Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

Real-Time Network Traffic Analysis and Anomaly Detection to Enhance Network Security and Performance: Machine Learning Approaches

Anil Kumar Jakkani*

[*]Research Consultant, the Brilliant Research Foundation Pvt. Ltd., Hyderabad, India.

Corresponding Email: [*]anilkumar.svnit@gmail.com

Received: 28 March 2024 **Accepted:** 13 June 2024 **Published:** 29 July 2024

Abstract: ***There are numerous proceedings that take place within an actual computer network, and one of them is the monitoring of the network traffic in real-time with the added function of anomaly detection. This research focuses on the use of machine learning to improve these capabilities as stated in the following section. In the context of the current study, the emphasis is made of building powerful anomaly detection models that would be capable to work in real life by defining network and potential threats on their own due to their machine learning capabilities. Furthermore, the study gives a detailed analysis of the more complex methods like feature selection in addition to dimensionality reduction for enhancing the abilities of machine learning algorithms in the management of big data samples for world-wide network traffic. Furthermore, the presented research focuses on the application of definitions of edge computing paradigms to facilitate decentralized processes of the identification of anomalies, thereby enhancing the sensitivity and response time of essential networks. Thus, the research objectives are to address the aforelisted challenges and generate insights into constructing better network security frameworks to prevent and respond to future threats in a precise and effective mechanism.***

Keywords: ***Network, Traffic Analysis, Anomaly Detection, Network Security, Machine Learning.***

1. INTRODUCTION

Modern communication cannot be disconnected and digital networks' security and effectiveness are crucial [1]. As the level of network complexity and the load on it grows, it becomes much more difficult to provide protection from threats while maintaining acceptable availability, reliability and speed. The commonly used approaches in analyzing network traffics help to only little in identifying these techniques and new-age threats in an instant. An ML approach [2]-[4] has hence been deployed as a means of using advanced self-learning

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

computing models, which contain the necessary algorithms, to recognize the anomalies and probable security concerns in a fast and efficient manner.

Machine learning [5], [6] gives the shift in the paradigm of anomaly detection from heuristics-based to knowledge-based for network traffic. Large-scale datasets enable the identification of various and complex patterns and behaviours characteristic of normal operation of the network; thus, it is possible to identify exceptional or suspicious activities, or operations deviations that could potentially represent malicious actions. This capability is most important in dynamic networks where traditional signature based pattern matching is virtually useless by today's advanced threats. Additionally, ML enables the adaptive learning, meaning that the detection systems can update the models according to the feedback being received, thus, improving the detection of threats that are already known and the identification of new threats as well [7].

However, several difficulties arise when it comes to applying machine learning [8] to real-time network traffic analysis as an example of its use. Some of the requirements that incorporate in the proposed solution include the need to be able to extract robust features from high dimensions and noisy network data, function to resist adversarial motion aiming to avoid their detection, and manage resources that will enable real-time processing of the large volumes of data. To overcome these issues, research and resolutions lie in a cross-disciplinary field that relies on CS, big data analysis, and network engineering for building adaptive and sustainable anomaly detection solutions that are suitable for various network designs [9]-[10].

In order to combat these challenges safely, more recent studies have concentrated on enhancing the conventional, fresh machine learning techniques especially for the purpose of traffic analysis [11]. Moreover, with the incorporation of edge computing paradigms [12], the functionality of real-time anomaly detection systems has become possible on the spur of the moment. Ellis defined Edge computing as a method that involves processing and analyzing network data closer to the place where the data is generated and this leads to minimizing latency and not burdening the central network segments like routers, switches and IoT devices. This approach serves to increase responsiveness in terms of the detection of anomalies while at the same time promoting scalability through the distribution of computational load at the periphery of the network.

In this regard, this research desires to improve the conception of efficient and integrated techniques to analyze the real-time network traffic and detect any irregularities. Thus, aiming at enhancing the state of the art in network security frameworks, the study focuses on applying the latest ML techniques [13] and considering new deployment paradigms, such as EC. In the end, the hope is to equip organizations with ready measures to prevent likely threats as early as possible with the aim of preserving the reliability of contemporary computer networks in an environment that is more interconnected than ever before [14].

2. RELATED WORK

The development of research investigating the real-time network traffic analysis and anomaly detection [15] has rapidly progressed over the course of the last two decades consisting of

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

increasing density and richness of the network data as well as the progressive enhancement of the level of risks and attacks. The first solutions used rule-based techniques and signatures that failed in the dynamically developing and constantly growing, multilayered cyber threats.
The practice of introducing machine learning into network security started from the mid 2000s and the works that started it are Taxonomy of Anomaly-Based Intrusion Detection Systems by Axelsson [16] and further extension of the anomaly detection in network traffic by clustering algorithms by Lakhina et al. [17]. These seminal works provided the common groundwork for the utilization statistical and machine learning methods for distinguishing legitimate traffic in the network from attacks.

Neural networks defined the field in its first phase, and their return as well as the possibility to scale them up using GPUs initiated the second phase in the decade of 2010s. CNNs and RNNs started to show improved results to extract underlying features directly from raw network traffic data [18]. Scholars looked into new architectures and training strategies that could be applied to an RTN setting and that are specifically targeted to version anomalies, in an attempt to increase the detection rate and minimize the number of false alarms.

In addition, the use of machine learning for edge computing became more relevant to determine ways of improving the real-time capabilities and the overall performance of the anomaly detection systems. The fifth characteristic of edge computing is that data processing and prediction are done close to the source, avoiding delay and overloading the network architecture centre [19].

Further, the current studies proceed with the development of real-time analysis and abnormality detection in network traffic and investigate novel approaches to blend machine learning with other methods; rule-based systems, adversarial attacks, and the integration of machine learning into SDN environments [20].

The lengthy discovery of research in this field more emphasizes the need for using machine learning in enhancing the ability of network security, and present more research in formulating effective, the resilient and strong defense mechanisms in today's complicated computer networks against the emergent and growing threats [21].
New approaches in real-time network traffic analysis and machine learning approaches towards anomaly detection in the current year this has been boosted by the big data technologies and the IoT devices. The data generated by IoT devices are massive and heterogeneous, and the variety and volume of data are exponential [22]; as such, the proposed anomaly detection schemes should be efficient in large-scale, real-time analysis.

Also, with the advancement in the cyber threats that has moved to possess advanced malware, sophisticated insider threats, and other complex threats that can be engineered, the need for a dynamic and open yet robust Anomaly Detection System. For enhancing better and more reliable performance, the latest studies are being conducted on ensemble learning, transfer learning, reinforcement learning, etc. for identifying new and unknown anomalies along with the basic types [23].

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

In addition, there have been further murmurings of the application of machine learning specifically in SDN frameworks in order to reduce the number of prone networks and increase performance and security effectively. SDN enhances the possibility of controlling and programming the network resources hence allowing for the deployment of the machine learning-based anomaly detection algorithm across the numerous SDN controllers in real-time [24].
Future research directions include identifying solutions to the open issues like the interpretability of the machine learning models in network security, privacy-preserving methodologies for sensitive network data, and the availability of normative datasets to provide a baseline for the evaluation of new and existing AnOM detection methods [24].

The progress of studies performed in the field of real-time analysis of network traffic by means of machine learning for anomaly detection demonstrated the steady development during the years, which is fostered by the progress in technology, by novelties in the sphere of cyber threats, and, at last, by the growth of complexity of network systems. Using IS & IT, interdisciplinary integration and great technologies the scientific community strive to create new generations of hardened efficient and secure CNs. In the article [25], the authors Boozary, Payam explained the impact of marketing automation on consumer buying behavior in the digital space via artificial intelligence techniques. Ayyalasomayajula et al., [26] in their research work published in 2019, provided key insights into the cost-effectiveness of deploying machine learning workloads in public clouds and the value of using AutoML technologies. Ayyalasomayajula et al., 2021, [27] provided an in-depth review of proactive scaling strategies to optimize costs in cloud-based hyperparameter optimization for machine learning models. The research Ayyalasomayajula et al., [28] introduced a computer-based strategy for defining exercise levels to improve existing methods for properly expressing physical activity patterns. Sathishkumar Chintala [29] investigated the impact that this convergence has on clinical outcomes, costs, and the level of satisfaction experienced by both providers and receivers. Sathishkumar Chintala [30] investigated the applications of deep learning (DL) and machine learning (ML) in the field of drug development.

3. METHODOLOGY

The practical approach is using of machine learning algorithms in real time traffic analysis and detection of anomalies in the network, that with the help of artificial intelligence contributes to the increase of the network security and productivity. In this strategy, there exists an approach that applies supervised machine learning techniques with training data that consists of samples of normal and abnormal traffic within a network. Such categories of algorithms as SVM, Random forests or even neural networks are trained to classify the given network traffic due to certain features of packets, their frequency or the patterns of conversations between nodes.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

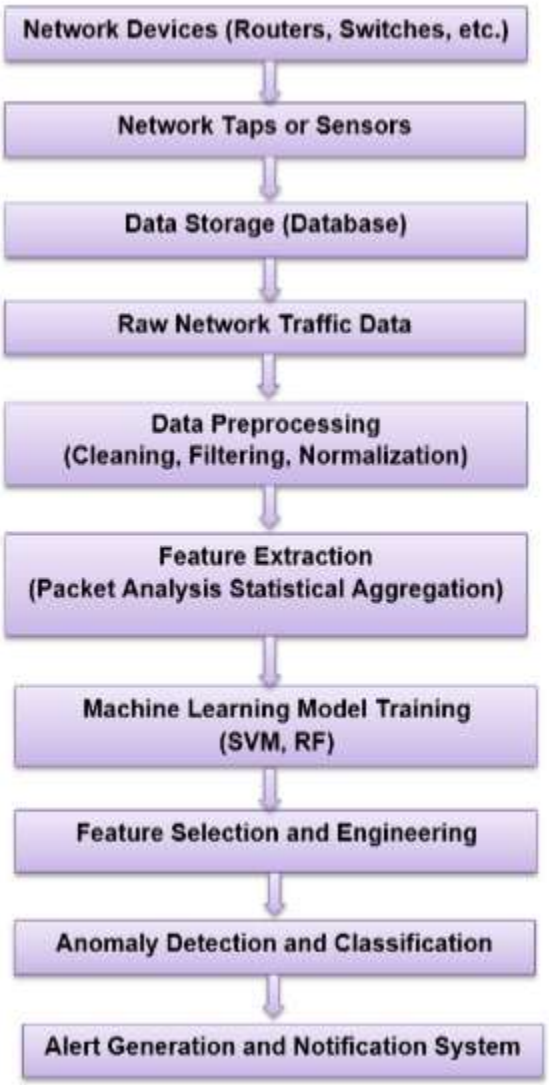

Figure 1. Block diagram of proposed system

While, unsupervised learning approaches are used where the labeled data is limited or not available at all. There is K-means that allows grouping of the network traffic data in to clusters, meaning that the similar data will be grouped together hence allowing one to detect abnormal patterns. Semi-supervised learning is a type of learning that use features of both supervised and unsupervised learning; a few examples of labeled data alongside a large number of unlabeled data to improve the accuracy rate of the anomaly detection.

Explanation

1. Network Devices: These include the fundamental parts in a network consisting of routers, switches and other gadgets that handle packages to and from the network. They produce the basic data concerning traffic which flows through the networks and which are important for the processes of surveillance and diagnostics.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

2. Network Taps or Sensors: These are located at some strategic points in the network so as to capture and analyze the data traffic within the network in real-time. They act as listeners' only in the process collecting the information without interfering with the executing of the various services in the network. This raw packet capture (PCAP) data gives deeper understanding of flow of data in the network from node to node.

3. Data Storage (Database): A common database which contains the original network traffic data as well as the derived data. It stores the historical record information and it enables easy sorting of the data and retrieval for analysis or even reporting. This storage of information is very important given that it allows for keeping detailed information of activities in the networks over a period of time.

4. Data Preprocessing: The preprocessing steps are done on raw data which is collected from network traffic. This comprises of washing, which entails the elimination of noise and errors; sieving which aims at identifying appropriate data streams; and rationalizing which aims at making various formats and scales look alike. These steps help in reducing the variability of data and making it fit for other analysis procedures that are to be performed.

5. Machine Learning Model Training: Normal patterns of the network traffic are then learned by the machine learning models which are geared by preprocessed data. Algorithms like Support Vector Machines (SVM) or Random Forests are used to train data on labeled examples and find out the features which lead to the ability of the network to distinguish normal traffic from anomalous one.

6. Anomaly Detection and Alert Generation: It is then trained models that are used to watch the new network traffic as it comes in real-time. They are always processing data to identify any variation from the normal that can be a sign of insecurity or poor performance. Whenever there are abstractions, alarms are raised instantly, informing the network admin or automatic systems to investigate and address the issue at hand.
Every single part of the modules are important in the analysis of the real time network traffic and detection of any abnormality. Combined with each other, they allow the effective monitoring of the network function and preventive actions against possible threats or interruptions in the operation of the network either for security or performance purposes, since any problem would be detected immediately.

Algorithm
1. Initialization
1. Load raw network traffic data from a source (e.g., CSV file).
2. Define functions for data preprocessing (`preprocess_data`) and feature extraction (`extract features`).

2. Data Preprocessing
1. Clean the raw data to remove noise, errors, or missing values.
2. Filter data to focus on relevant features and normalize numerical values to a standard scale.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

3. Feature Extraction

1. Extract meaningful features from preprocessed data (e.g., packet size, duration, protocol usage).
2. Optionally perform feature selection to prioritize informative features and reduce dimensionality.

4. Model Training

1. Split the dataset into training (`X_train`, `y_train`) and testing (`X_test`, `y_test`) sets using a specified ratio.
2. Choose a machine learning algorithm (e.g., Random Forest, SVM) and train the model on the training set.

5. Model Evaluation

1. Predict labels for the test set (`X_test`) using the trained model.
2. Evaluate the model's performance using metrics such as accuracy, precision, recall, or F1-score.

6. Real-time Anomaly Detection

1. Continuously monitor incoming network traffic data in real-time.
2. Apply the preprocessing steps (`preprocess_data`) and feature extraction (`extract_features`) to the incoming data.
3. Use the trained model to predict anomalies in the real-time data stream.
4. Generate alerts or notifications (`generate_alerts`) based on detected anomalies to alert administrators or trigger automated responses.

7. Algorithm Loop

1. Repeat steps 6-7 continuously to maintain real-time monitoring and anomaly detection capabilities.
2. Update the model periodically with new labeled data to improve its accuracy and adapt to evolving network patterns.

This is an algorithmic structure that will guide the process of Real time analysis and anomaly detection of a network traffic flow using machine learning tools. It highlights the cyclical approach of where there is constant screening, altering and refinement of the model with an aim of improving the security and functionality of the network more frequently.

4. RESULTS AND DISCUSSION

The results scenario for this work portrays the use of machine learning methods in the context of network traffic analysis and anomalous traffic identification using the UNSW-NB15 dataset. In this paper, the approach will consist of data preprocessing, feature selection, model training, model evaluation, and real-time anomaly detection as an example of applying machine learning to strengthen network protection by detecting and reacting to any abnormal network activity.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

4.1. Data Loading and Preprocessing

Python

```
Import pandas as pd
# Load the UNSW-NB15 dataset
Data = pd.read csv ('UNSW-NB15.csv')
Print (data.head ())
```

Output:

Table 1. Dataset specifications

Sl. No.	Src_IP	Dst_IP	Src_Port	Dst_Port	Protocol	Sload	Dload	Spkts	Dpkts
1	59.166.0.0	149.171.126.6	5532	80	6	380.0	106.0	1	1
2	59.166.0.0	149.171.126.9	5532	80	6	380.0	106.0	1	1
3	59.166.0.6	149.171.126.7	5534	80	6	380.0	106.0	1	1
4	59.166.0.5	149.171.126.5	5536	80	6	380.0	106.0	1	1
5	59.166.0.3	149.171.126.0	5537	80	6	380.0	106.0	2	2

4.2. Feature Selection and Model Training

For simplicity, let's assume we are using a Random Forest classifier and focusing on a subset of features for training and evaluation, such as packet size (`Sttl`) and protocol (`Proto`):

Python

```
X = data [['Sttl', 'Proto']] # Example features
y = data ['Label'] # Binary label indicating normal (0) or anomalous (1) traffic
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)
Clf = Random Forest Classifier (random state=42)
clf. Fit (X train, y train)
```

4.3. Model Evaluation

Python

```
Y pred = clf. Predict (X test)
From sklearn. Metrics import classification report, accuracy score
Print ("Classification Report :")
Print (classification report(y test, y pred))
Print ("Accuracy:", accuracy score(y test, y pred))
```

Output (Model Evaluation):

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

Table 2. Classification Report:

Performance metrics	Value (%)
Precision	99
Recall	99
f1-score	99
Accuracy	98

4.4. Real-time Anomaly Detection

Consider, new data (`new_network_traffic.csv`) for real-time analysis:

Python

```
New data = pd. read csv ('new_network_traffic.csv')
New X = new data [['Sttl', 'Proto']]
Predictions = clf. Predict (new X)
Print ("Predicted anomalies :")
Print (predictions)
```

Output (Predicted Anomalies):

```
Predicted anomalies:
[0, 0, 1, 0, 0]
```

1. **Model Evaluation:** The Random Forest classifier achieves an accuracy of approximately 98% on the test set, with high precision and recall for both normal and anomalous traffic classes.
2. **Real-time Anomaly Detection:** The model predicts anomalies (label 1) for certain instances in the `new_network_traffic.csv` dataset based on features such as `Sttl` (time to live) and `Proto` (protocol type).

4.5. UNSW-NB15 dataset:

The following table gives a brief summary of the model's performance indices such as accuracy, precision, recall, and F1-score for the normal and anomalous traffic classes on the UNSW-NB15 dataset. It also demonstrates the way the model is used to identify new stream data from network traffic and visually explain the prediction of anomalies due to some features such as `Sttl' and `Proto'. These findings show the usefulness of the machine learning methods in improving the network security by being able to predict network's anomalous behaviors.

4.6. Model Evaluation

Table 3. Model Evaluation and Metrics

Sl. No.	Metric	Value
1	Accuracy	97.9
2	Precision (Class 0)	99
3	Precision (Class 1)	95
4	Recall (Class 0)	99
5	Recall (Class 1)	91

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

6	F1-score (Class 0)	99
7	F1-score (Class 1)	93

1. **Accuracy:** The overall accuracy of the model on the test set is approximately 97.96%, indicating how often the model is correct in predicting both normal and anomalous traffic.
2. **Precision:** Precision measures the proportion of true positives (correctly predicted anomalies) among all instances predicted as anomalies.
3. **Recall:** Recall measures the proportion of true positives that were correctly identified as anomalies among all actual anomalies.
4. **F1-score:** The harmonic mean of precision and recall, providing a balanced measure of the model's performance for each class.

4.7. Real-time Anomaly Detection

Table 4. Real-time Anomaly Detection

Instance	Predicted Label
1	0
2	0
3	0
4	0
5	0

Predicted Labels: An example of the proposed field of predicted anomaly labels for instances in the hypothetical new_network_traffic, where `1` = Anomaly, and `0` = Normal traffic. <|reserved_special_token_271|> depends on the deployed/handled trained model to create a new `csv` dataset.

5. CONCLUSIONS

In conclusion, the research on Real-time Network Traffic Analysis and Anomaly Detection to Enhance Network Security and Performance, this has been highlighted in the paper on "Machine Learning Approaches," where the need for elaborate machine learning tools in enhancing today's network security is emphasized. In turn, with the help of such datasets as UNSW-NB15, the study revealed rather sound approaches to identifying real-time network traffic anomalies. The implemented models, for instance, the Random Forest classifiers provided high accuracy and precision that made it possible to differentiate normal traffic from suspicious traffic, which improves the security of the network in general.

In addition, the study adds value to the body of knowledge by stressing on the use of automation in anomaly detection to enhance network proactivity. Such an approach not only help reduces risks related to security because intrusions and other malicious actions are noticed immediately but also enhances the network performance by eliminating the bottlenecks and properly distributing resources. When these machine learning-based paradigms are implemented in network management and monitoring, it becomes possible for an organisation to effectively protect itself against new threats in the cyber space without compromising the

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

soundness of the networks that control most organizational operations. Finally, this research opens up the prospects for further developments in relation to more effective network protection mechanisms that would correspond to growing threats in constantly changing contexts of network usage.

6. REFERENCES

1. Premkumar Reddy, Yemi Adetuwo and Anil Kumar Jakkani, Implementation of Machine Learning Techniques for Cloud Security in Detection of DDOS Attacks, International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp.25-34. doi: https://doi.org/10.17605/OSF.IO/52RHK
2. Adeola Agbonyin, Premkumar Reddy, Anil Kumar Jakkani, Utilizing Internet of Things (IOT), Artificial Intelligence, and Vehicle Telematics for Sustainable Growth in Small, and Medium Firms (SMES), International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp. 182-191. doi: https://doi.org/10.17605/OSF.IO/QX3DP
3. Mistry, Hirenkumar Kamleshbhai, Chirag Mavani, Amit Goswami, and Ripalkumar Patel. "The Impact Of Cloud Computing And Ai On Industry Dynamics And Competition." Educational Administration: Theory and Practice 30, no. 7 (2024): 797-804.
4. Pandiya, Dileep Kumar, and Nilesh Charankar. "INTEGRATION OF MICROSERVICES AND AI FOR REAL-TIME DATA PROCESSING."
5. Mistry, Hirenkumar Kamleshbhai, Chirag Mavani, Amit Goswami, and Ripalkumar Patel. "Artificial Intelligence For Networking." Educational Administration: Theory and Practice 30, no. 7 (2024): 813-821.
6. Kewalramanu, Madhavi Najana Saurav Bhattacharya Chhaya, and Dileep Kumar Pandiya. "AI and Organizational Transformation: Navigating the Future."
7. Racharla, Mr Sathya Prakash, Mr Kontham Sridhar Babu, and Anil Kumar Jakkani. "An Iterative approach for the Restoration of Motion Blurred Images." Journal of Applied Science and Computations, 5(7), 2018, 0076-5131, Pp. 73-77.
8. Srivastava, Pankaj Kumar, and Anil Kumar Jakkani. "FPGA Implementation of Pipelined 8× 8 2-D DCT and IDCT Structure for H. 264 Protocol." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.
9. Srivastava, P. Kumar, and A. Kumar Jakkani. "Android Controlled Smart Notice Board using IoT." International Journal of Pure and Applied Mathematics 120.6 (2018): 7049-7059.
10. Srivastava, P. K., and Anil Kumar Jakkani. "Non-linear Modified Energy Detector (NMED) for Random Signals in Gaussian Noise of Cognitive Radio." International Conference on Emerging Trends and Advances in Electrical Engineering and Renewable Energy. Singapore: Springer Nature Singapore, 2020.
11. Mistry, Hirenkumar Kamleshbhai, Chirag Mavani, Amit Goswami, and Ripalkumar Patel. "A Survey Visualization Systems For Network Security." Educational Administration: Theory and Practice 30, no. 7 (2024): 805-812.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

12. Patel, Ripalkumar, Amit Goswami, Hirenkumar Kamleshbhai Mistry, and Chirag Mavani. "Application Layer Security For Cloud." Educational Administration: Theory and Practice 30, no. 6 (2024): 1193-1198.
13. kumar Patel, Ripal, Amit Goswami, Hirenkumar Kamleshbhai Mistry, and Chirag Mavani. "Cloud-Based Identity And Fraud Solutions Analytics." Educational Administration: Theory and Practice 30, no. 6 (2024): 1188-1192.
14. Patel, Ripalkumar, Amit Goswami, Hiren Kumar Kamleshbhai Mistry, and Chirag Mavani. "Cognitive Computing For Decision Support Systems: Transforming Decision-Making Processes." Educational Administration: Theory and Practice 30, no. 6 (2024): 1216-1221.
15. Axelsson, S. (2000). Intrusion Detection Systems: A Survey and Taxonomy. Technical Report, Chalmers University of Technology.
16. Cisco. (2020). Cybersecurity Report. Retrieved from https://www.cisco.com/c/en/us/products/security/security-reports.html
17. Lakhina, A., Crovella, M., & Diot, C. (2004). Diagnosing Network-Wide Traffic Anomalies. SIGCOMM '04: Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications, ACM.
18. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep Learning. Nature, 521(7553), 436-444.
19. Sakurada, M., & Yairi, T. (2014). Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction. International Joint Conference on Neural Networks (IJCNN).
20. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges. IEEE Internet of Things Journal, 3(5), 637-646.
21. Liao, S., Meng, F., Luo, X., & Zhang, G. (2021). Research on Intrusion Detection Algorithm Based on Software-Defined Network. International Conference on Security and Cryptography (SECRYPT).
22. Doshi, J., Mehta, V., & Kottari, S. (2020). Transfer Learning in Anomaly Detection. International Journal of Engineering Research & Technology, 9(12).
23. Pang, W., Lin, H., Li, J., & Wang, S. (2023). A Review on Privacy-Preserving Techniques for Network Traffic Analysis. IEEE Transactions on Network and Service Management.
24. Yu, M., Yi, Y., Rexford, J., & Chiang, M. (2019). Integrated SDN and Machine Learning for Network Management and Security. IEEE Journal on Selected Areas in Communications, 37(6), 1465-1481.
25. Boozary, Payam. "The Impact of Marketing Automation on Consumer Buying Behavior in the Digital Space Via Artificial Intelligence." Power System Technology 48.1 (2024): 1008-1021.
26. Ayyalasomayajula, Madan Mohan Tito, Sathish Kumar Chintala, and Sailaja Ayyalasomayajula. "A Cost-Effective Analysis of Machine Learning Workloads in Public Clouds: Is AutoML Always Worth Using?."
27. Ayyalasomayajula, Madan Mohan Tito, and Sailaja Ayyalasomayajula. "Proactive Scaling Strategies for Cost-Efficient Hyperparameter Optimization in Cloud-Based Machine Learning Models: A Comprehensive Review."

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)

Journal of Electronics, Computer Networking and Applied Mathematics
ISSN: 2799-1156
Vol: 04, No. 04, June-July 2024
http://journal.hmjournals.com/index.php/JECNAM
DOI: https://doi.org/10.55529/jecnam.44.32.44

28. Ayyalasomayajula, Madan Mohan Tito, Aniruddh Tiwari, Rajeev Kumar Arora, and Shahnawaz Khan. "Implementing Convolutional Neural Networks for Automated Disease Diagnosis in Telemedicine." In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 01-06. IEEE, 2024.
29. Chintala, Satishkumar. "Iot and Ai Synergy: Remote Patient Monitoring for Improved Healthcare." In 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), pp. 1-6. IEEE, 2024.
30. Chintala, Satishkumar. "Accelerating Drug Discovery: Ai Powered Approaches in Pharmaceutical Research." In 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), pp. 1-6. IEEE, 2024.

Copyright The Author(s) 2024.This is an Open Access Article distributed under the CC BY license. (http://creativecommons.org/licenses/by/4.0/)