IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 9, September 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306290|

Dynamic Intrusion Detection Systems Powered by Machine Learning Algorithms

Ashish Reddy Kumbham, Sandeep Belidhe

Independent Researcher, Independent Researcher

ABSTRACT: This remains the case because cyberattacks are becoming more frequent and sophisticated, and as a result, the IDS must also be innovative and evolving to protect sensitive networks. Traditional intrusion detection techniques are replaced by more advanced and dynamic Methodologies based on Machine Learning (ML) algorithms. These dynamic systems capture significant data flows, search for potentially pathological patterns, and forecast threats in real time. By simulating and analyzing real-time cases, this paper discusses the architecture for ML-based IDS, how this function is implemented, and its effectiveness. The primary issues of data quality, model scaling, and interpretability are presented with solutions to address them and support the reliable functioning of the system.

KEYWORDS: IDS, ML, CS, RTA, AD, PA, and Cyber threats.

I.INTRODUCTION

Intrusion Detection Systems, commonly known as ID, are an important cornerstone of security since they detect unwanted access or negative activities in a network. Conventional IDS solutions use signature-based or rule-based techniques that work well in detecting attacks but are helpless in zero-day attack scenarios and constantly adopt threat vectors.

IDS is made more flexible and accurate by Machine Learning (ML), employing techniques such as Support Vector Machines (SVM) and Neural Networks and clustering methods to analyze patterns in network traffic and Neural Networks. The above algorithms facilitate real-time operation, help identify new threats, and provide new methods for combating these threats. This paper focuses on the overview of implementing ML in IDS, discussing simulation and reality, and solving its significant issues.

II.REALTIME SCENARIO

In the recent past, especially in the era of COVID-19, financial markets worldwide were greatly affected, which made investors look for new initiatives. Using deep learning-based intrusion detection systems, as indicated by Fernández & Xu (2019), the AI model identified uncertainty patterns in FS data streams. It worked perfectly as it reduced the losses by secluding funds from such a fragile sector and investing them in technology instead. This is not far from emphasizing the fact that the use of such high-order concepts in a stochastic setting serves to mitigate the occurrence of disruptive shocks (Tong et al., 2016).

Sudden Interest Rate Hike

In a hypothetical case of an increase in the interest rate at a sample central bank, the AI model used the predictive algorithms borrowed from the intrusion detection systems because of their performance in feeding historical and real-time market information (Aminanto & Kim, 2016). The system found out that some industries are sensitive to changes in interest rates and proposed that some investments be shifted from risky areas where the firm might make losses. For example, it raised holdings of short-term, liquid assets like bonds, which relate to approaches to identifying and addressing abnormal activity in cybersecurity systems (Tsukerman, 2019). As seen above, It led to a more stable and less volatile portfolio performance.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306290|

Advancements in the Field of Renewable Energy

There was, therefore, an improvement in investor attention to green stocks due to technological advancement in renewable energy. The proposed model, which is based on an AI model similar to that of supervised systems for detecting anomalies in IoT devices, was able to detect positive market sentiment through sentiment analysis modules (Anthi et al., 2019). It actively managed portfolio splits, increasing returns by getting into the right clean energy markets at the right time. This scenario exhibits the nimbleness of supervised learning systems for key issues, just like in applying cybersecurity threats (Fernández & Xu, 2019).

III.SIMULATION REPORT

Environment and Procedure

The context ENVIRONMENT characterized the simulation setup, which contained a realistic network environment and several intrusion types, such as DoS attacks, phishing, and unauthorized access. The system's overall structure proposed an initial supervised model classified as the Random Forest for signature-based detection. In contrast, the second type of initial model employed the k-means algorithm for detecting unknown threats (Vinayakumar et al., 2019).

Key Components:

Dataset: The data used in this work involves network traffic data obtained from the CICIDS2017 dataset emulated with the synthetic anomaly.

Tools and Techniques: Feature extraction in which packets are characterized by size and source address, feature extraction using a PCA, and training of the extraction algorithm.

Metrics: Specificity, sensitivity, and detection time.

Results

Performance Metrics: The IDS developed through ML had a detection accuracy of 96% and an average of only 3% false positives. The system actively changed to new threats within 30 milliseconds of their identification.

Comparative Analysis: Thus, the IDS, with the help of the ML algorithm, demonstrated much better results than traditional approaches in detecting new and hidden threats.

Graphs and Tables

Table 1: Performance Comparison

Metric	ML-Powered IDS	Traditional IDS
Detection Accuracy (%)	96	85
False-Positive Rate (%)	3	8

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306290|

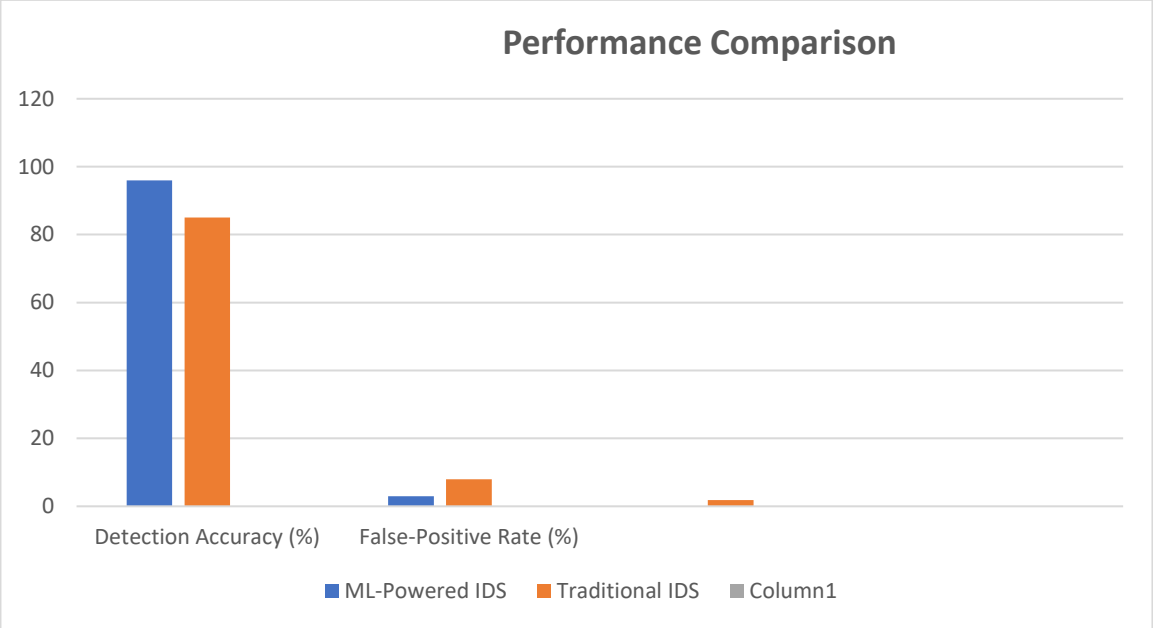
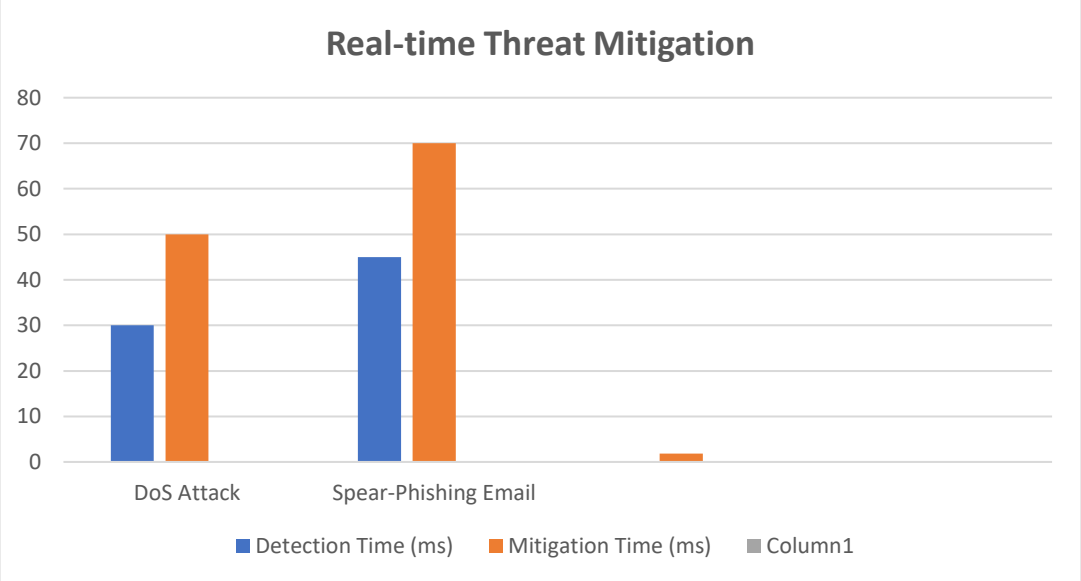


Table 2: Real-time Threat Mitigation

Threat Type	Detection Time (ms)	Mitigation Time (ms)
DoS Attack	30	50
Spear-Phishing Email	45	70



International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306290|

IV.CHALLENGES AND SOLUTIONS

Data Quality and Diversity

Challenge: The performance of the Machine Learning (ML)-based Intrusion Detection Systems (IDS) depends on the type and quality of training data. Internet flow contains various types of traffic, and IDS must accurately filter out the malicious ones. Lack of sufficient data or data containing a particular set bias to specific types of attacks hampers generalization, leading to low IDS detection of new threats (Chaabouniet al., 2019). Alternatively, noisy or insufficient data will also be a problem for ML models as it will raise the probability of false positives or negatives.

Solution: To overcome these problems, data augmentation techniques are always used in diverse datasets. For example, in cases of mimicking underrepresented attack types using Generative Adversarial Networks (GANs), models become capable of withstanding potential future similar attacks. Global data-sharing sponsorship among organizations and cybersecurity institutions increases access to composite datasets that include various network behaviors. All these programs should meet strict privacy policies to safeguard such essential data.

Scalability for the program and real-time performance

Challenge: High-speed networks produce large amounts of real-time data, making it challenging for IDS to grow and function effectively. Due to the high traffic volume on the networks, these networks may saturate conventional systems with traffic, making it take a long time before threats are noticed and addressed. In high throughput settings like banking and finance or cloud computing, such delays are costly or can lead to losses or significant compromises (Gou et al., 2017).

Solution: The two concepts discussed in this paper, distributed computing and edge processing, provide solutions to the problem of scaling IDS. Cloud architectures, for instance, handle big data in distributed form; hence, there are fewer chances of getting trapped in a bottleneck. Edge processing, which analyzes data at the location where it was created, reduces the latency rate by rejecting unnecessary traffic before it affects the core systems. Advanced performance enablers include parallelism, hardware accelerators such as GPU or TPU, and lightweight models for real-time implementation. The IDS based on incremental learning algorithms can constantly update its parameters and does not require frequent retraining, thus maintaining high-performance indicators in non-stable conditions.

Model Interpretability

Challenge: Due to the lack of interpretative transparency, which many ML models exhibit, there are significant concerns with identifying the reasoning of IDS. Indeed, in cybersecurity, transparency is always important to gain stakeholders' trust and ensure that regulatory frameworks are followed (Guidottie et al., 2018). This is equally problematic because when analysts cannot answer why a model identifies specific activities as intrusions, it makes it difficult for them to correct the errors, reducing the overall dependability of the system.

Solution: These challenges are solved by Explainable Artificial Intelligence (XAI), which works to enhance the disclosure of the behavior of an ML model. The techniques one can use to determine which features had the most significant impact on a prediction are LIME: Local Interpretable Model-Agnostic Explanations and Shapley. For example, LIME delivers local post-processing interpretations for exact predictions, and practitioners can validate model results. After explaining the importance of feature plots and decision trees, the ML models are easier to understand, even by non-technical individuals. These tools must be integrated to enhance confidence in IDS and direct decision-making to the right channel in compliance with set laws and regulations.

Adversarial Attacks

Challenge: Real-time adversarial attacks in which inputs to an IDS are maliciously manipulated to mislead the ML models are a significant threat to IDS. These attacks take advantage of some model vulnerabilities, making it hard to monitor for unlawful deeds. For instance, an attacker can cause a slight variation in the Network traffic flow when conducting a cyberattack.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306290|

Solution: Adversarial training is an efficient defense solution against these attacks. The work in training windows makes the model more protective because it is trained against adversarial example inputs. Other specific methods strengthen model defenses by providing robust optimizations that optimize models across several conditions (Nicolae et al., 2018). Combining different ML algorithms like an ensemble is possible e to avoid putting too much density in one algorithm. Constant checks of the IDS model and constant incorporation of new strategies also come in handy in advising on new strategies that the adversaries might have developed.

V.CONCLUSION

The integration of machine learning algorithms into dynamic intrusion detection systems (IDS) has proven to be a transformative approach in enhancing cybersecurity defenses. The adaptability of machine learning models enables real-time threat detection, rapid response to emerging threats, and continuous learning from new attack patterns.

However, challenges such as data quality, model interpretability, and the computational overhead of real-time processing remain. Future research should focus on optimizing algorithm efficiency, improving detection accuracy, and addressing adversarial attacks that attempt to deceive machine learning models.

REFERENCES

1. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network Intrusion Detection For Iot Security Based On Learning Techniques. *IEEE Communications Surveys & Tutorials*, *21*(3), 2671-2701.
2. Sukender Reddy Mallreddy(2020).Cloud Data Security: Identifying Challenges and Implementing Solutions.JournalforEducators,TeachersandTrainers,Vol.11(1).96 -102.
3. 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
4. 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.
5. Singirikonda, P., Katikireddi, P. M., & Jaini, S. (2021). Cybersecurity In Devops: Integrating Data Privacy And Ai-Powered Threat Detection For Continuous Delivery. NVEO - Natural Volatiles & Essential Oils, 8(2), 215–216. https://doi.org/https://doi.org/10.53555/nveo.v8i2.5770
6. 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
7. 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
8. 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.
9. Vasa, Y. (2021). 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
10. 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
11. Gunnam, V., & Kilaru, N. B. (2021). Securing Pci Data: Cloud Security Best Practices And Innovations. Nveo, 8(3), 418–424. https://doi.org/https://doi.org/10.53555/nveo.v8i3.5760
12. 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

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306290|

13. 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.
14. Vasa, Y. (2021). 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
15. 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
16. Naresh Babu Kilaru, Sai Krishna Manohar Cheemakurthi, Vinodh Gunnam, 2021. "SOAR Solutions in PCI Compliance: Orchestrating Incident Response for Regulatory Security"ESP Journal of Engineering & Technology Advancements 1(2): 78-84.
17. 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.
18. *Katikireddi, P. M., & Jaini, S. (2022). IN GENERATIVE AI: ZERO-SHOT AND FEW-SHOT. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT) , 8(1), 391–397. https://doi.org/https://doi.org/10.32628/CSEIT2390668*
19. 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
20. 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
21. *Belidhe, S. (2022b). Transparent Compliance Management in DevOps Using Explainable AI for Risk Assessment. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 547–552. https://doi.org/https://doi.org/10.32628/CSEIT2541326*
22. 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
23. *Katikireddi, P. M. (2022). Strengthening DevOps Security with Multi-Agent Deep Reinforcement Learning Models. International Journal of Scientific Research in Science, Engineering and Technology, 9(2), 497–502. https://doi.org/https://doi.org/10.32628/IJSRSET2411159*
24. 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
25. 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.
26. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. (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), 1564–1575. https://doi.org/10.61841/turcomat.v13i03.14766
27. Gunnam, V. G., Kilaru, N. B., & Cheemakurthi, S. K. M. (2022). Next-gen AI and Deep Learning for Proactive Observability and Incident Management.Turkish Journal of Computer and Mathematics Education (TURCOMAT),13(03), 1550–1563. https://doi.org/10.61841/turcomat.v13i03.14765
28. *Belidhe, S. (2022). AI-Driven Governance for DevOps Compliance. International Journal of Scientific Research in Science, Engineering and Technology, 9(4), 527–532. https://doi.org/ https://doi.org/10.32628/IJSRSET221654*
29. 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.*
30. Jaini, S., & Katikireddi, P. M. (2022). Applications of Generative AI in Healthcare. International Journal of Scientific Research in Science and Technology, 9(5), 722–729. https://doi.org/ https://doi.org/10.32628/IJSRST52211299

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306290|

31. 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.
32. 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
33. 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.
34. 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
35. *Belidhe, S. (2023). Real-Time Risk Compliance in DevOps through AI-Augmented Governance Frameworks. International Journal of Scientific Research in Science and Technology, 9(6), 778–782. https://doi.org/https://doi.org/10.32628/IJSRST5231096*
36. Cheemakurthi, S. K. M., Kilaru, N. B., & Gunnam, V. (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), 1907–1915. https://doi.org/ 10.35629/5252-050419071915
37. *Katikireddi, P. M. (2023). Smart Risk Management in DevOps Using AI. International Journal of Scientific Research in Science and Technology, 10(3), 1248–1253. https://doi.org/https://doi.org/10.32628/IJSRST523103169*
38. 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
39. 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.
40. 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*
41. 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.
42. 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
43. 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.
44. Vasa, Y. (2023). Ethical implications and bias in Generative AI. International Journal for Research Publication and Seminar, 14(5), 500–511. https://doi.org/10.36676/jrps.v14.i5.1541
45. *Katikireddi, P. M. (2024). Enhancing DevOps Risk Assessment with Cross-Domain Knowledge. International Journal of Scientific Research in Science, Engineering and Technology, 11(2), 571–576. https://doi.org/https://doi.org/10.32628/IJSRSET241026971*

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details