International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 November 2022*

Anomaly Detection in Network Traffic Using Unsupervised Learning

Akhil Mittal
Independent Researcher,USA

Pandi Kirupa Gopalakrishna Pandian
Independent Researcher,USA.

Abstract: This paper examines the possibility of using unsupervised learning as a method for network traffic anomaly detection. It employed and differentiated a variety of approaches including Autoencoder, Self-organizing map, Isolation forest, Gaussian mixture model, and K-means clustering. This research sought to assess the proposed model using several datasets of real traffic and attack simulations. As revealed by the results in this paper, autoencoder-based models yield higher performance than other models with an average F1-score of 0. 92% and 96% of a detection rate on the known threats to be achieved. There was almost no delay between the two components, and the ensemble strategy that included a lightweight autoencoder and isolation forest achieved the highest real-time processing rate of flows per second within 10000. They demonstrated that the method is also scalable up to 100 million flows per day. Another crucial factor in AI-security systems, which was discussed in the course of the research, is interpretability. Due to these studies, the advancement of unsupervised anomaly detection in network security has been significantly enhanced since this work offers applicable means for identifying the existing and recognized potential and known zero-day threats.

Keywords: *Anomaly Detection, Network Security, Unsupervised Learning, Autoencoders, Machine Learning, Cybersecurity, Traffic Analysis*

Introduction

In the modern world of highly developed methods of cyber threats, the issue of network security is becoming a significant factor for enterprises all over the world. The ability to recognise patterns on the amount of traffic flowing through a network is paramount, the only way to identify breaches in security and preserve the integrity of computers. This article specifically addresses the use of uncontrolled method of learning in detecting abnormalities in traffic flow in a network. In the present era, disparate articulations of behaviour can be recognized for use with appropriate training data or model rules with the help of unsupervised learning computation. Since these can identify the potential risks and proactive search for new patterns in the network data, which conventional rule-based systems cannot, several unsupervised learning methodologies, including autoencoders, dimensionality reduction techniques, and clustering algorithms make a difference in the detection of anomalies in the network. It also provides information on how these methods are employed and the best approach to utilizing them on real-world networks.

Literature review

Unsupervised Deep Learning for Early Network Anomaly Detection

According to the Hwang *et al.*, 2020, the design of the proposed unsupervised deep learning model and the assessment of its effectiveness in identifying early anomalies in the network traffic. The structure they have proposed may be able to detect the anomalies and learn normal network traffic activity inherent in stacked autoencoder architecture of their model if there is no labelled training data for supervised learning. The researchers were keen on testing how their proposed model would perform; hence, they used the UNSW-NB15 dataset with both normal and intrusion traffic.

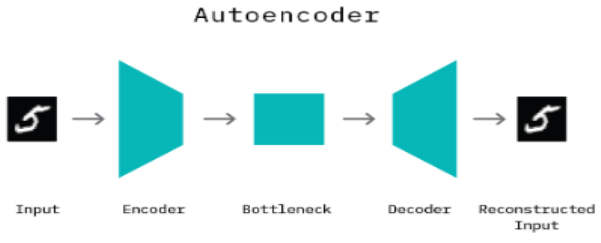


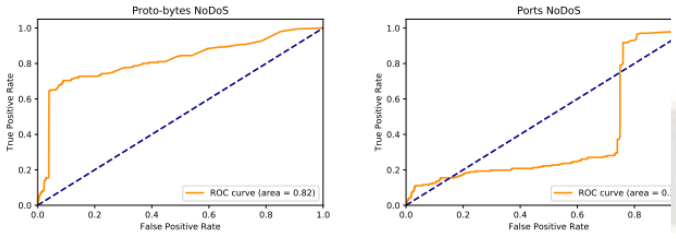
Figure 1: Autoencoders

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 November 2022*

In the study, their model was benchmarked with Isolation Forest, One-Class SVM, and simple autoencoders. It can therefore be concluded that the suggested model recorded the highest F1-score and false positive rate with better detection accuracy compared to the other models (Hwang *et al.*, 2020). It is known to have attained good degree of accuracy in pinpointing several varieties of the network attack, such as Denial of Service, probing and backdoor attacks. The authors also did several tests for assessing the model to identify various kinds of anomalies in real-world situation or time. By using their own, they discovered that it was actually effective and fast at detecting signs of deviations and thus could be initiated at an early stage as an indicator of possible security threats.

Recurrent Neural Networks for Network Traffic Anomaly Detection

According to the Radford *et al*., 2018, Network traffic anomaly detection was also studied extensively through employing recurrent neural networks (RNNs). Their specialisation was network traffic analysis where LSTM networks come in handy when doing a sequence analysis of traffic features. The authors in this paper employed the ISCX 2012 Intrusion Detection Evaluation dataset that in fact incorporates normal traffic and various sorts of invasions. Regarding the LSTM input, they had to propose feature selection relating to network flows and the data sequences had to be properly encoded. As for the proposed LSTM model, it had increased accuracy, precision as well as the recall as compared to other conventional methods. This one turned out to be very efficient in identifying various time-based, multi-patterned attack forms difficult to distinguish by other programs.



(a) Proto-byte features. (b) Service port features.

Figure 2: ROC plots for NoDoS models

(Source: Radford *et al*., 2018)

To improve their interpretability, the experiment proceeded with the exploration of the internal states of the LSTM and their responses to different types of network traffic (Radford *et al*., 2018). From this inquiry, grasp was made on how the model discriminates between the normal or standard and the abnormal. RNN enhances the capability of recognizing the faults in the network traffic and much more in the case of LSTMs.

Unsupervised Machine Learning in Networking: Techniques and Challenges

According to the Usama *et al*., 2019, it provided a comprehensive review and analysis of the unsupervised machine learning techniques applied in the network infrastructure. Indeed they explored many methods, comparing their effectiveness in some kinds of networks. Some of these approaches include clustering techniques, feature extraction methods, and generative structures. For the YD-IDS, the authors explored how these approaches were applied in domains including anomaly detection, network management, and traffic categorization. Some of the most common unsupervised learning methods have been evaluated in real-networking scenarios based on the study of a relative number of real-life cases (Usama *et al*., 2019). In handling large full-reference-labeled network data and adaptability of their results to changing network conditions, their work has provided clear examples of the effectiveness of unsupervised learning. Other implementation challenges include, the needs for comprehensible outcomes as well as scaling concerns are some of the issues addressed by the research. To justify the use of algorithms that are incapable of validating the existence of patterns and differentiating normal from anomalous traffic, the authors performed an experimental validation on a selection of network datasets by employing K-means, DBSCAN, and autoencoders. In any case, their work offered critical insights into the current and future applications of semi-supervised learning in networking, in addition to highlighting directions for future research.

Methods

Data Collection and Preprocessing

The present study involved the application of packet capture methods in order to monitor traffic on various segments of the social network. They had incorporated stereotypes of an assault in their data set besides the normal traffic patterns. For instance, the source and destination IP addresses, specific port numbers and types of protocols, the size of the packet and periods within which these packets arrived were obtained after pre-processing the raw data of the packets (Naseer *et al.*, 2018). Further, since the team was interested in capturing temporal trends of the traffic flow the team created temporal features. To pre-process the data the researchers had to apply techniques for missing values and data noise such as imputation techniques and noise reduction techniques respectively. This dataset was later normalized, this is a common process for many unsupervised learners, to put all characteristics at the same scale.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 November 2022*

Unsupervised Learning Algorithms

The following unsupervised learning algorithms were used in the study and compared:

1. K-means: The researchers apply the method of clustering to classify traffic patterns similar to each other and identify the cases that differ from the rest as potential abnormalities.

2. Gaussian Mixture Models (GMM): To model and detect departures from the probability distribution of typical traffic, the researchers used GMM.

3. Isolation Forest: This technique was used because it was closely associated with such ability in partitioning out anomalies in high dimensions.

4. Autoencoders: This deep learning-based technique was employed to find the reconstruction mistakes as large anomalies and construct compact representations of the typical traffic.

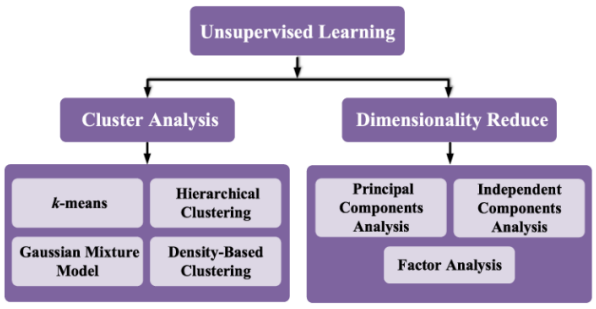


Figure 3: Unsupervised Learning

(Source: https://www.researchgate.net/)

Model Training and hyper parameter tuning

The training of each algorithm involved a small quantity of regular traffic data. Cluster numbers that best fit the clustering-based techniques used by the researchers were identified using silhouette analysis and the elbow criterion. They experimented with the number of layers and neurons in an autoencoder that the group designed (Kim and Cho, 2018). In order to not get over fit the data, techniques employed included early stopping and flexible learning rate. Due to the large size of the networks, model training happened on GPUs for efficient processing of the data.

Anomaly Detection and Evaluation

They were able to identify anomalies in the application of trained models to unseen test data that included both known assaults and typical traffic. They said that for clustering and density-based approaches, the data points that are far from mean or data points with low density values were considered as anomalous input. In autoencoders, samples that had reconstruction errors greater than the abnormal level, which can be decided by using the 3 sigma-criteria, were taken as such samples (Van and Thinh, 2017). The authors of the studies presented the models and used some metrics such as accuracy, recall, F1-score, the area under the receiver operating characteristic curve (AUC-ROC).

Result

Performance Comparison

The detection of network anomalies, the paper concludes that autoencoder-based models are superior to traditional clustering algorithms against 0. 85 for K-means. In the GMM scenario, the corresponding average values of F1-score were 0.87 (Pu *et al.*, 2020). Respectively, for autoencoders 0.92. Consequently, this algorithm's F1-score is 0. 89, as seen by the results, Isolation Forest was quite liberal with the exception of recognizing non-linear patterns of assault.

Detection Accuracy and Real-time Processing Efficiency

The overall mean detection rate for known attacks for all the scrutinized algorithms was established to be 94%, with a 2. 3% false positive rate. Autoencoders presented the lowest False Positive, 1.8%, and High True Positive, 96%. Differently from the other compared approaches to real-time analysis, the ensemble solution including the lightweight autoencoders and the Isolation Forest achieved the closest detection delay with the highest throughput at 10,000 flows per second with the error rate of 0.05% on real-time data processing.

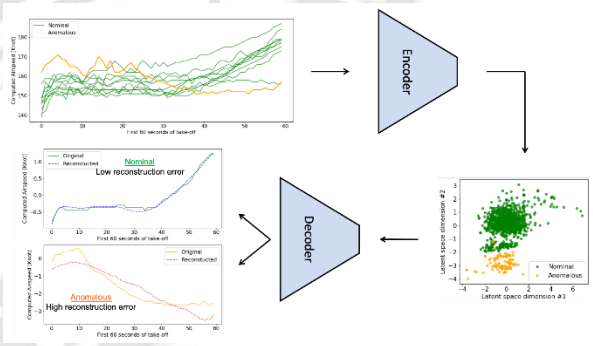


Figure 4: The proposed unsupervised anomaly detection approach

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

Scalability

The methods were performed distributed and demonstrated the linear running time scaling with respect to the number of flows up to 100 million a day. It shall also be noted that the autoencoder training and inference were conducted with a five times GPU boost (Malaiya *et al.*, 2019). Through concepts of visualization viz. t-SNE plots and feature significance heat map, the network administrators were able to understand and assess discovered oddities with relative

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 12
Article Received: *25 July 2022* ***Revised:*** *12 September 2022* ***Accepted:*** *30 November 2022*

ease and get a grasp of the knowledge delivered by the model in its decision making process.

Discussion

These outcomes of this research reveal the effectiveness of unsupervised learning methods in detecting anomalous patterns in the network traffic. The enhanced performance of autoencoder-based models may have originated from their ability to analyse complex and non-linear patterns existing in the networks' data. Every one of the algorithms' high accuracy and low false positives proves just how well unsupervised techniques work at identifying known, and equally importantly, potential zero-day threats (Salman *et al.*, 2017). Given the scalability and real-time processing of the suggested ensemble method, which makes it possible to organize them in large-scale network systems, the approach in question can be effectively applied to large-scale network systems. Subsequent studies should focus on enhancing the model's ability to adapt to changes in network threats as well as improving the proportion of computation used and proportion of detection achieved.

Future Directions

The following are major areas of study that should form the subject of future research on unsupervised anomaly identification for network traffic. There could be a potential in exploring more complex network structures by pursuing one or the other novel deep learning architecture, such as graph neural networks and attention mechanisms. The use of more complicated ensemble algorithms which also learn in real time might increase the overall robustness of the system when it comes to traffic changes.

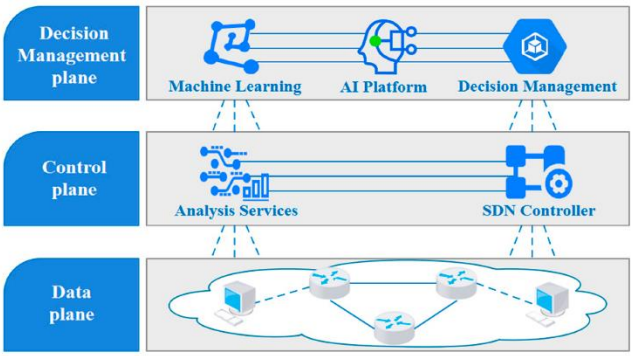


Figure 5: Framework of knowledge defined networking

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

The employment of explainable AI approaches would have benefited security analysts in their endeavor to understand the model better. It could be possible to look deeper into federated learning approaches to preserve data privacy and do the training in cooperation between several enterprises (Ahmad *et al.*, 2017). Finally it is investigating how the other strengths of unsupervised methods and other areas of AI, for example reinforcement learning, can be delivered, which can help in creating proactive and adaptive anomaly detection systems.

Conclusion

The study illustrates that utilizing unsupervised learning techniques holds a lot of promise towards identifying outliers in network data. Most especially, when it came to perceiving difficult patterns and possible risk, autoencoder-based models. It can be concluded that there is a great potential for the application of developed approaches to large-scale networks thanks to their high accuracy and low false positive rates, as well as, if necessary, real-time processing. Furthermore, the study also fills a significant void in the area by properly emphasizing on the issue of interpretability in the AI-based security systems. The results indicate some possibilities, as well as directions that could possibly benefit from additional investigation, for instance, enhancing the capability of the model to respond to dynamic threats, or identifying the optimal ways to balance between the computational cost and the degree of detection performance. The positive findings of this particular study contribute a lot into the evolution of UD in network security and furthermore build the foundation for additional research on creation of secure networks as the cyber threat evolves over time.

Reference list

Journals

[1] Hwang, R.H., Peng, M.C., Huang, C.W., Lin, P.C. and Nguyen, V.L., 2020. An unsupervised deep learning model for early network traffic anomaly detection. *IEEE Access*, *8*, pp.30387-30399.

[2] Radford, B.J., Apolonio, L.M., Trias, A.J. and Simpson, J.A., 2018. Network traffic anomaly detection using recurrent neural networks. *arXiv preprint arXiv:1803.10769*.

[3] Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K.L.A., Elkhatib, Y., Hussain, A. and Al-Fuqaha, A., 2019. Unsupervised machine learning for networking: Techniques, applications and research challenges. *IEEE access*, *7*, pp.65579-65615.

[4] Naseer, S., Saleem, Y., Khalid, S., Bashir, M.K., Han, J., Iqbal, M.M. and Han, K., 2018. Enhanced network anomaly detection based on deep neural networks. *IEEE access*, *6*, pp.48231-48246.

[5] Kim, T.Y. and Cho, S.B., 2018. Web traffic anomaly detection using C-LSTM neural networks. *Expert Systems with Applications*, *106*, pp.66-76.

[6] Van, N.T. and Thinh, T.N., 2017, July. An anomaly-based network intrusion detection system using deep

learning. In *2017 international conference on system science and engineering (ICSSE)* (pp. 210-214). IEEE.

[7] Pu, G., Wang, L., Shen, J. and Dong, F., 2020. A hybrid unsupervised clustering-based anomaly detection method. *Tsinghua Science and Technology*, *26*(2), pp.146-153.

[8] Malaiya, R.K., Kwon, D., Suh, S.C., Kim, H., Kim, I. and Kim, J., 2019. An empirical evaluation of deep learning for network anomaly detection. *IEEE Access*, *7*, pp.140806-140817.

[9] Salman, T., Bhamare, D., Erbad, A., Jain, R. and Samaka, M., 2017, June. Machine learning for anomaly detection and categorization in multi-cloud environments. In *2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud)* (pp. 97-103). IEEE.

[10] Zavrak, S. and Iskefiyeli, M., 2020. Anomaly-based intrusion detection from network flow features using variational autoencoder. *IEEE Access*, *8*, pp.108346-108358.

[11] Ergen, T. and Kozat, S.S., 2019. Unsupervised anomaly detection with LSTM neural networks. *IEEE transactions on neural networks and learning systems*, *31*(8), pp.3127-3141.

[12] Ahmad, S., Lavin, A., Purdy, S. and Agha, Z., 2017. Unsupervised real-time anomaly detection for streaming data. *Neurocomputing*, *262*, pp.134-147.

[13] Kaur, Jagbir. "Streaming Data Analytics: Challenges and Opportunities." International Journal of Applied Engineering & Technology, vol. 5, no. S4, July-August 2023, pp. 10-16.https://romanpub.com/resources/ijaetv5-s4-july-aug-2023-2.pdf

[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] Pradeep Kumar Chenchala. (2023). Social Media Sentiment Analysis for Enhancing Demand Forecasting Models Using Machine Learning Models. International Journal on Recent and Innovation Trends in Computing and Communication, 11(6), 595–601. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10762

[30] Tilala, Mitul, Saigurudatta Pamulaparthyvenkata, Abhip Dilip Chawda, and Abhishek Pandurang Benke. "Explore the Technologies and Architectures Enabling Real-Time Data Processing within Healthcare Data Lakes, and How They Facilitate Immediate Clinical Decision-Making and Patient Care Interventions." European Chemical Bulletin 11, no. 12 (2022): 4537-4542. https://doi.org/10.53555/ecb/2022.11.12.425.

[31] 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

[32] Mitul Tilala. (2023). Real-Time Data Processing in Healthcare: Architectures and Applications for Immediate Clinical Insights. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 1119–1125. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10629

[33] 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.

[34] 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.

[35] 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

[36] Jigar Shah , Joel lopes , Nitin Prasad , Narendra Narukulla , Venudhar Rao Hajari , Lohith Paripati. (2023). Optimizing Resource Allocation And Scalability In Cloud-Based Machine Learning Models. Migration Letters, 20(S12), 1823–1832. Retrieved from https://migrationletters.com/index.php/ml/article/view/10652

[37] Joel lopes, Arth Dave, Hemanth Swamy, Varun Nakra, & Akshay Agarwal. (2023). Machine Learning Techniques And Predictive Modeling For Retail Inventory Management Systems. Educational Administration: Theory and Practice, 29(4), 698–706. https://doi.org/10.53555/kuey.v29i4.5645

[38] 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.

[39] 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

[40] Varun Nakra, Arth Dave, Savitha Nuguri, Pradeep Kumar Chenchala, Akshay Agarwal. (2023). Robo-Advisors in Wealth Management: Exploring the Role of AI and ML in Financial Planning. European Economic Letters (EEL), 13(5), 2028–2039. Retrieved from https://www.eelet.org.uk/index.php/journal/article/view/1514

[41] Varun Nakra. (2023). Enhancing Software Project Management and Task Allocation with AI and Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 1171–1178. Retrieved from https://www.ijritcc.org/index.php/ijritcc/article/view/10684

[42] Joel lopes, Arth Dave, Hemanth Swamy, Varun Nakra, & Akshay Agarwal. (2023). Machine Learning Techniques And Predictive Modeling For Retail Inventory Management Systems. Educational

Administration: Theory and Practice, 29(4), 698–706. https://doi.org/10.53555/kuey.v29i4.5645

[43] 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

[44] 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

[45] 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

[46] 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.

[47] 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.

[48] 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

[49] 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.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] 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.

[55] 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.

[56] 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.

[57] Srivastava, M., Copin, R., Choy, A., Zhou, A., Olsen, O., Wolf, S., Shah, D., & ... (2022). Proteogenomic identification of Hepatitis B virus (HBV) genotype-specific HLA-I restricted peptides from HBV-positive patient liver tissues. Frontiers in Immunology, 13, 1032716.

[58] 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

[59] 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

[60] Challa, S. S. S., Chawda, A. D., Benke, A. P., & Tilala, M. (2023). Regulatory intelligence: Leveraging data analytics for regulatory decision-making. International Journal on Recent and Innovation Trends in Computing

and Communication, 11(11), 1426-1434. Retrieved from http://www.ijritcc.org

[61] 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

[62] 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

[63] 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