International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

Adversarial Machine Learning for Robust Intrusion Detection Systems

Akhil Mittal
Independent Researcher,USA
Pandi Kirupa Gopalakrishna Pandian
Independent Researcher,USA.

Abstract: In this study, adversarial machine learning to enhance IDS's capability to counterattack sophisticated cyberattacks employed in the investigation. This paper describes challenges in practice of adversarial techniques, performance measurement and ethical issues. In the research proposal, the authors describe the comprehensive and multi-level method of detecting artifacts, building complex models, and gathering data. Researchers stressed important conclusions regarding aggressiveness of privacy-preserving methods, the need for developing new performance metrics, and the tension between robust model and detection performance. The research assists in developing IDS that are both efficient and formally correct in various contexts of a network.

Keywords*: Intrusion,detection, systems, adversarial, Machine Learning, develop, robust*

Introduction

Intrusion detection systems (IDS) ability to stand against other elaborate cyber-attacks is something that has become essential to improve through the use of adversarial machine learning. Better solutions are sorely missing as classical IDS become vulnerable to adversarial instances and forms of evasion. It is the objective of this project to develop a dependable IDS that would be effective at detecting and mitigating strong cyber threats with the use of adversarial machine learning. The vision is to create IDS that are robust against adversarial attacks and maintain high detection rates despite adversarial changes in the environment using adversarial training, model hardening, and adaptive defenses' integration. The work analyzes the challenges brought by malicious machine learning in IDS and provides futuristic solutions to improve the system's stability.

Literature review

Android Malware Classification using Adversarial Machine Learning for Hacking According to the author, Chen *et. al.* 2018, This paper explains how adversarial attacks can threaten the effectiveness of the machine learning-based Android malware detection systems. Thus, to counter such rooted-deceived programs, the authors propose KuafuDet, a two-phase iterative adversarial-based detection system with a similarity-based filter. They divide the type of attackers into three classes and prove how effective the toxin attacks are against existing defense mechanisms. Thus, in non-adversarial environments, KuafuDet achieves the result of 96%, while in adversarial environments, the result does not go below 15%. The technology is easily expandable, works, and is even better than the leading antivirus programs. It reaffirms the consideration of hostile incidents within the process of swinging mobile malware detection and introduces an inventive approach to enhance the protection from these attacks.

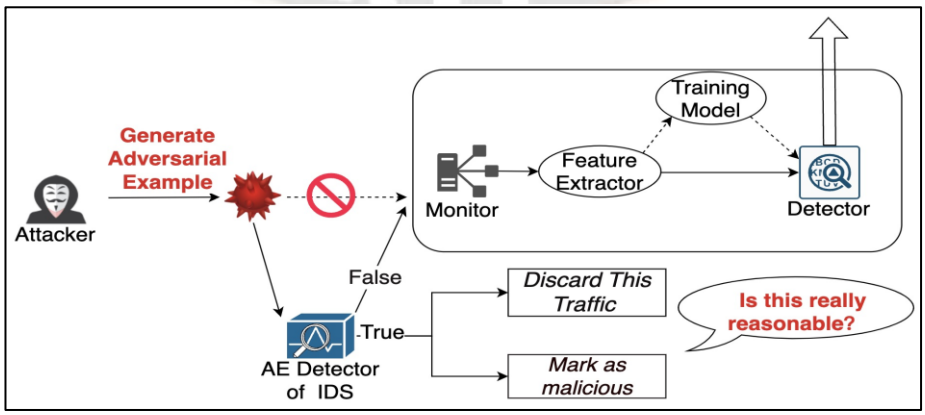

Figure 1: Intrusion Detection network

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

Achievements and Challenges in ML for Image Forensics

According to the author, Nowroozi *et. al.* 2021, the paper discusses the rising relevance of picture forensics to prevent the spread of doctored images, which cause harm to criminal and civil jurisdiction. It highlights the fact that different machine learning approaches are progressively applied in picture forensics for classification, identification, and verification of pictures' origin and integrity. However, the study also revealed that such machine learning-based defenses are very vulnerable to adversarial attacks. These restrictions may lead to rather unfair trials or, in other words, evidence that is inadmissible according to the legal norms. Thus, in image forensics, the authors highlight the need for developing good techniques to protect the learning algorithms, most of all from adversarial examples and counter-forensics tactics.

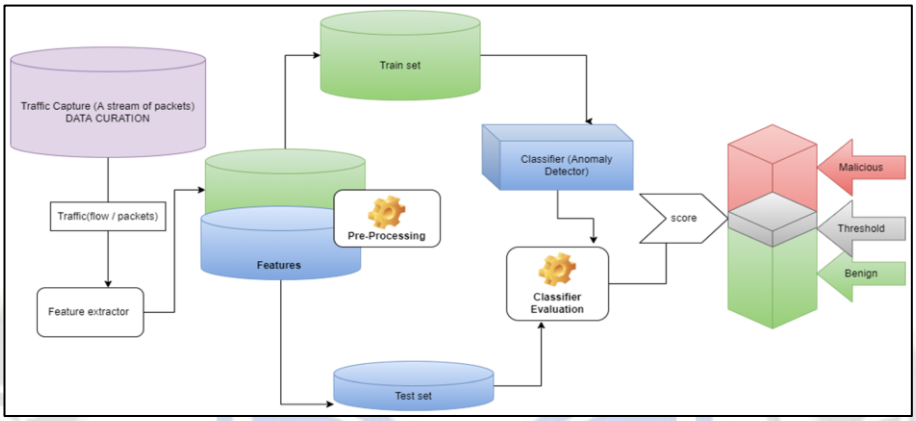

Figure 2 : Intrusion Detection System

(Source: https://www.mdpi.com)

Methods

Data collection and data processing

It is required to form a diverse dataset of the network traffic containing both the shared and abnormal examples in real life. To ensure the inclusion of various attack types and typical traffic patterns, real network traces are used and commonly used data sets(Rathore et al., 2021). The gathered data undergo rich preprocessing; this includes feature extraction process as well as normalization and cleaning process.In order to obtain meaningful structures from raw network data, statistical feature extraction, deep packet analysis, and protocol analysis are employed. To overcome the problem of imbalanced data sets that are characteristic of IDS, undersampling methods are employed like SMOTE or apply oversampling techniques like SMOTE or others. To improve the data set and increase the model's robustness , adversarial examples are generated through techniques like PGD and FGSM. After data processing, the collected dataset is split into training dataset, validation dataset and test dataset. In this way, the attack distribution is kept to all sets by proper stratification if required.

Designing of Machine Learning Models

The strategy involves the development of a large archive of machine learning models designed for accurate intrusion detection(Al-Dujaili et al., 2018). Both conventional and deep learning architectures are investigated: algorithms like Gradient Boosting Machines & Random Forests; SVM with different Kernels; Deep learning models like Convolutional Neural Network & Multilayer Perceptron; Recurrent Neural Network especially for sequential detection like LSTM & GRU. The adversarial training techniques including defensive distillation, gradient masking and input transformation, and augmentation training data with adversarial samples are employed. Protection measures such as spatial smoothing layers and the feature squeezing are integrated into the architecture. A multi-task training strategy for which both the tasks, namely adversarial example detection and its classification into an attack type, are performed concurrently are employed(Qayyum et al., 2020). Efficiency and the robustness of the model can be enhanced and that can be done through the hyperparameter tuning methods such as Grid Search and Bayesian Search.

Implementation and Deployment

A significant task of the implementation phase is to build an efficient and, at the same time, highly portable IDS that includes the intended machine learning algorithms. In model implementation, we utilize high I/O and computation efficient computing libraries or frameworks such as TensorFlow or PyTorch. The general deployment plan is to employ the microservice architecture for the system's clean and scalable design, to utilize Docker for easy and scalable

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

deployment at the container level, and to integrate into the current networks through APIs and network taps. In the current work, our multi-stage pipeline for detecting adversarial examples is created from an adversarial example detection and mitigation layer, feature preprocessing and extraction layer, a layer of trained detection models in its first stage, and an adaptive retraining method designed to handle concept drift in the second stage. Procedures for making and sustaining records to record system behavior and look for potential hostile adversaries are installed(Osahor and Nasrabadi, 2019). Thus, to keep the IDS's capabilities of detecting new threats and ensuring its effectiveness against them, we also include a feedback loop for the model retraining and updating it by the fresh threat data and the identified adversarial samples.

Result

Challenges faced in incorporation of Adversarial Machine Learning for IDS

The following challenges arise when it comes to the implementation of adversarial machine learning for IDS; the process of devising complete datasets that may contain all possible types of attack is not realistic because the threats are constantly evolving, which can lead to model bias or inadequate threat coverage. In addition, the generation of adversarial examples that would be potent without degrading the performance of the IDS is rendered harder as a result of the high dimensionality and intricate nature of network traffic data. One issue is the trade-off between the model's accuracy in detecting attacks and the extent of its non-susceptibility to attacks because overly non-susceptible models may sacrifice the ability to distinguish between attacks' subtle variations.(Frederickson et al., 2018) Also, there may be a significant increase in computing costs in the sense of measly, which reduces the real-time detection skills. Last but not the least, in the cases of security scenarios, where understanding the rationale behind the detections is essential, interpretability of the adversarial trained models gains importance. Methods for data collection, IDS model design, and the specific techniques for improving IDS performance at these stages are yet to be developed.

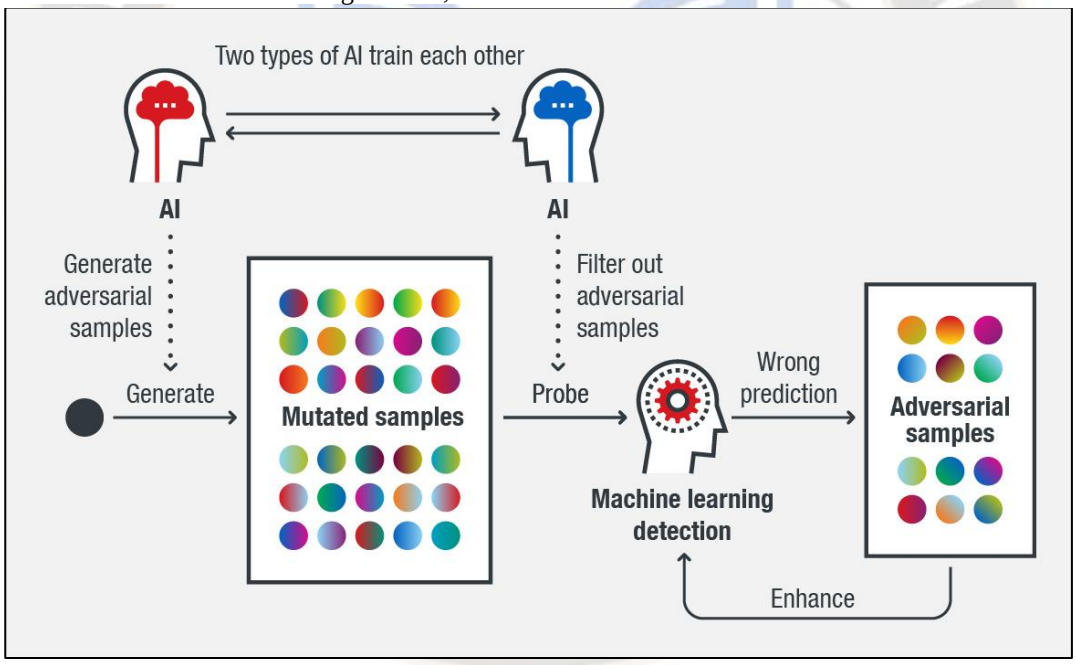

Figure 3 : Adversarial Machine Learning system

(Source: https://media.springernature.com)

Evaluation Metrics and Performance Trade-offs

Adversarial machine learning for IDS has some crucial points that need to be considered concerning the number of parameters and possible consequences. Traditional credentials like recall, accuracy, and precision could possibly be insufficient in expressing the strength of the system before hostilities(Khanapuri et al., 2019). The need to come up with new and standard measures that are geared towards evaluating the model's robustness to different adversarial attacks is indisputable. Sensitivity and robustness often go hand in hand with it, meaning that a more robust system may show a higher false negative ratio in relation to non-malicious threats. The choice of the right evaluation scenarios is critical to do since application in real environments as well as in a video laboratory may behave quite differently at times. Since IDS operates in real-time, the time-based metrics are very relevant in this case. Also, since the opponent is constantly

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*

updating their strategies, it is necessary to assess how effectively the system will be protected from new, unknown threats. When working in developing an IDS that can be described as highly robust the use of adversarial machine learning, it is necessary to consider various types of performance measurement and their interconnection.

Ethical and Privacy Implications

The adversarial machine learning in particular creates serious privacy and ethical issues for intrusion detection systems(Mundra et al., 2020). Due to the need for data gathering used in its operation, or deep packet inspections to identify, intrusions into the privacy of persons using the Internet may be occasioned inadvertently. Adversarial examples used in training may also lead to unexpected behavior in instances that are at the brink, which may cause false positives that maliciously single out specific users or categories of traffic. There is a greater ethical question about the adversarial tactics that mimic actual assaults since such conduct may be considered as endorsing wrong doings. Adversarial ML in IDS may call for new frameworks from a legislative standpoint to ensure that the ethical use of AI and the protection of the law is followed. But the social impact also has to be acknowledged, for instance, that these technologies might be used for censorship or surveillance(Nowroozi et al., 2021). In the context of adversarial machine learning based intrusion detection systems there are challenges that need to be met in terms of ethical and privacy matters in their proper development and implementation.

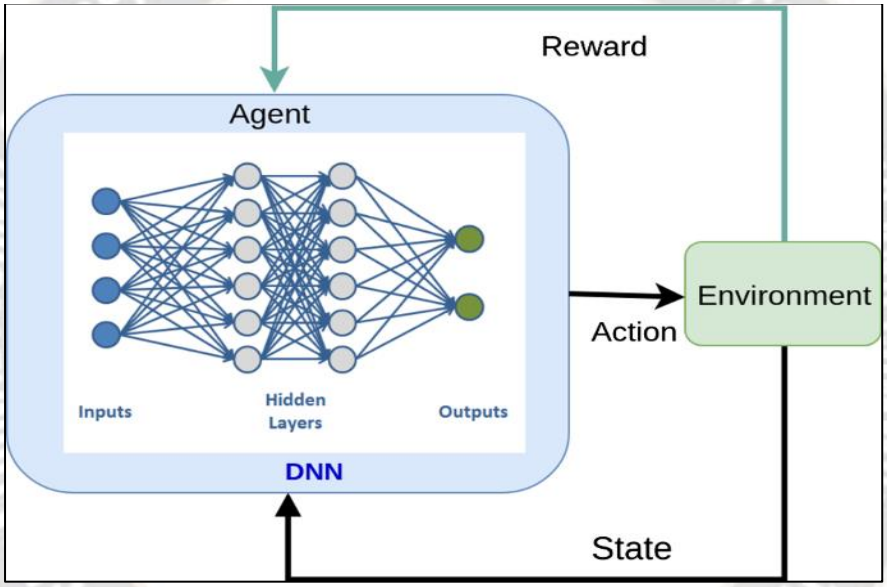

Figure 4 : Intrusion detection system

(Source: https://media.springernature.comg)

Discussion

The following important characteristics are disclosed based on the analysis of adversarial machine learning for the development of robust intrusion systems(Mundra et al., 2020). The problems with implementation raise awareness of the fact that it is not easy to design a good IDS within the context of increasing cyber threats and more importantly require different approaches to data handling and model construction. This paper confirms by evaluating various measurements and performance trade-offs the importance of introducing new more appropriate standards, which should not only detect adversaries' attack rates but also provide efficient overall insight into the system susceptibility. The controversies regarding the ethical and privacy aspects associated with these high-tech systems show that the efficient application of such systems may only be achieved with the consideration of the disadvantages(Chen, and Bourlai, 2017). All these considerations indicate that there is a need to use a multivariable approach to increase the capabilities of adversarial machine learning, which certainly has the potential for improving IDS robustness, while at the same time addressing the contextual factors such as technological advances, ethical considerations, and the actual feasibility of the studied approaches.

Future Directions

Further research in this area should focus on developing more sophisticated approaches to the generation of adversarial examples specific to the network traffic data set. One should also explore how explainable AI techniques can be incorporated to enhance the interpretability of adversarially

trained models. Studying and improving the strategies of transfer learning for better recognition of novel attack patterns can enhance the possibility of IDS enormously. Therefore, there is a desire for research on privacy-preserving adversarial learning to address the ethical issues (Debicha et al., 2021). The results of research would be more regular and objective if global standards and measurement tools for adversarial robustness in IDS were developed. Last of all, exploring the combined associations of federated learning with adversarial machine learning could open applications for more powerful, privacy-preserving intrusion detection systems.

Conclusion

In conclusion adversarial machine learning is a viable approach to building robust IDS against advanced cyber threats. However, there are several challenges hindering the implementation process ranging from ethical dilemmas concerning the model's deployment to technical hurdles in the course of its development. While seeking high resilience, as it is demonstrated in the paper, it is noteworthy that the choice of resistance, accuracy, and time-consuming should be always balanced in the practical applications. Intrusion detection systems need to be adaptive and capable to respond to the new threats; this creates a need for IDS. From the current research, it is expected that future work in this area is going to focus on standardized assessment metrics, enhanced approaches that facilitate privacy preservation, and better explanation and understanding of models. It cannot be denied that the creation of heinous programs or hacking, in the context of adversarial machine learning of intrusion detection systems, will succeed if there are techniques that are not only technically right but also moral and practicable in different network environments.

Reference List

Journals

[1] Chen, S., Xue, M., Fan, L., Hao, S., Xu, L., Zhu, H. and Li, B., 2018. Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach. *computers & security*, *73*, pp.326-344.

[2] Debicha, I., Debatty, T., Dricot, J.M. and Mees, W., 2021. Adversarial training for deep learning-based intrusion detection systems. *arXiv preprint arXiv:2104.09852*.

[3] Chen, L., Ye, Y. and Bourlai, T., 2017, September. Adversarial machine learning in malware detection: Arms race between evasion attack and defense. In *2017 European intelligence and security informatics conference (EISIC)* (pp. 99-106). IEEE.

[4] Frederickson, C., Moore, M., Dawson, G. and Polikar, R., 2018, July. Attack strength vs. detectability dilemma in adversarial machine learning. In *2018 international joint conference on neural networks (IJCNN)* (pp. 1-8). IEEE.

[5] Nowroozi, E., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R., 2021. A survey of machine learning techniques in adversarial image forensics. *Computers & Security*, *100*, p.102092.

[6] Osahor, U.M. and Nasrabadi, N.M., 2019, May. Deep adversarial attack on target detection systems. In *Artificial intelligence and machine learning for multi-domain operations applications* (Vol. 11006, pp. 620-628). SPIE.

[7] Qayyum, A., Usama, M., Qadir, J. and Al-Fuqaha, A., 2020. Securing connected & autonomous vehicles: Challenges posed by adversarial machine learning and the way forward. *IEEE Communications Surveys & Tutorials*, *22*(2), pp.998-1026.

[8] Tuna, O.F., Catak, F.O. and Eskil, M.T., 2022. Closeness and uncertainty aware adversarial examples detection in adversarial machine learning. *Computers and Electrical Engineering*, *101*, p.107986.

[9] Rathore, H., Samavedhi, A., Sahay, S.K. and Sewak, M., 2021. Robust malware detection models: learning from adversarial attacks and defenses. *Forensic Science International: Digital Investigation*, *37*, p.301183.

[10] Mundra, K., Modpur, R., Chattopadhyay, A. and Kar, I.N., 2020, January. Adversarial image detection in cyber-physical systems. In *Proceedings of the 1st ACM workshop on autonomous and intelligent mobile systems* (pp. 1-5).

[11] Khanapuri, E., Chintalapati, T., Sharma, R. and Gerdes, R., 2019, May. Learning-based adversarial agent detection and identification in cyber physical systems applied to autonomous vehicular platoon. In *2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)* (pp. 39-45). IEEE.

[12] Al-Dujaili, A., Huang, A., Hemberg, E. and O'Reilly, U.M., 2018, May. Adversarial deep learning for robust detection of binary encoded malware. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 76-82). IEEE.

[13] Mundra, K., Modpur, R., Chattopadhyay, A. and Kar, I.N., 2020, January. Adversarial image detection in cyber-physical systems. In *Proceedings of the 1st ACM workshop on autonomous and intelligent mobile systems* (pp. 1-5).

[14] Pandi Kirupa Kumari Gopalakrishna Pandian, Satyanarayan kanungo, J. K. A. C. P. K. C. (2022). Ethical Considerations in Ai and Ml: Bias Detection and Mitigation Strategies. International Journal on Recent and Innovation Trends in Computing and

Communication, 10(12), 248–253. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/10511

[15] Ashok : "Ashok Choppadandi, Jagbir Kaur, Pradeep Kumar Chenchala, Akshay Agarwal, Varun Nakra, Pandi Kirupa Gopalakrishna Pandian, 2021. "Anomaly Detection in Cybersecurity: Leveraging Machine Learning Algorithms" ESP Journal of Engineering & Technology Advancements 1(2): 34-41.")

[16] Kaur, J. (2021). Big Data Visualization Techniques for Decision Support Systems. Jishu/Journal of Propulsion Technology, 42(4). https://propulsiontechjournal.com/index.php/journal/article/view/5701

[17] Ashok : "Choppadandi, A., Kaur, J.,Chenchala, P. K., Nakra, V., & Pandian, P. K. K. G. (2020). Automating ERP Applications for Taxation Compliance using Machine Learning at SAP Labs. International Journal of Computer Science and Mobile Computing, 9(12), 103-112. https://doi.org/10.47760/ijcsmc.2020.v09i12.014

[18] Chenchala, P. K., Choppadandi, A., Kaur, J., Nakra, V., & Pandian, P. K. G. (2020). Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. International Journal of Open Publication and Exploration, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127

[19] Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). AI Applications in Smart Cities: Experiences from Deploying ML Algorithms for Urban Planning and Resource Optimization. Tuijin Jishu/Journal of Propulsion Technology, 40(4), 50-56.

[20] Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service . (2019). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98

[21] Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service. International Journal

[22] of Transcontinental Discoveries, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98

[23] Choppadandi, A., Kaur, J., Chenchala, P. K., Kanungo, S., & Pandian, P. K. K. G. (2019). AI-Driven Customer Relationship Management in PK Salon Management System. International Journal of Open Publication and Exploration, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128

[24] Ashok Choppadandi, Jagbir Kaur, Pradeep Kumar Chenchala, Akshay Agarwal, Varun Nakra, Pandi Kirupa Gopalakrishna Pandian, 2021. "Anomaly Detection in Cybersecurity: Leveraging Machine Learning Algorithms" ESP Journal of Engineering & Technology Advancements 1(2): 34-41.

[25] Ashok Choppadandi et al, International Journal of Computer Science and Mobile Computing, Vol.9 Issue.12, December- 2020, pg. 103-112. (Google scholar indexed)

[26] Choppadandi, A., Kaur, J., Chenchala, P. K., Nakra, V., & Pandian, P. K. K. G. (2020). Automating ERP Applications for Taxation Compliance using Machine Learning at SAP Labs. International Journal of Computer Science and Mobile Computing, 9(12), 103-112. https://doi.org/10.47760/ijcsmc.2020.v09i12.014

[27] Chenchala, P. K., Choppadandi, A., Kaur, J., Nakra, V., & Pandian, P. K. G. (2020). Predictive Maintenance and Resource Optimization in Inventory Identification Tool Using ML. International Journal of Open Publication and Exploration, 8(2), 43-50. https://ijope.com/index.php/home/article/view/127

[28] AI-Driven Customer Relationship Management in PK Salon Management System. (2019). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128

[29] Mitul Tilala, Abhip Dilip Chawda, Abhishek Pandurang Benke, Akshay Agarwal. (2022). Regulatory Intelligence: Leveraging Data Analytics for Regulatory Decision-Making. International Journal of Multidisciplinary Innovation and Research Methodology, ISSN: 2960-2068, 1(1), 78–83. Retrieved from https://ijmirm.com/index.php/ijmirm/article/view/77

[30] Tilala, Mitul, and Abhip Dilip Chawda. "Evaluation of Compliance Requirements for Annual Reports in Pharmaceutical Industries." NeuroQuantology 18, no. 11 (November 2020): 138-145. https://doi.org/10.48047/nq.2020.18.11.NQ20244.

[31] Kamuni, Navin, Suresh Dodda, Venkata Sai Mahesh Vuppalapati, Jyothi Swaroop Arlagadda, and Preetham Vemasani. "Advancements in Reinforcement Learning Techniques for Robotics." Journal of Basic Science and Engineering 19, no. 1 (2022): 101-111. ISSN: 1005-0930.

[32] Dodda, Suresh, Navin Kamuni, Jyothi Swaroop Arlagadda, Venkata Sai Mahesh Vuppalapati, and Preetham Vemasani. "A Survey of Deep Learning Approaches for Natural Language Processing Tasks." International Journal on Recent and Innovation Trends in Computing and Communication 9, no. 12 (December 2021): 27-36. ISSN: 2321-8169. http://www.ijritcc.org

[33] Narukulla, Narendra, Joel Lopes, Venudhar Rao Hajari, Nitin Prasad, and Hemanth Swamy. "Real-Time Data Processing and Predictive Analytics Using Cloud-Based Machine Learning." Tuijin Jishu/Journal of Propulsion Technology 42, no. 4 (2021): 91-102.

[34] Nitin Prasad. (2022). Security Challenges and Solutions in Cloud-Based Artificial Intelligence and Machine Learning Systems. International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 286–292. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10750

[35] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76

[36] Shah, J., Prasad, N., Narukulla, N., Hajari, V. R., & Paripati, L. (2019). Big Data Analytics using Machine Learning Techniques on Cloud Platforms. International Journal of Business Management and Visuals, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76

[37] Cygan, Kamil J., Ehdieh Khaledian, Lili Blumenberg, Robert R. Salzler, Darshit Shah, William Olson, Lynn E. Macdonald, Andrew J. Murphy, and Ankur Dhanik. "Rigorous Estimation of Post-Translational Proteasomal Splicing in the Immunopeptidome." bioRxiv (2021): 1-24. https://doi.org/10.1101/2021.05.26.445792

[38] Shah, Darshit, Ankur Dhanik, Kamil Cygan, Olav Olsen, William Olson, and Robert Salzler. "Proteogenomics and de novo Sequencing Based Approach for Neoantigen Discovery from the Immunopeptidomes of Patient CRC Liver Metastases Using Mass Spectrometry." The Journal of Immunology 204, no. 1_Supplement (2020): 217.16-217.16. American Association of Immunologists.

[39] Mahesula, Swetha, Itay Raphael, Rekha Raghunathan, Karan Kalsaria, Venkat Kotagiri, Anjali B. Purkar, Manjushree Anjanappa, Darshit Shah, Vidya Pericherla, Yeshwant Lal Avinash Jadhav, Jonathan A.L. Gelfond, Thomas G. Forsthuber, and William E. Haskins. "Immunoenrichment Microwave & Magnetic (IM2) Proteomics for Quantifying CD47 in the EAE Model of Multiple Sclerosis." Electrophoresis 33, no. 24 (2012): 3820-3829. https://doi.org/10.1002/elps.201200515.

[40] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76

[41] Cygan, K. J., Khaledian, E., Blumenberg, L., Salzler, R. R., Shah, D., Olson, W., & ... (2021). Rigorous estimation of post-translational proteasomal splicing in the immunopeptidome. bioRxiv, 2021.05.26.445792.

[42] Mahesula, S., Raphael, I., Raghunathan, R., Kalsaria, K., Kotagiri, V., Purkar, A. B., & ... (2012). Immunoenrichment microwave and magnetic proteomics for quantifying CD 47 in the experimental autoimmune encephalomyelitis model of multiple sclerosis. Electrophoresis, 33(24), 3820-3829.

[43] Mahesula, S., Raphael, I., Raghunathan, R., Kalsaria, K., Kotagiri, V., Purkar, A. B., & ... (2012). Immunoenrichment Microwave & Magnetic (IM2) Proteomics for Quantifying CD47 in the EAE Model of Multiple Sclerosis. Electrophoresis, 33(24), 3820.

[44] Raphael, I., Mahesula, S., Kalsaria, K., Kotagiri, V., Purkar, A. B., Anjanappa, M., & ... (2012). Microwave and magnetic (M2) proteomics of the experimental autoimmune encephalomyelitis animal model of multiple sclerosis. Electrophoresis, 33(24), 3810-3819.

[45] Salzler, R. R., Shah, D., Doré, A., Bauerlein, R., Miloscio, L., Latres, E., & ... (2016). Myostatin deficiency but not anti-myostatin blockade induces marked proteomic changes in mouse skeletal muscle. Proteomics, 16(14), 2019-2027.

[46] Shah, D., Anjanappa, M., Kumara, B. S., & Indiresh, K. M. (2012). Effect of post-harvest treatments and packaging on shelf life of cherry tomato cv. Marilee Cherry Red. Mysore Journal of Agricultural Sciences.

[47] Shah, D., Dhanik, A., Cygan, K., Olsen, O., Olson, W., & Salzler, R. (2020). Proteogenomics and de novo sequencing based approach for neoantigen discovery from the immunopeptidomes of patient CRC liver metastases using Mass Spectrometry. The Journal of Immunology, 204(1_Supplement), 217.16-217.16.

[48] Shah, D., Salzler, R., Chen, L., Olsen, O., & Olson, W. (2019). High-Throughput Discovery of Tumor-Specific HLA-Presented Peptides with Post-Translational Modifications. MSACL 2019 US.

[49] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76

[50] Pavan Ogeti, Narendra Sharad Fadnavis, Gireesh Bhaulal Patil, Uday Krishna Padyana, Hitesh Premshankar Rai. (2022). Blockchain Technology for Secure and Transparent Financial Transactions. European Economic Letters (EEL), 12(2), 180–188. Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1283

[51] Fadnavis, N. S., Patil, G. B., Padyana, U. K., Rai, H. P., & Ogeti, P. (2021). Optimizing scalability and performance in cloud services: Strategies and solutions. International Journal on Recent and Innovation Trends in Computing and Communication, 9(2), 14-23. Retrieved from http://www.ijritcc.org

[52] Challa, S. S. S., Tilala, M., Chawda, A. D., & Benke, A. P. (2021). Navigating regulatory requirements for complex dosage forms: Insights from topical, parenteral, and ophthalmic products. NeuroQuantology, 19(12), 971-994. https://doi.org/10.48047/nq.2021.19.12.NQ21307

[53] Fadnavis, N. S., Patil, G. B., Padyana, U. K., Rai, H. P., & Ogeti, P. (2020). Machine learning applications in climate modeling and weather forecasting. NeuroQuantology, 18(6), 135-145. https://doi.org/10.48047/nq.2020.18.6.NQ20194