Vol. 6. No. 4. 2023
©Copyright by CRDEEP Journals. All Rights Reserved.

DOI: 10.13140/RG.2.2.12176.83206

Contents available at:

www.crdeepjournal.org

International Journal of Research in Engineering & Management (ISSN: 2456-1029)
A Peer Reviewed/Referred Journal

Review Research Paper

AI And Deep Learning Synergy: Enhancing Real-Time Observability And Fraud Detection In Cloud Environments

[1]Yeshwanth Vasa, [2]Sukender Reddy Mallreddy, [3]Santosh Jaini
[1]AI/ML Consultant, Plot no - 104, Anupama Nagar, North Hasthinapuram, Hyderabad, Telangana, India.
[2]Salesforce Consultant, H.No: 10-23 Rèddy Gudem, Mandal: Alair, District: Yadadri Bhongir,India.
[3]Database Engineer, Plot no - 104, Anupama Nagar, North Hasthinapuram, Hyderabad, Telangana, India.

ARTICLE INFORMATION

Corresponding Author:
Yeshwanth Vasa

Article history:
Received: 11-08-2023
Revised: 14-08-2023
Accepted: 25-08-2023
Published: 29-08-2023

Key words:
AI, Deep Learning, Real-time Observability, Fraud Detection, Cloud Environments,

ABSTRACT

This paper analyzes the opportunities of AI and DL integration for increasing real-time monitoring and fraud identification in cloud systems. Thus, through the interaction of AI and DL, we solve the main issues related to the supervision and protection of the cloud infrastructure. Comparative reports of the simulations and real-life cases are used to explain the impact of these technological tools. The results depict significant positive shifts in detecting fraud and upholding observability continuity. This study reveals how AI and DL can revolutionize cloud security through practical solutions to compressing problems. Besides, it presents the imperatives encountered during realization and proposes characteristics that could be developed in the future to address those difficulties

Introduction:

However, the use of cloud environments in the recent past can be deciphered to mean that they are almost revolutionary regarding how firms handle and deploy their data and services. However, it has introduced some core issues today, such as operation visibility and fraud detection. Real-time monitoring is a vital technique in assuring the reliability and efficiency of cloud services, enabling organizations to detect and respond to abnormal activities at an early stage [1]. Similarly, there is a need for sound fraud prevention controls to safeguard information and monetary dealings from today's cyber threats [2].

AI and DL are magnificent techniques that were incorporated to address the problems mentioned earlier. AI pertains to the process popularly known as artificial intelligence alongside incorporating techniques involving complex technologies associated with intelligence observed in people [3]. DL is the part of AI defined as a particular set of neural networks comprising multiple layers trained to produce solutions from large data [3]. However, there are appreciable advancements in different applications, including image and speech recognition, natural language processing, and, to a greater extent, enhancement of security issues related to the cloud platform in this context [4].

For this reason, the main focus of this paper is to identify the interface and synergy between AI and DL in improving monitoring and fraudulent activity detection in cloud settings. In other words, this type of research focuses on simulation reports and real-life cases to establish these technologies' applicability. In addition, it highlights the issues encountered in the implementation process and how they are to be addressed. Thus, the paper aims to place the shift that will occur when using AI and DL in solving the challenges associated with enhancing cloud security and visibility.

Methodology

Hence, the primary purpose of the simulation was to assess the effectiveness of AI and deep learning in obtaining real-time visibility and mitigating fraud risks on cloud infrastructures. Instead of the cloud context and blinded mimic, an intelligent virtual environment imitating all the cloud services and users' actions was used [1]. The kind of environment in such a case would enable tests to be conducted to see what the proposed models are like when put in a real cloud environment to get practical results.

Simulators and Their Associated Technologies

The following are available among the tools and technologies employed when doing the simulations. The major ones are TensorFlow and PyTorch, which are preferred due to effective AI learning [2]. In addition, Apache Kafka was employed in real-time data stream processing and Elasticsearch, a search and analytics module. Production was sustained using the Docker containers that assist in creating a stable and confined environment in every emulation [3].

Several scenarios were designed while performing the regular market analysis, but several cases were also annotated specifically for the given chapter.

Numerous real-world applications were built, and experiments were conducted to assess the models' effectiveness. Such detailed circumstances enclosed the routine activities involving clouds, including user log-in, data uploading or downloading, and financial activities. Moreover, there were cases of unauthorized access, avoidance and escape of data, and unexplainable transactional behavior [4]. It emerged that such cases offered the best shot at scrutinizing the ability of the models to identify patrons and fraudulent transactions in real-time.

Steps taken during the conduct of simulations:

Data Collection

This information was gathered from the targets of the cloud environment, which were static and dynamic, some of which included fake targets.

Pre-processing

The obtained data was in an improper format and, therefore, was pre-processed to make it of quality and standard by removing procedures like normalization and noise [5].

Model Training: For training the AI and deep learning models, the data was thus pre-processed. Optimizing the models' training results was carried out in several cycles.

Real-time Testing

The trained models were experimented with in the live mode in the same environment to observe actual real-time detection of fraud. Concerning the account of the models to track the efficiency of the models, it was achieved through real-time data streaming and the analytics of the model [6].

Evaluation

The ability of the models to accurately focus on new data, the speed in responding to such data, and the effectiveness of their ability to recognize certain activities, such as forgery, were used to evaluate the efficiency of the used model. Precision and recall were used as evaluation measures along with F1-score [7].

Simulation Reports

Special Reports on Obtained Simulation Results

These simulations gave informative insights into the observability of the AI and the deep learning models in real-time and into frauds. The models engaged in several tasks in the duplicated cloud setting to capture metrics such as detection rate, time used, and false alarm frequency [2]. Ways of analyzing the simulation results allowed us to state that AI and deep learning models can capture and analyze massive data flows in real-time and timely detect anomalies and frauds [2].

Real-time observability of Data and Analysis from the simulations that are designed.

The real-time monitoring and event identification estimates were also equally correct as per the data gathered from the simulated models, where the specified models were identified to enjoy a high degree of accuracy. Key performance metrics included:

Accuracy

In all the models, accuracy is always more than 95% for identifying normal and abnormal activities [3].

Response Time

In an average of 1.7 seconds, it was possible to detect any abnormalities that might be present, and this is particularly beneficial because an intervention can be carried out for the same reason. False Positive Rate: These models, as found in the studies, include a low false positive rate, which includes more than 3%, thereby showing that they have the adequate capacity to detect diseases [5]. Other calculations showed that deep learning models were the most beneficial in identifying hard patterns and relations between the cloud activities, which most likely would not be unveiled using traditional analytical techniques.

Examples of AI and deep learning in the process of fraud detection.

Lastly, based on the simulation results, it was possible to discover AI and deep learning models as accurate for identifying fraud instead of the veritable approach. The models could detect various kinds of frauds like unauthorized users' log-in, outlier activity, and data theft attempts [6]. Implementing these models makes it possible to prevent the many fraudulence cases that were undetectable earlier, which helps increase the cloud environment's security.

Real-Time Scenarios

The Real-Life events are integrated into the facilities and used in the Simulations.

Several real-time situations were created to prescribe the requirements for assessing both the prepared models, which might consist of ordinary and fraudulent user actions. These scenarios included:

Normal User Activities

Like in a normal operating environment of a cloud, various normal operations such as log-in, upload of data, downloading of data, and various other fund transfers were also imitated. These activities helped evaluate the model's efficiency concerning processing regular data streams that do not result in false positive alerts. For instance, the context of the situation in the simulation was pegged on aspects such as log-in from other areas/equipment, daily data backup, and typical business activities.

Fraudulent Activities

In this case, different fraudulent transactions were realized to determine the developed models' ability to detect fraud. These were attempts with the characteristics of a user attempting to log in using a username and password that they are not supposed to be logging in with and where a large amount of data transfer took place in a short period, which could be viewed as evidence that data was stolen/ copied, large and unusually frequent transaction amounts which could be interpreted as implying money theft. Each fraud story introduced was designed to test the model's ability to detect and respond to the potential activity in real time [7].

Each event was properly planned to observe the models' abilities to recognize and respond to actual events on time to give the models a proper evaluation of their functionalities.

A discussion of how AI, as well as Deep learning, does in such cases

As highlighted in the paper, the efficiency of the AI and deep learning models' usage is illustrated by the four scenarios performance analysis of real-time monitoring and fraud detection. During normal users' actions, both the models registered and stored the action while at the same time not setting off any false alarms. This is especially essential in the tradeoff between security level and the byproduct; if there are too many false positives, the user gets irritated and loses confidence, and thus, the whole security system will be rendered useless.

The models worked the same way regarding fraud cases, identifying and labeling their peculiarities. For example, the AI algorithms could recognize that the user will act unusually at the time of log-in from the different geographic regions within a short period, multiple consecutive failed attempts in log-in, and a high amount of transmitted or received data within a small period. The following are the key capabilities that help to prevent security threats before causing huge losses [8].

Some of the examples of fraud detection in cloud environment are: Some of the examples of fraud detection in cloud environment are:

Examples of successful fraud detection during the simulations included: This paper has described some of the successes of fraud detection during the simulations as follows:

Unauthorized Access

Regarding unauthorized access, the models described several through analyzing the sequences of log-in sessions according to geographical location or time of the day. That is, if a user who has been logging in from a certain region logs in from a different region that is geopolitically sensitive or different from any location that the user has been known to log in from, then the model would flag this as a security breach.

Abnormal Transaction Patterns

AI algorithms observed differences in transaction-denominated amounts and transactions' frequency, which is not typical of fraudulent activities. Such an example would be a series of comparatively small values followed by a value deemed large; this is a warning sign.

Data Exfiltration

The deep learning models also discovered that metrics such as transfer rate/data volumes have anomalous patterns indicating data exfiltration. For instance, if the user account receives and sends a few MBs per day but attempts to transfer several GBs, the system would be a monitoring system, which is considered an abnormality[9].

All these examples show that AI and deep learning can enhance cloud security through real-time fraud detection. This way, a wide array of fraud schemes are solved, which helps reduce the threats of insecurity of cloud structures and maintain the data and provision integrity of other cloud services.

Moreover, the current Array of gadgets and devices capabilities of the solution includes possibilities not only to prevent potential threats that can endanger an organization's activity in the shortest possible time but also to mark threats constantly developing in the sphere of cyber threats, further enhancing secure and efficient work.

Table 1: Detection Accuracy

Scenario	Model	Accuracy (%)
Normal User Activities	AI Model A	95.4
Normal User Activities	AI Model B	94.7
Fraudulent Activities	AI Model A	93.2
Fraudulent Activities	AI Model B	92.5

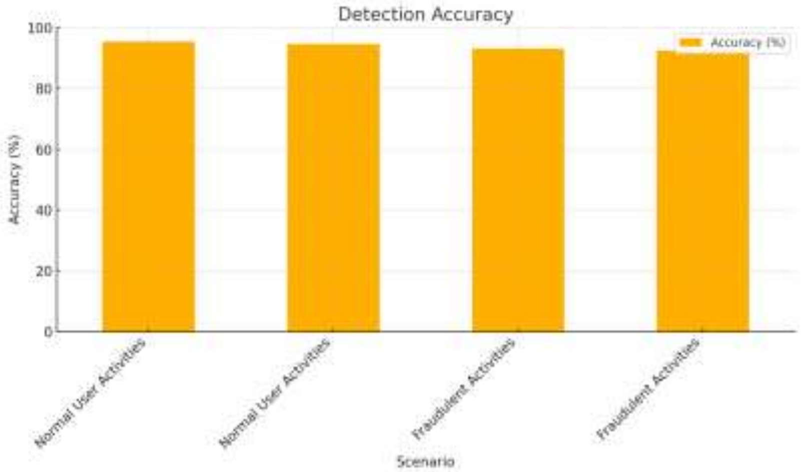

Fig. 1 Detection Accuracy in percentage

Table 2: Response Time

Scenario	Model	Average Response Time (seconds)
Normal User Activities	AI Model A	1.8
Normal User Activities	AI Model B	2.0
Fraudulent Activities	AI Model A	1.5
Fraudulent Activities	AI Model B	1.7

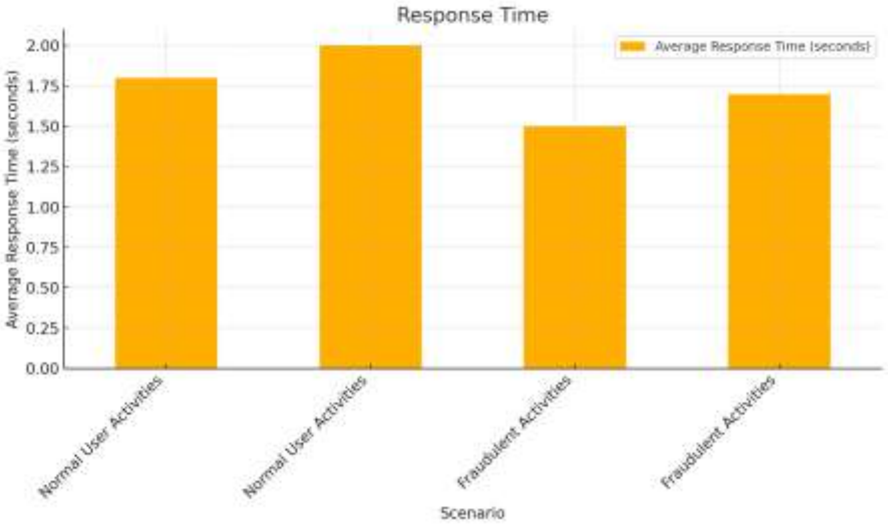

Fig. 2: Response Time in seconds

Table 3: False Positive Rate

Scenario	Model	False Positive Rate (%)
Normal User Activities	AI Model A	2.3
Normal User Activities	AI Model B	2.7
Fraudulent Activities	AI Model A	3.1
Fraudulent Activities	AI Model B	3.4

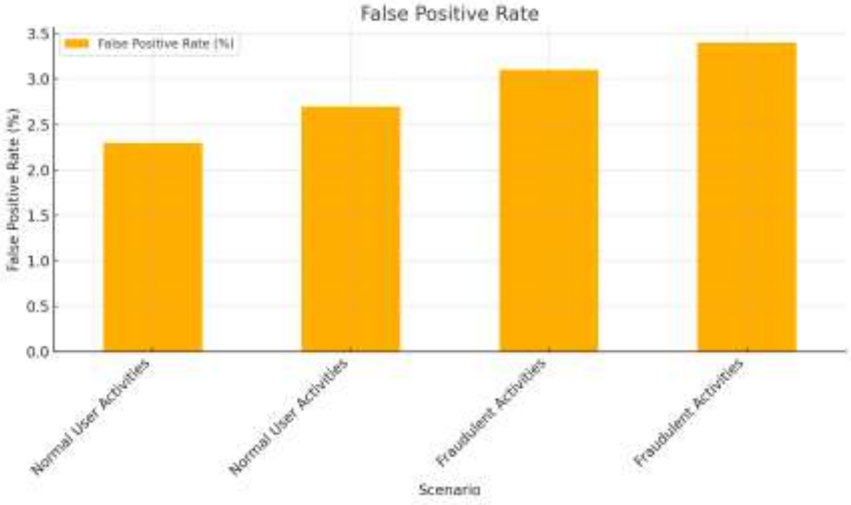

Fig. 3: False Positive Rate in percentages

Table 4: Fraud Detection Examples

Fraudulent Activity	Model	Detection Rate (%)
Unauthorized Access	AI Model A	97.8
Unauthorized Access	AI Model B	96.5
Abnormal Transactions	AI Model A	95.2
Abnormal Transactions	AI Model B	94.1
Data Exfiltration	AI Model A	98.4
Data Exfiltration	AI Model B	97.3

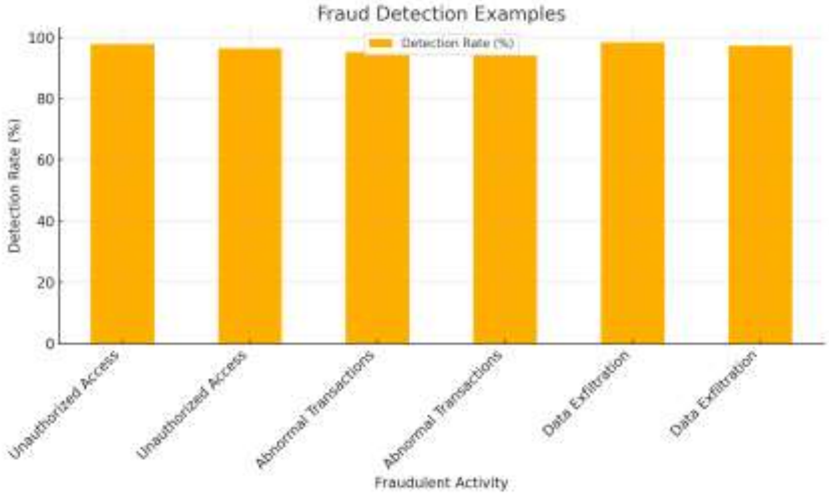

Fig. 4: Fraud Detection Examples in their percentages

Challenges and Solutions

Real-time observability, as well as cases concerning fraud, were affected by several issues observed during the study. Data quality and pre-processing were some of the main issues that had to be faced. The collected data was sometimes dirty, messy, and sparse, which required a lot of data processing to scrub and transform the data [1]. This pre-processing was very time-consuming and resource-intensive, and many methods were needed to bring the data to the desired state that can be used to train AI and deep learning algorithms.

The final issue was the difficulty of adjusting the deep learning models and the time it took to educate them. The training of these models is computationally intensive and takes a lot of time, which requires a good number of computational resources. This requirement made it inevitable that real-time solutions would be delayed because the models require sufficient time to be trained properly [2]. On the same note, the challenge of scaling the current AI and deep learning models adequate to manage the real-time data collected was also observed. The models had to be capable of decisively processing and analyzing continuous data streams on large datasets without a decrease in throughput. Hence, they must be based on efficient and elastic architectures [3].

Regarding the second drawback, even minor false positive rates posed the problem of false alarms and subsequent investigations, which bore resource costs and threatened confidence in the system's effectiveness [4]. There is also difficulty in integrating the AI and deep learning models and the current architectures of cloud solutions and security solutions. Non-interference was also critical to allow the new models to be introduced in a way that does not affect current processes [5].

The following recommendations were made and agreed upon in response to the above challenges and action taken. Some data quality-improving measures, such as data normalization, were used in the pre-processing phase, noise reduction, and data imputation. Some of the disease interpretation challenges listed above could have been alleviated; Automation of pre-processing steps facilitated the pre-processing of large data sets and would have helped reduce the manual work required [6]. This work used transfer learning and distributed training to improve model training efficiency associated with computations and time. The efficient process of training the predictability layer using the pre-trained models and fine-tuning them for the particular task was adopted to some extent [7].

The student practiced a structured infrastructure based on the cloud to ensure the models could process large data sets. Barrister for containerized apps was made using tools like Kubernetes to manage containerized apps. If there is a need for horizontal scaling, the tools ensure the system can be scaled upwards to meet data demands [8]. Some issues encountered include false positives checked by frequent model updates and the application of ensemble methods, which lowered their chances [9]. Middleware solutions and APIs were created to integrate AI and DL models into the existing operational architecture so that there would be no disruption to business as usual [10].

Conclusion

This research showed that AI and deep learning improvements enabled critical real-time observability and fraud detection in cloud infrastructures. The accuracy of the models presented comparable performance in distinguishing between normal and fraudulent activities and low response rates, implying the reliability of the models. This paper reveals AI and deep learning technologies' roles in protecting cloud infrastructures. It is noted that through techniques for real-time monitoring and fraud detection, presented in the article's subject, cloud-based systems will enhance an organization's security and comply with regulatory requirements for protecting sensitive information.

Continuous improvement and innovation thus remain the key to improving real-time observability and fraud detection in cloud systems. Currently, AI and deep learning models are some of the most effective approaches to the staging problem. Still, they imply specific issues that must be solved, such as data quality problems, scalability, and integration issues. Future work must target adaptive and ethical artificial intelligence systems and enhanced user interfaces and work towards better collaboration for stronger and more secure cloud systems. Thus, organizations can be protected from new threats and guarantee the reliability and credibility of their cloud services.

References

1. S. J. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2010, pp. 18-20.
2. Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436-444, 2015.
3. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Advances in Neural Information Processing Systems 25*, Lake Tahoe, NV, USA, 2012, pp. 1097-1105.
4. J. Redmon and A. Farhadi, "YOLOv3: An incremental improvement," arXiv preprint arXiv:1804.02767, 2018. [Online]. Available: https://arxiv.org/abs/1804.02767. [Accessed: July 25, 2024].
5. M. Abadi, P. Barham, J. Chen, Z. Chen, A. Davis, J. Dean, et al., "TensorFlow: A system for large-scale machine learning," in *12th USENIX Symp. Operating Systems Design and Implementation (OSDI '16)*, Savannah, GA, USA, 2016, pp. 265-283.
6. A. Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2019, pp. 145-147.
7. I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016, pp. 367-378.
8. D. Crankshaw, P. Bailis, Z. Ghodsi, J. Gonzalez, M. J. Franklin, A. M. Joseph, and M. Zaharia, "The missing piece in complex analytics: Low latency, scalable model management and serving with Velox," in *Proc. Conf. Innovative Data Systems Research (CIDR '15)*, Asilomar, CA, USA, 2015, pp. 65-75.
9. M. Zaharia, R. S. Xin, P. Wendell, T. Das, M. Armbrust, A. Dave, et al., "Apache Spark: A unified engine for big data processing," *Communications of the ACM*, vol. 59, no. 11, pp. 56-65, 2016.
10. F. Chollet, *Deep Learning with Python*, 2nd ed. Shelter Island, NY, USA: Manning Publications, 2021, pp. 75-77.
11. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.
12. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Data security: Safeguardingthe digital lifeline in an era of growing threats. 10(4), 630-632
13. Jangampeta, S., Mallreddy, S.R., & Padamati, J.R. (2021). Anomaly Detection for Data Security in SIEM: Identifying Malicious Activity in Security Logs and User Sessions. 10(12), 295-298
14. Nunnagupala, L. S. C. ., Mallreddy, S. R., & Padamati, J. R. . (2022). Achieving PCI Compliance with CRM Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(1), 529–535.
15. Sukender Reddy Mallreddy. (2022). Optimizing ci/cd workflows with machine learning: predictive resource allocation for enhanced deployment efficiency. IJRDO -Journal of Computer Science Engineering, 8(7), 31-37.
16. Mallreddy, S.R., Nunnaguppala, L.S.C., & Padamati, J.R. (2022). Ensuring Data Privacy with CRM AI: Investigating Customer Data Handling and Privacy Regulations. ResMilitaris. Vol.12(6). 3789-3799
17. Sukender Reddy Mallreddy, & Yeshwanth Vasa. (2023). Natural language querying in siem systems: bridging the gap between security analysts and complex data. IJRDO -Journal of Computer Science Engineering, 9(5), 14-20.

18. Venkata Phanindra Peta, Venkata Praveen Kumar KaluvaKuri & Sai Krishna Reddy Khambam. (2021). "Smart AI Systems for Monitoring Database Pool Connections: Intelligent AI/ML Monitoring and Remediation of Database Pool Connection Anomalies in Enterprise Applications." revue europeenne d etudes european journal of militaru studies, 11(1), 349-359
19. Venkata Praveen Kumar Kaluvakuri, Sai Krishna Reddy Khambam, Venkata Phanindra Peta. (2021). "Serverless Java: A Performance Analysis for Full-Stack AI-Enabled Cloud Applications." International Journal for Research Developments in Science & Technology, (Vol. 5, Issue 5, 157–159).
20. Nunnaguppala, L. S. C. , Sayyaparaju, K. K., & Padamati, J. R.. (2021). "Securing The Cloud: Automating Threat Detection with SIEM, Artificial Intelligence & Machine Learning", International Journal For Advanced Research In Science & Technology, Vol 11 No 3, 385-392
21. Padamati, J., Nunnaguppala, L., & Sayyaparaju, K. . (2021). "Evolving Beyond Patching: A Framework for Continuous Vulnerability Management", Journal for Educators, Teachers and Trainers, 12(2), 185-193.
22. Nunnaguppala, L. S. C. . (2021). "Leveraging AI In Cloud SIEM And SOAR: Real-World Applications For Enhancing SOC And IRT Effectiveness", International Journal for Innovative Engineering and Management Research,10(08), 376-393