNN, Random Forest, CICIDS2017.

1. INTRODUCTION

The utilization of machine learning has become pivotal in the detection of cyber-attacks, with various algorithms being employed for this purpose. This study endeavours to conduct a comparative analysis of different machine learning methodologies utilized in identifying cyber-attacks, drawing insights from diverse metrics. The foundation of this paper lies in a comprehensive literature review of detection techniques deployed in identifying cyber threats. Emphasis is placed on comparing and contrasting different machine learning algorithms through the presentation of a comparative table. However, our practical experience in investigating unsolicited remote port scans has led us to observe a significant trend: a considerable portion of these scans originates from compromised hosts, indicating potential hostile intent. As such, considering port scans as potentially malicious and promptly reporting them to the administrators of the corresponding remote networks appears to be a prudent course of action. Nonetheless, the primary focus of this paper remains on the technical intricacies involved in port scan detection, independent of the interpretation or response strategies associated with such scans. Specifically, our attention is directed towards the detection of port scans through network intrusion detection systems (NIDS), while addressing evasion tactics in a manner conducive to real-world implementation within dynamic network environments.

Within subsequent sections, we aim to provide a clear definition of port scanning, supplemented by illustrative examples and an exploration of evasion techniques employed by attackers. A comprehensive review of existing research pertaining to port scan detection is presented, followed by the introduction of proposed algorithms and preliminary data supporting our approach. Furthermore, potential avenues for extending this research are discussed alongside considerations for broader applications. Throughout this paper, it is assumed that readers possess a foundational understanding of Internet protocols, fundamental concepts related to network intrusion detection and scanning, as well as rudimentary knowledge in probability theory, information theory, and linear algebra.

Port scans serve two primary purposes for attackers: information gathering and disruption. While our primary focus lies in the detection of information-gathering port scans, the threat of malicious flooding with excessive information remains a critical consideration in algorithm design. We introduce the concept of a "scan footprint" to delineate the set of port/IP combinations of interest to attackers, distinct from the scan script, which dictates the temporal sequence of exploration.

2. LITERATURE REVIEW

In the realm of cyber security, Yaokai Feng et al. (2018) introduced a novel machine learning framework aimed at early detection of distributed cyber-attacks. By discerning crucial features from network traffic data, their approach leveraged SVM feature selection alongside a classifier, exhibiting notable efficacy in preempting cyber threats. The study emphasized the pivotal role of feature selection in optimizing algorithmic performance for timely detection of cyber-attacks.

A seminal contribution by R. Christopher (2001), titled "Port scanning techniques and the defense against them," disseminated by the SANS Institute, delineates port scanning as a prevalent strategy utilized by adversaries to pinpoint

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 86-92

exploitable services for system infiltration. Systems tethered to LANs or the Internet via modems often host services across a spectrum of ports, prompting attackers to conduct port scans to glean information about active services, user ownership, anonymous login support, and authentication requirements. Port scanning entails a systematic probing of individual ports, with response characteristics indicating potential vulnerabilities. The significance of port scanners lies in their capacity to uncover security weaknesses, empowering network security practitioners to bolster system defenses. Conversely, the detection and mitigation of port scans are imperative for safeguarding network integrity. Measures such as restricting access to open ports for authorized users and implementing stringent access controls are essential for fortifying system security against potential intrusions.

Limitations of the current system:

1) Stringent regulatory constraints
2) Complexity poses challenges for non-technical users
3) Resource limitations impede functionality
4) Ongoing necessity for frequent patches
5) Persistent vulnerability to cyberattacks

3. PROPOSED SYSTEM

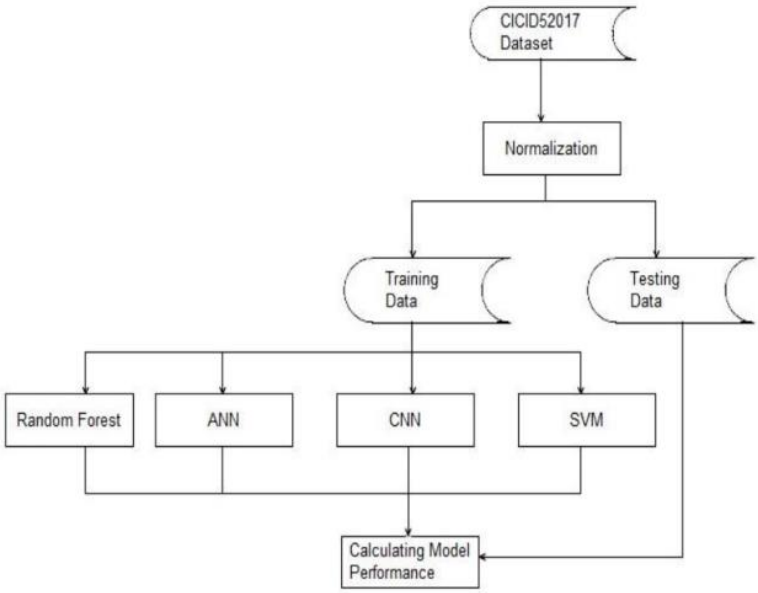
The proposed algorithm entails several crucial steps:

1) Normalization of each dataset.
2) Division of the dataset into testing and training sets.
3) Creation of Intrusion Detection System (IDS) models utilizing RF, ANN, CNN, and SVM algorithms.
4) Evaluation of the performance of each model.

Advantages:

- Enhanced protection against malicious network attacks.
- Identification and removal of malicious elements within an existing network.
- Prevention of unauthorized access to the network by users.
- Restriction of programs from accessing potentially infected resources.
- Enhanced security for confidential information.

SYSTEM DESIGN



4. METHODOLOGY

The SVM, ANN, CNN, Random Forest, and deep learning algorithms were applied to detect port scan attempts using the CICIDS2017 dataset. The methodology's flowchart is depicted in the accompanying figure. Initially, 692,703 records from the dataset underwent standardization. Subsequently, these standardized records were divided into a 75% training dataset and a 25% testing dataset. Finally, the models were evaluated using the testing dataset, and their performance metrics were computed accordingly.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

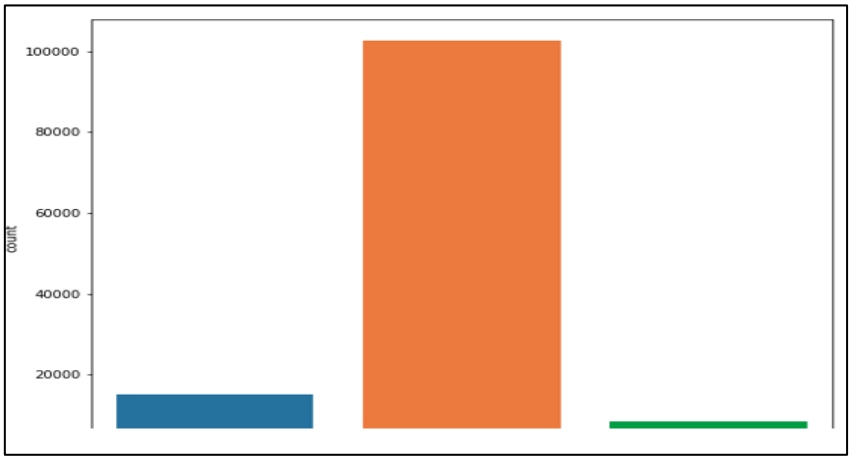
www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 86-92

5. RELATED WORK

1. DDoS Attacks: A Distributed Denial-of-Service (DDoS) Attack floods a server with internet traffic, aiming to disrupt access to linked online services and websites.
2. Malware: Any software or code designed to inflict harm on computers, networks, or servers is categorized as malware or malicious software.
3. Denial-of-Service (DoS) Attacks: During a DoS attack, users are unable to access email, websites, or other resources controlled by a compromised computer or network, though most of these attacks do not result in data loss.
4. Phishing Attacks: Phishing scams attempt to steal user credentials or sensitive data, often by tricking individuals into providing passwords or account numbers, or by deploying malicious files that can infect systems or devices.
5. Ransomware: Ransomware is a sophisticated form of malwarea that employs strong encryption to hold data or system functionality hostage, exploiting system vulnerabilities.
6. Backdoor Trojans: Backdoor Trojans create a secret entry point on a victim's system, granting attackers full and remote control, which can be utilized for various cybercrimes.
7. IoT-Based Attacks: Any cyber-attack targeting Internet of Things (IoT) devices or networks qualifies as an IoT attack, allowing hackers to compromise devices, steal data, or enlist infected devices in botnets for launching DoS or DDoS attacks.
8. Supply Chain Attacks: Supply chain attacks target trusted third-party vendors providing essential services or software, posing significant risks to the integrity and security of the supply chain ecosystem.

6. RESULTS




```
In [6]: columns=["duration","protocol_type","service","flag","src_bytes","dst_bytes","land",
        "wrong_fragment","urgent","hot","num_failed_logins","logged_in",
        "num_compromised","root_shell","su_attempted","num_root","num_file_creations",
        "num_shells","num_access_files","num_outbound_cmds","is_host_login",
        "is_guest_login","count","srv_count","serror_rate","srv_serror_rate",
        "rerror_rate","srv_rerror_rate","same_srv_rate","diff_srv_rate","srv_diff_host_rate","dst_host_count","dst_host_sr
        "dst_host_diff_srv_rate","dst_host_same_src_port_rate",
        "dst_host_srv_diff_host_rate","dst_host_serror_rate","dst_host_srv_serror_rate",
        "dst_host_rerror_rate","dst_host_srv_rerror_rate","attack","last_flag"]

In [7]: train.columns=columns
        test.columns=columns

In [8]: train.head()

Out[8]:
```

duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	num_failed_logins	logged_in	num_compromised	root_
0	0	udp	other	SF	146	0	0	0	0	0	0	0	0
1	0	tcp	private	S0	0	0	0	0	0	0	0	0	0
2	0	tcp	http	SF	232	8153	0	0	0	0	0	1	0
3	0	tcp	http	SF	199	420	0	0	0	0	0	1	0
4	0	tcp	private	REJ	0	0	0	0	0	0	0	0	0

```
In [9]: test.head()
```

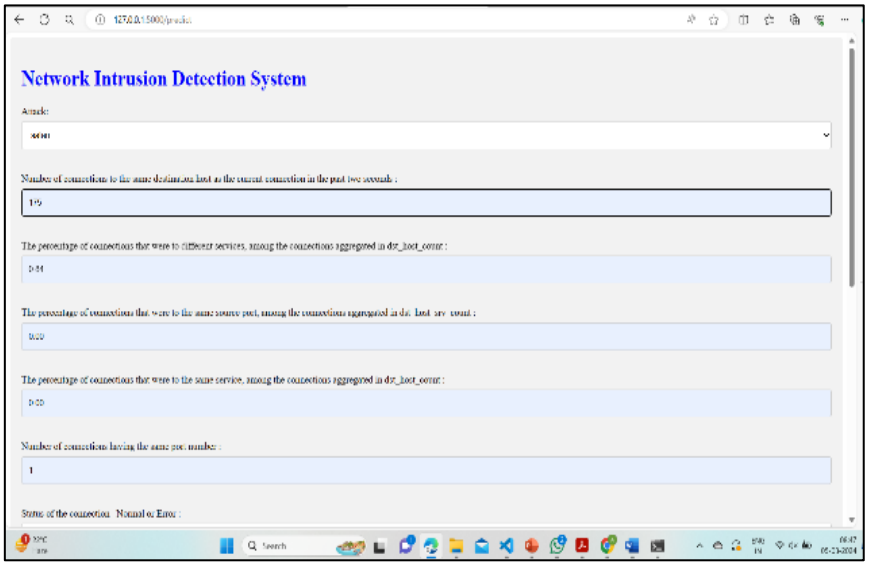
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

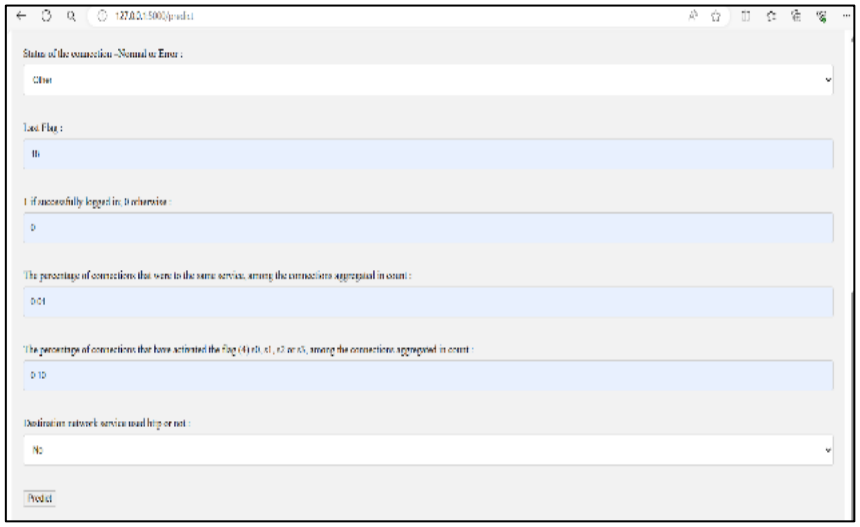
e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 86-92





7. CONCLUSION

In this project, we aim to leverage port scan attempts alongside other attack types using AI and deep learning algorithms, as well as Apache Hadoop and Spark technologies, based on the dataset at hand. The integration of these advanced algorithms enables us to effectively detect cyber-attacks within networks. Over the years, numerous cyber-attacks have occurred, resulting in the accumulation of datasets containing information about the characteristics of these attacks. By utilizing these datasets, we endeavour to predict whether a cyber-attack has taken place. To achieve this, we employ four algorithms: SVM, ANN, RF, and CNN. This research seeks to determine which algorithm yields the highest accuracy rates, thus facilitating the identification of cyber-attacks with greater precision and reliability.

8. REFERENCES

[1] Jeyaselvi, M., M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy. "SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks." Advances in Information Communication Technology and Computing, pp. 461-471. Springer, Singapore, 2022.

[2] V. Praveena, A. Vijayaraj, P. Chinnasamy, I. Ali, R. Alroobaea et al., "Optimal deep reinforcement learning for intrusion detection in uavs", Computers Materials & Continua, vol. 70, no. 2, pp. 2639-2653, 2022.

[3] K. M. Sudar, P. Nagaraj, P. Deepalakshmi and P. Chinnasamy, "Analysis of Intruder Detection in Big Data Analytics", 2021 International Conference on Computer Communication and Informatics (ICCCI), pp. 1-5, 2021.

[4] Ajmeera Kiran and D. Vasumathi, "Optimal Privacy Preserving Technique Over Big Data Analytics Using Oppositional Fruitfly Algorithm", Recent Patents on Computer Science, vol. 13, no. 2, 2020.

[5] V. Padmanaban and M.Nalini, Proceedings of the 2019 international IEEE Conference on Innovations in Information and Communication Technology, (2019).

[6] Jeyaselvi, M., M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy. "SVM-BasedCloning and Jamming Attack Detection in IoT Sensor Networks." Advances in Information CommunicationTechnology and Computing, pp. 461-471. Springer, Singapore, 2022.

[7] Jayapal, P., V. Muvva, and V. Desanamukula. "Stacked extreme learning machine with horse herd optimization: A methodology for traffic sign recognition in advanced driver assistance systems." Mechatronics and Intelligent Transportation Systems 2.3 (2023): 131-145.

[8] Vellela, S.S., Balamanigandan, R. Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023- 15926-5

[9] Vellela, S. S., BashaSk, K., &Yakubreddy, K. (2023). Cloud-hosted concept-hierarchy flex-based infringement checking system. International Advanced Research Journal in Science, Engineering and Technology, 10(3).

[10] Rao, D. M. V., Vellela, S. S., Sk, K. B., &Dalavai, L. (2023). Stematic Review on Software Application Under-distributed Denial of Service Attacks for Group Website. DogoRangsang Research Journal, UGC Care Group I Journal, 13.

[11] K. N. Rao, B. R. Gandhi, M. V. Rao, S. Javvadi, S. S. Vellela and S. KhaderBasha, "Prediction and Classification of Alzheimer's Disease using Machine Learning Techniques in 3D MR Images," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 85-90, doi: 10.1109/ICSCSS57650.2023.10169550.

[12] Venkateswara Reddy, B., Vellela, S. S., Sk, K. B., Roja, D., Yakubreddy, K., &Rao, M. V. Conceptual Hierarchies for Efficient Query Results Navigation. International Journal of All Research Education and Scientific Methods (IJARESM), ISSN, 2455-6211.

[13] S Phani Praveen, RajeswariNakka, AnuradhaChokka, VenkataNagarajuThatha, SaiSrinivasVellela and UddagiriSirisha, "A Novel Classification Approach for Grape Leaf Disease Detection Based on Different Attention Deep Learning Techniques" International Journal of Advanced Computer Science and Applications(IJACSA), 14(6), 2023. http://dx.doi.org/10.14569/IJACSA.2023.01406128

[14] Vellela, S. S., &Balamanigandan, R. (2022, December). Design of Hybrid Authentication Protocol for High Secure Applications in Cloud Environments. In 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 408-414). IEEE.

[15] Vellela, S. S., Balamanigandan, R., & Praveen, S. P. (2022). Strategic Survey on Security and Privacy Methods of Cloud Computing Environment. Journal of Next Generation Technology, 2(1).

[16] Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07).

[17] Sk, K. B., &Vellela, S. S. (2019). Diamond Search by Using Block Matching Algorithm. DIAMOND SEARCH BY USING BLOCK MATCHING ALGORITHM. International Journal of Emerging Technologies and Innovative Research (www. jetir. org), ISSN, 2349-5162.

[18] VenkateswaraRao, M., Vellela, S., Reddy, V., Vullam, N., Sk, K. B., &Roja, D. (2023, March). Credit Investigation and Comprehensive Risk Management System based Big Data Analytics in Commercial Banking. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) (Vol. 1, pp. 2387-2391). IEEE.

[19] Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., & Vellela, S. S. (2021). Challenges and issues of data analytics in emerging scenarios for big data, cloud and image mining. Annals of the Romanian Society for Cell Biology, 412-423.

[20] Vellela, S. S., Reddy, B. V., Chaitanya, K. K., &Rao, M. V. (2023, January). An Integrated Approach to Improve E-Healthcare System using Dynamic Cloud Computing Platform. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 776-782). IEEE.

[21] Vullam, N., Vellela, S. S., Reddy, V., Rao, M. V., SK, K. B., &Roja, D. (2023, May). Multi-Agent Personalized Recommendation System in E-Commerce based on User. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1194-1199). IEEE.

[22] Sk, K. B., Vellela, S. S., Yakubreddy, K., &Rao, M. V. (2023). Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation. KhaderBashaSk, Venkateswara Reddy B, SaiSrinivasVellela, KancharakuntYakub Reddy, M VenkateswaraRao, Novel and Secure Protocol for Trusted Wireless Ad-hoc Network Creation, 10(3).

[23] Reddy, N.V.R.S., Chitteti, C., Yesupadam, S., Desanamukula, V.S., Vellela, S.S., Bommagani, N.J. (2023). Enhanced speckle noise reduction in breast cancer ultrasound imagery using a hybrid deep learning model. Ingénierie des Systèmesd'Information, Vol. 28, No. 4, pp. 1063-1071. https://doi.org/10.18280/isi.280426

[24] Vellela, S.S., Balamanigandan, R. An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Netw. Appl. 16, 2714–2731 (2023). https://doi.org/10.1007/s12083-023-01558-x

[25] Madhuri, A., Praveen, S. P., Kumar, D. L. S., Sindhura, S., &Vellela, S. S. (2021). Challenges and issues of data analytics in emerging scenarios for big data, cloud and image mining. Annals of the Romanian Society for Cell Biology, 412-423.

[26] Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2022). A New Multi-Level Semi-Supervised Learning Approach for Network Intrusion Detection System Based on the 'GOA'. Journal of Interconnection Networks, 2143047.

[27] Praveen, S. P., Sarala, P., Kumar, T. K. M., Manuri, S. G., Srinivas, V. S., &Swapna, D. (2022, November). An Adaptive Load Balancing Technique for Multi SDN Controllers. In 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1403-1409). IEEE.

[28] Babu, G. B., Gopal, M. V., Srinivas, V. S., & Krishna, V. Efficient Key Generation for Multicast Groups Based on Secret Sharing.

[29] Yakubreddy, K., Vellela, S. S., Sk, K. B., Reddy, V., & Roja, D. (2023). Grape CS-ML Database-Informed Methods for Contemporary Vineyard Management. International Research Journal of Modernization in Engineering Technology and Science, 5(03).

[30] Sk, K. B., Roja, D., Priya, S. S., Dalavi, L., Vellela, S. S., & Reddy, V. (2023, March). Coronary Heart Disease Prediction and Classification using Hybrid Machine Learning Algorithms. In 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1-7). IEEE.

[31] Vellela, S. S., & Sk, B. Khader and B, Venkateswara Reddy and D, Roja and Javvadi, Sravanthi, MOBILE RFID APPLICATIONS IN LOCATION BASED SERVICES ZONE (June 14, 2023). International Journal of Emerging Technologies and Innovative Research, 10(6).

[32] Venkateswara Reddy, B., &KhaderBashaSk, R. D. Qos-Aware Video Streaming Based Admission Control And Scheduling For Video Transcoding In Cloud Computing. In International Conference on Automation, Computing and Renewable Systems (ICACRS 2022).

[33] D, Roja and Dalavai, Lavanya and Javvadi, Sravanthi and Sk, KhaderBasha and Vellela, SaiSrinivas and B, Venkateswara Reddy and Vullam, Nagagopiraju, Computerised Image Processing and Pattern Recognition by Using Machine Algorithms (April 10, 2023). TIJER International Research Journal, Volume 10 Issue 4, April 2023, Available at SSRN: https://ssrn.com/abstract=4428667

[34] S. S. Priya, S. SrinivasVellela, V. R. B, S. Javvadi, K. B. Sk and R. D, "Design And Implementation of An Integrated IOT Blockchain Framework for Drone Communication," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-5, doi: 10.1109/CONIT59222.2023.10205659.

[35] N. Vullam, K. Yakubreddy, S. S. Vellela, K. BashaSk, V. R. B and S. SanthiPriya, "Prediction And Analysis Using A Hybrid Model For Stock Market," 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1-5, doi: 10.1109/CONIT59222.2023.10205638.

[36] S. S. Vellela, V. L. Reddy, R. D, G. R. Rao, K. B. Sk and K. K. Kumar, "A Cloud-Based Smart IoT Platform for Personalized Healthcare Data Gathering and Monitoring System," 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), Ravet IN, India, 2023, pp. 1-5, doi: 10.1109/ASIANCON58793.2023.10270407.

[37] Vellela, S. S., Roja, D., Reddy, V., Sk, K. B., &Rao, M. V. (2023). A New Computer-Based Brain Fingerprinting Technology.

[38] Vellela, S. S., Sk, K. B., Dalavai, L., Javvadi, S., &Rao, D. M. V. (2023). Introducing the Nano Cars Into the Robotics for the Realistic Movements. International Journal of Progressive Research in Engineering Management and Science (IJPREMS) Vol, 3, 235-240.

[39] Kommineni, K. K., Madhu, G. C., Narayanamurthy, R., & Singh, G. (2022). IoT Crypto Security Communication System. In IoT Based Control Networks and Intelligent Systems: Proceedings of 3rd ICICNIS 2022 (pp. 27-39). Singapore: Springer Nature Singapore.

[40] Vellela, S. S., Pushpalatha, D., Sarathkumar, G., Kavitha, C. H., & Harshithkumar, D. (2023). Advanced Intelligence Health Insurance Cost Prediction Using Random Forest. ZKG International, 8.

[41] Vellela, S. S., Chaganti, A., Gadde, S., Bachina, P., & Karre, R. (2023). A Novel Approach for Detecting Automated Spammers in Twitter. V. SAI SRINIVAS, CHAGANTI ASWINI, GADDE SRI MADHURI, BACHINA PADMA PRIYA, KARRE ROHI WALTER, A NOVEL APPROACH FOR DETECTING AUTOMATED SPAMMERS IN TWITTER, Mukt Shabd, 11, 49-53.

[42] Vellela, S. S., Sk, K. B., & Reddy, V. (2023). Cryonics on the Way to Raising the Dead Using Nanotechnology.

[43] Vellela, S. S., Narapasetty, S., Somepalli, M., Merikapudi, V., & Pathuri, S. (2022). Fake News Articles Classifying Using Natural Language Processing to Identify in-article Attribution as a Supervised Learning Estimator. Mukt Shabd Journal, 11.

[44] Vellela, S. S., Sk, K. B., & Venkateswara Reddy, B. " Skin Diseases Detection and Classification using Deep Learning Algorithm Convolutional Neural Network. International Journal of Creative Research Thoughts (IJCRT), ISSN, 2320-2882.

[45] Vellela, S. S., Roja, D., Sowjanya, C., SK, K. B., Dalavai, L., & Kumar, K. K. (2023, September). Multi-Class Skin Diseases Classification with Color and Texture Features Using Convolution Neural Network. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1682-1687). IEEE.

[46] Davuluri, S., Kilaru, S., Boppana, V., Rao, M. V., Rao, K. N., & Vellela, S. S. (2023, September). A Novel Approach to Human Iris Recognition And Verification Framework Using Machine Learning Algorithm. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 2447-2453). IEEE.

[47] Vellela, S. S., Vuyyuru, L. R., MalleswaraRaoPurimetla, N., Dalavai, L., & Rao, M. V. (2023, September). A Novel Approach to Optimize Prediction Method for Chronic Kidney Disease with the Help of Machine Learning Algorithm. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1677-1681). IEEE.

[48] Biyyapu, N., Veerapaneni, E. J., Surapaneni, P. P., Vellela, S. S., & Vatambeti, R. (2024). Designing a modified feature aggregation model with hybrid sampling techniques for network intrusion detection. Cluster Computing, 1-19.

[49] Burra, R. S., APCV, G. R., & Vellela, S. S. (2024). Infinite Learning, Infinite Possibilities: E-Assessment with Image Processing Technologies. International Research Journal of Modernization in Engineering Technology and Science, 6.

[50] Praveen, S. P., Vellela, S. S., & Balamanigandan, R. (2024). SmartIris ML: Harnessing Machine Learning for Enhanced Multi-Biometric Authentication. Journal of Next Generation Technology (ISSN: 2583-021X), 4(1).

[51] Burra, R. S., APCV, G. R., & Vellela, S. S. (2024). Strategic Insights: Unleashing the Power of Big Data Analytics for Credit Investigation and Risk Mitigation in Commercial Banking. INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE, 4(01), 458-464.

[52] Burra, R. S., APCV, G. R., & Vellela, S. S. (2024). Enhancing Ddos Detection Through Semi-Supervised Machine Learning: A Novel Approach for Improved Network Security. International Research Journal of Modernization in Engineering Technology and Science, 6.

[53] Vullam, N., Roja, D., Rao, N., Vellela, S. S., Vuyyuru, L. R., & Kumar, K. K. (2023, November). Enhancing Intrusion Detection Systems for Secure E-Commerce Communication Networks. In 2023 International Conference on the Confluence of Advancements in Robotics, Vision and Interdisciplinary Technology Management (IC-RVITM) (pp. 1-7). IEEE.

[54] Kumar, E. R., Chandolu, S. B., Kumar, K. P. V., Rao, M. V., Muralidhar, V., Nagarjuna, K., & Vellela, S. S. (2023, November). UAVC: Unmanned Aerial Vehicle Communication Using a Coot Optimization-Based Energy Efficient Routing Protocol. In 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET) (pp. 1-5). IEEE.

[55] Reddy, V., Sk, K. B., Roja, D., Purimetla, N. R., Vellela, S. S., & Kumar, K. K. (2023, November). Detection of DDoS Attack in IoT Networks Using Sample elected RNN-ELM. In 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET) (pp. 1-7). IEEE.

[56] Vellela, S. S., Sk, K. B., & Reddy, V. An Intelligent Decision Support System for retrieval of patient's information.