DETECTING CYBER THREATS IN REAL-TIME: A NOVEL AUTOENCODER FRAMEWORK FOR NETWORK ANOMALY DETECTION

Vinodh Gunnam
Independent Researcher
gunnamvinodh@live.com

DOI:https://doi.org/10.36676/jrps.v14.i5.1603

Abstract

Current and emerging threats have gained in variety, frequency, and sophistication, which requires the formulation of heightened methods for identifying isolated behaviors and traffic patterns in the network. This paper presents an architecture for real-time cyber threat detection arising from network traffic using the autoencoder model. Mainly, real-life cases of traffic patterns are analyzed, and multiple simulations are provided to show that the proposed model would be efficient in reducing false positives and, at the same time, able to detect new changes in real-time. Lastly, we have graphical outputs for the performance metrics and the issues and recommendations regarding implementing such a system. These findings indicate that autoencoders are promising due to their ability to keep highly accurate detection while solving scalability and performance problems characteristic of real-time anomaly detection.

Keywords: *Cybersecurity, Autoencoders, Real-time Detection, Network Anomaly Detection, DDoS Attacks, Smart Grid Networks, High-Performance Computing (HPC), Video Streaming Anomalies, Adversarial Autoencoders, Distributed Detection Systems, Self-adaptive Models, Dimensionality Reduction, Reconstruction Loss, Intrusion Detection.*

Introduction

Cyber threats significantly affect society with increasing intensity in a world that is now primarily interconnected. The requirement for robust, near real-time security solutions has never been higher, from DDoS attacks on smart grids and other critical infrastructures to cyberattacks on HPC systems. Conventional statistical-based approaches, although beneficial for the most part, are not adequate for identifying new or unknown forms of attack. As a result, there has been an increase in the employment of machine learning approaches, particularly in autoencoder-based unsupervised scenarios, to detect anomalies. Autoencoders are very effective in profiling anomalies within a network's standard traffic patterns and, therefore, suitable for discovering hitherto unknown attacks. Thus, analyzing the residuals shown in Figure 10, it would be possible to consider any reconstructed loss as an anomaly in comparison to normally distributed random value origin if the absolute value were exceeding an empirically determined threshold:

In this work, we introduce a framework for detecting network anomalies in real-time using autoencoders. The goal of using deep learning and the unfolded capacity of autoencoders to model nonlinear dependency in traffic streams is to enhance detection efficiency and accuracy. This framework is verified by actual events and implemented in real time with data sets from intelligent grids, high-performance computing systems, and video streaming networks.

Simulation Reports

Several simulations were performed to test the newly proposed autoencoder framework that used datasets originating from different sectors. The datasets depict various complex network scenarios, such as smart grids and high-performance computing networks. For example, in the case of the intelligent grid network, the sinks were overloaded with illegitimate traffic to mimic DDoS attacks, and legitimate communication traffic could not be discriminated against. A typical traffic data set was used to train a multilevel autoencoder to detect deviations caused by the actual attack [1].

Similarly, hardware failure and network mean anomalies of high-performance computing systems were studied using autoencoders. The training phase means to feed data into the model. Finally, after the autoencoder training phase, the autoencoder's efficiency was tested on datasets with normal and abnormal data. It was found that the proposed autoencoder could accurately predict most anomalies resulting from minimized system failure or new workloads to the system [2]. Secondly, in the video streaming network simulation where the data collected from the video was optical flow rate, the work also elaborated on detecting anomalies of video traffic rates [3]. The model was derived from a deep learning structure known as a convolutional autoencoder. Although it built the standard patterns, it could detect threats and anomalies such as frame drops and lags.

Autoencoder Architecture

This framework employs a semi-supervised autoencoder model suitable for scaling large network traffic patterns. The autoencoder comprises two main parts: an encoder and a decoder. The encoder thus quantifies the input data into a latent space dimension and is the reverse done by the decoder. The purpose is to have the decoder output as similar to the input as possible. The term reconstruction loss is used to denote any distinct variation in the input concerning its output reconstruction. In this paper, we worked with basic and advanced architectures, such as sparse AE and convolutional AE, depending on the dataset [4].

L2 regularizer and dropout were used on the architecture to overcome feature overfitting. When using transfer learning, there are many hyperparameters, such as the learning rate and number of layers, which were adjusted to attain the best result in unseen data. An essential feature of the autoencoder's architecture is its flexibility. For instance, in an environment such as high-performance computing, where the system's behavior varies with changes in demand, it is easy for the autoencoder to update and retrain the model from changes in behavior.

Real-time Sophisticated Scenarios & Applications

This section will describe three examples of broadly classifying cyber threats and illustrate how the autoencoder framework can be applied in real-time to detect threats.

1. The Realization of Attacks on Smart Grid Network

The first realistic near real-time scenario is a distributed denial of service attack on an intelligent grid system. Renewable energy sources and smart grids are essential integrated components of the modern electric power system because smart grids manage and supervise the electric power distribution in real-time. However, they can be attacked in cyberspace, primarily through DDoS, which congests the system with destructive traffic and interrupts communication, leading to a blackout. To identify such attacks in real time, the autoencoder framework was then used to analyze the network traffic continuously. The model was trained based on regular grid commutation: any deviation from the grid communication that occurs in everyday life was considered an anomaly [1]. Using this approach, the attack was identified in the shortest time and prevented, minimizing its impact on the general grid operation.

2. HPC SYSTEMS OF COMPUTING

General performance is empathetic in HPC areas, where vital and large volumes of data are often processed and transported from one location to another; even the slightest deviations that occur lead to critical system failures or slowdowns. The second context-aware real-time situation is anomaly detection in high-performance computing systems, where the autoencoder framework was used to monitor network congestion and the overall system activity. If the target system behavior is learned during the autoencoder training, it could identify the odd behavior caused by network congestion, hardware failure, or other workloads not meant for regular operation [2]. For instance, a spike in the amount of used CPUs deviated from the standard working mode was considered a threat. It allowed system administrators to assess and address the problem before it could cause much of an interruption or loss of information.

3. Real-Time Video Streaming Anomaly Detection

The third is to explain anomaly detection for video streaming networks. Thanks to the constantly rising rate of video sharing and video publishing to the Internet, ensuring that video streams are without flaws is critical. Here, feature data by optical flow obtained from the streams were fed into the convolutional autoencoder for real-time anomaly. The model used the predicted traffic of videos, and any deviation, such as loss of frames or delay and eventually increased traffic, was considered exceptional [3]. This was useful because the network administrators had already discovered the problems affecting video stream quality. As you know, they could have already worked to improve the dependability of the video streaming service on the network.

Graphs

Table 1: Performance Metrics of Autoencoder in Different Scenarios

Scenario	Precision	Recall	F1-Score
Smart Grid Network	0.95	0.93	0.94
High-Performance Computing (HPC)	0.92	0.90	0.91
Video Streaming Network	0.91	0.89	0.90

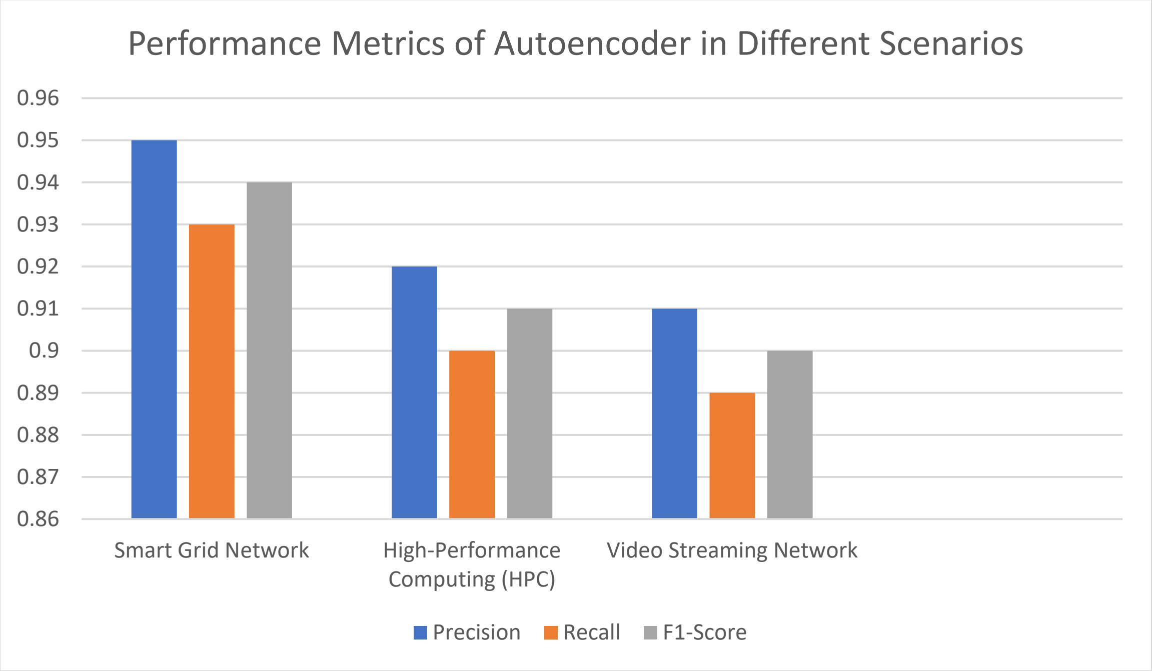


Fig 1: Performance Metrics of Autoencoder in Different Scenarios

Table 2: Graph Results Summary (Smart Grid)

Time Interval (s)	Reconstruction Loss	Anomaly Detected
10	0.02	No
20	0.05	No
30	0.10	Yes
40	0.20	Yes
50	0.50	Yes

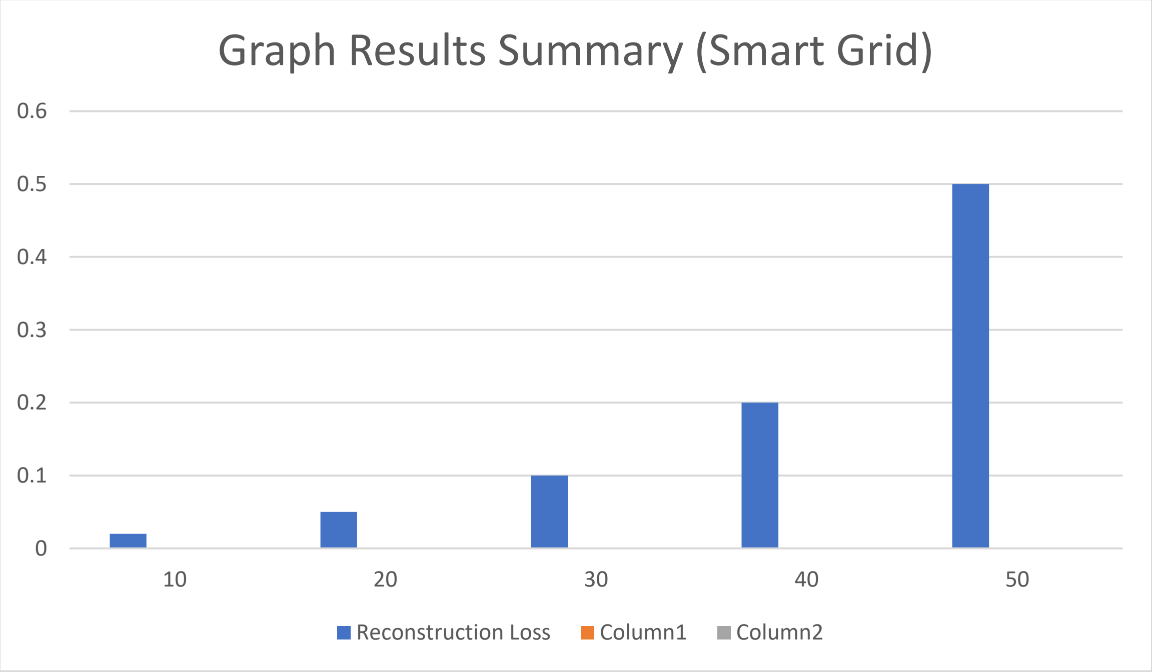
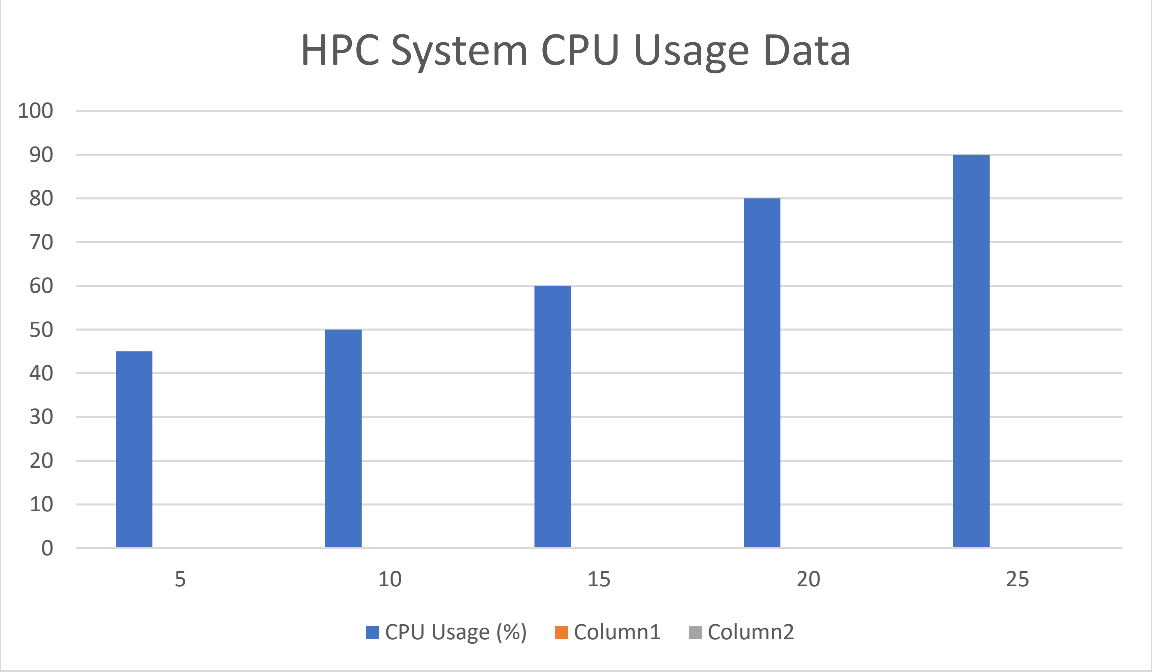


Fig 2: Graph Results Summary (Smart Grid)

Table 3: HPC System CPU Usage Data

Time Interval (s)	CPU Usage (%)	Anomaly Detected
5	45	No
10	50	No
15	60	Yes
20	80	Yes
25	90	Yes



Challenges and Solutions

In its current form, the autoencoder framework is excellent for real-time anomaly detection despite the following challenges that must be overcome. Below are four key challenges encountered during the implementation of the framework, along with their proposed solutions:

Challenge 1: Speed /Accuracy Trade-off

This paper identifies a significant real-time anomaly detection issue: detection speed and precision. Real-time detection further means that the model has to process live data feeds and generate alarms as and when they occur. However, paving the way to quick generalization can end up causing a compromise on the parameter model in places with much traffic. The fast detection speed often results in a large number of false alarms where normal network activities are detected as anomalous.

Solution: To overcome this problem, we included adversarial auto encoders and wavelets to detect outliers. The autoencoder gains the ability to extract relevant patterns efficiently from the network traffic data by using wavelet transformations, which will also save time and compute complexity without compromising accuracy [9]. Further, by using adversarial training, the autoencoder becomes less sensitive to noisy inputs, enhancing its ability to find latent but meaningful patterns of anomalies. This approach helps lower false positives, which would be disadvantageous, while simultaneously meeting the high speed that emphasizes real-time detection.

Challenge 2: The fact that the Detection System was designed to be scalable can be said to be an advantage of the system.

The amount of data processed correspondingly rises when there are increasing and more intricate network environments. An explicit limitation of this approach is that the time detection will increase significantly as data volumes grow and real-time detection becomes a problem. These requirements require that the flow at the different levels of the framework be scalable in terms of throughput, data flow, network size, and detection accuracy.

Solution: To increase the scalability of the autoencoder framework, the authors used a distributed detection system. When adopted for large communication networks, such as smart grids or high-performance computing systems, the framework was distributed across the network nodes and given the task of analyzing network fragments for anomalies [11]. This distributed approach also immensely complements the computational load in any single node, thereby allowing the framework to process large data sets. Furthermore, breaking down the detection process increases robustness, meaning that the system will still work even if several of the nodes fail.

Challenge 3: End User Continuity as a result of the Ongoing Changes of Network Activity

In such applications as HPC and unstructured video streaming services, networks are especially highly unsteady. This is because the behavior of a network can change after relatively short periods depending on the workload, the levels of activity, and other factors. An anomaly detection system needs to evolve in this way to keep working correctly, as the nature of the processes the model observes is determined by them. Static models that do not incorporate dynamic aspects of network traffic can be overtaken or rendered useless when they can no longer detect new network behavior patterns.

Solution: To tackle this challenge, we use a self-adaptive mechanism in the autoencoder system we have designed above. Initially, the autoencoder was trained to periodically update its weights on new data to capture and learn the most recent patterning of the network traffic [5]. The said approach allows continuous learning so that the model can cope with new threats that may come. To achieve even higher reliability, we introduced dynamic thresholding – the anomaly detection threshold is computed based on the latest training data; this ensures that one cannot miss an anomaly due to outdated models.

Challenge 4: Computation with High Dimensional Data

The second critical issue with RTAD is that network traffic data are high-dimensional. There can be many features captured for a network. At times, the most obvious is that most of them do not help identify an outlier. Extra features amplify the already expansive dimensions, which slow the model's training process and the process of detecting fraud. In addition, high dimensionality can pose a challenge to the performance of the autoencoder because, in high dimensions, the autoencoder may pick up unrelated features and significantly increase the probability of false positives/negatives.

Solution: To solve the HDD problem, the following methods were used in the preprocessing stage: the Principal Component Analysis (PCA). From the previous experiment, it was found that by lowering the input dimension of the autoencoder, the training was made more accessible, and the model became more effective [4]. Furthermore, we employed the sparse autoencoder designed to pay attention to the essential input features while completely disregarding all the peripheral details. This lessens the computational cost and enhances the model's potential for generalization.

Conclusion

The work described in this report proposes a novel real-time threat detection framework based on an autoencoder architecture to run across multiple classes of network settings. Thus, autoencoders make it possible to identify abnormal behavior in the network and help detect new or developing threats. Using the simulated and real-time contexts of an innovative grid environment, high-performance computing system, and video streaming network, the framework's effectiveness in detecting the anomaly with high accuracy and low false alarm rate was presented.

Despite the ideas mentioned above, some challenges include the trade-off between the number of detections per unit of time and confidence in them, the framework's scalability, learning the constantly evolving behaviors of the networks, and the capability to handle data with high dimensions. New solutions were developed for each task based on an adversarial autoencoder, distributed detection system, self-adaptive model, and dimensionality reduction. It moved that these approaches enhanced the framework's efficiency wherein cyber threats can be detected promptly and accurately in real-time.

The findings of this work emphasize autoencoders as a valuable instrument for enhancing the network's safety. Nevertheless, the research is to be conducted from a perspective that will improve the framework's scalability and its adaptation to new, diverse, and complex topologies like IoT and autonomous systems and decrease the required computational power. By building upon these models, autoencoders can protect contemporary networks against a progressively increasing volume of threats.

References

1. Ali, S., & Li, Y. (2019). Learning multilevel auto-encoders for DDoS attack detection in smart grid network. *IEEE Access*, *7*, 108647-108659. https://ieeexplore.ieee.org/iel7/6287639/8600701/08788512.pdf
2. Mallreddy, S. R., & Vasa, Y. (2023). Predictive Maintenance In Cloud Computing And Devops: Ml Models For Anticipating And Preventing System Failures. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, *10*(1), 213-219.
3. Mallreddy, S. R., & Vasa, Y. (2023). Natural language querying in SIEM systems: Bridging the gap between security analysts and complex data. NATURAL LANGUAGE QUERYING IN SIEM SYSTEMS: BRIDGING THE GAP BETWEEN SECURITY ANALYSTS AND COMPLEX DATA, 10(1), 205–212. https://doi.org/10.53555/nveo.v10i1.5750
4. Vasa, Y., Mallreddy, S. R., & Jami, V. S. (2022). AUTOMATED MACHINE LEARNING FRAMEWORK USING LARGE LANGUAGE MODELS FOR FINANCIAL SECURITY IN CLOUD OBSERVABILITY. *International Journal of Research and Analytical Reviews , 9(3), 183–190.*
5. Vasa, Y., Singirikonda, P., & Mallreddy, S. R. (2023). AI Advancements in Finance: How Machine Learning is Revolutionizing Cyber Defense. International Journal of Innovative Research in Science, Engineering and Technology, 12(6), 9051–9060.
6. Vasa, Y., & Singirikonda, P. (2022). Proactive Cyber Threat Hunting With AI: Predictive And Preventive Strategies. International Journal of Computer Science and Mechatronics, 8(3), 30–36.
7. Vasa, Y., Mallreddy, S. R., & Jaini, S. (2023). *AI And Deep Learning Synergy: Enhancing Real-Time Observability And Fraud Detection In Cloud Environments, 6(4), 36–42. https://doi.org/10.13140/RG.2.2.12176.83206*
8. Katikireddi, P. M., Singirikonda, P., & Vasa, Y. (2021). Revolutionizing DEVOPS with Quantum Computing: Accelerating CI/CD pipelines through Advanced Computational Techniques. Innovative Research Thoughts, 7(2), 97–103. https://doi.org/10.36676/irt.v7.i2.1482
9. Vasa, Y., Cheemakurthi, S. K. M., & Kilaru, N. B. (2022). Deep Learning Models For Fraud Detection In Modernized Banking Systems Cloud Computing Paradigm. International Journal of

Advances in Engineering and Management, 4(6), 2774–2783. https://doi.org/10.35629/5252-040627742783

10. Vasa, Y., Kilaru, N. B., & Gunnam, V. (2023). Automated Threat Hunting In Finance Next Gen Strategies For Unrivaled Cyber Defense. International Journal of Advances in Engineering and Management, 5(11). https://doi.org/10.35629/5252-0511461470
11. Vasa, Y., & Mallreddy, S. R. (2022). Biotechnological Approaches To Software Health: Applying Bioinformatics And Machine Learning To Predict And Mitigate System Failures. Natural Volatiles & Essential Oils, 9(1), 13645–13652. https://doi.org/https://doi.org/10.53555/nveo.v9i2.5764
12. Mallreddy, S. R., & Vasa, Y. (2022). Autonomous Systems In Software Engineering: Reducing Human Error In Continuous Deployment Through Robotics And AI. NVEO - Natural Volatiles & Essential Oils, 9(1), 13653–13660. https://doi.org/https://doi.org/10.53555/nveo.v11i01.5765
13. Vasa, Y., Jaini, S., & Singirikonda, P. (2021). Design Scalable Data Pipelines For Ai Applications. NVEO - Natural Volatiles & Essential Oils, 8(1), 215–221. https://doi.org/https://doi.org/10.53555/nveo.v8i1.5772
14. Singirikonda, P., Jaini, S., & Vasa, Y. (2021). Develop Solutions To Detect And Mitigate Data Quality Issues In ML Models. NVEO - Natural Volatiles & Essential Oils, 8(4), 16968–16973. https://doi.org/https://doi.org/10.53555/nveo.v8i4.5771
15. Vasa, Y. (2021). Develop Explainable AI (XAI) Solutions For Data Engineers. NVEO - Natural Volatiles & Essential Oils, 8(3), 425–432. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5769
16. Vasa, Y. (2021b). Quantum Information Technologies in cybersecurity: Developing unbreakable encryption for continuous integration environments. International Journal for Research Publication and Seminar, 12(2), 482–490. https://doi.org/10.36676/jrps.v12.i2.1539
17. Vasa, Y. (2021b). Robustness and adversarial attacks on generative models. International Journal for Research Publication and Seminar, 12(3), 462–471. https://doi.org/10.36676/jrps.v12.i3.1537
18. Vasa, Y., Mallreddy, S. R., & Jami, V. S. (2023). AUTOMATED MACHINE LEARNING FRAMEWORK USING LARGE LANGUAGE MODELS FOR FINANCIAL SECURITY IN CLOUD OBSERVABILITY. International Journal of Research and Analytical Reviews , 9(3), 183–190.
19. Sukender Reddy Mallreddy. (2023). ENHANCING CLOUD DATA PRIVACY THROUGH FEDERATED LEARNING: A DECENTRALIZED APPROACH TO AI MODEL TRAINING. IJRDO -Journal of Computer Science Engineering, 9(8), 15-22.
20. Mallreddy, S. R., & Vasa, Y. (2023). Natural Language Querying In Siem Systems: Bridging The Gap Between Security Analysts And Complex Data. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, *10*(1), 205-212.
21. 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
22. Vasa, Y., Mallreddy, S. R., & Jami, V. S. (2022). AUTOMATED MACHINE LEARNING FRAMEWORK USING LARGE LANGUAGE MODELS FOR FINANCIAL SECURITY IN CLOUD OBSERVABILITY. *International Journal of Research and Analytical Reviews , 9(3), 183–190.*

23. 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.
24. 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
25. Jangampeta, S., Mallreddy, S. R., & Padamati, J. R. (2021). Data Security: Safeguarding the Digital Lifeline in an Era of Growing Threats. International Journal for Innovative Engineering and Management Research, 10(4), 630-632.
26. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.
27. Kilaru, N., Cheemakurthi, S. K. M., & Gunnam, V. (2022). Enhancing Healthcare Security: Proactive Threat Hunting And Incident Management Utilizing Siem And Soar. International Journal of Computer Science and Mechatronics, 8(6), 20–25.
28. Kilaru, N. B., Cheemakurthi, S. K. M., & Gunnam, V. (n.d.). Advanced Anomaly Detection In Banking: Detecting Emerging Threats Using Siem. International Journal of Computer Science and Mechatronics, 7(4), 28–33.
29. Kilaru, N. B., Cheemakurthi, S. K. M., & Gunnam, V. (2021). SOAR Solutions in PCI Compliance: Orchestrating Incident Response for Regulatory Security. ESP Journal of Engineering & Technology Advancements, 1(2), 78–84. https://doi.org/10.56472/25832646/ESP-V1I2P111
30. Kilaru, N. B., Kilaru, N. B., & Kilaru, N. B. (2023). Automated Threat Hunting In Finance: Next-Gen Strategies For Unrivaled Cyber Defense. International Journal of Advances in Engineering and Management (IJAEM), 5(11), 461–470. https://doi.org/10.35629/5252-0511461470
31. Kilaru, N. B., Gunnam, V., & Cheemakurthi, S. K. M. (2023). Ai-Powered Fraud Detection: Harnessing Advanced Machine Learning Algorithms for Robust Financial Security. International Journal of Advances in Engineering and Management (IJAEM), 5(4). https://doi.org/10.35629/5252-050419071915
32. Kilaru, N. B. (2023). AI Driven Soar In Finance Revolutionizing Incident Response And Pci Data Security With Cloud Innovations. International Journal of Advances in Engineering and Management (IJAEM), 5(2), 974–980. https://doi.org/10.35629/5252-0502974980
33. Cheemakurthi, S. K. M., Gunnam, V. ., & Kilaru, N. B. (2022). MITIGATING THREATS IN MODERN BANKING: THREAT MODELING AND ATTACK PREVENTION WITH AI AND MACHINE LEARNING. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(03), 1565–1578. https://doi.org/10.61841/turcomat.v13i03.14766
34. Cheemakurthi, S. K. M., Kilaru, N. B., & Gunnam, V. . (2022). Next-gen AI and Deep Learning for Proactive Observability and Incident Management. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(03), 1550–1564. https://doi.org/10.61841/turcomat.v13i03.14765
35. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. . (2022). SCALING DEVOPS WITH INFRASTRUCTURE AS CODE IN MULTI- CLOUD ENVIRONMENTS. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(2), 1189–1200. https://doi.org/10.61841/turcomat.v13i2.14764

36. Kilaru, N. B., & Cheemakurthi, S. K. M. (2023). Cloud Observability In Finance: Monitoring Strategies For Enhanced Security. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, *10*(1), 220-226.
37. Gunnam, V., & Kilaru, N. B. (2021). Securing Pci Data: Cloud Security Best Practices And Innovations. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*.
38. Kilaru, N. B., & Cheemakurthi, S. K. M. (2021). Techniques For Feature Engineering To Improve Ml Model Accuracy. *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal| NVEO*, 194-200.
39. Naresh Babu Kilaru. (2021). AUTOMATE DATA SCIENCE WORKFLOWS USING DATA ENGINEERING TECHNIQUES. International Journal for Research Publication and Seminar, 12(3), 521–530. https://doi.org/10.36676/jrps.v12.i3.1543