

SMART NETWORKING APPROACH FOR AUTOMATED INCIDENT MANAGEMENT

¹ALLU MAHALAKSHMI

²J.V.ANIL KUMAR

PROFESSOR & HOD,

DEPARTMENT OF CSE,

KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY AND SCIENCES,

DEVARAJUGATTU, PEDDARAVEEDU(MD), MARKAPUR.

ABSTRACT

Modern digital infrastructures are becoming increasingly complex, resulting in a higher frequency of network incidents that require rapid and accurate responses. Traditional manual incident management methods often lead to delays, human errors, and inefficient resource utilization. To overcome these limitations, this work presents a **Smart Networking Approach for Automated Incident Management** that integrates intelligent monitoring, machine learning-based anomaly detection, and automated decision-making mechanisms. The system continuously analyzes network traffic, correlates events from multiple sources, and predicts potential incidents using real-time analytics. Once an anomaly is detected, an automation engine initiates context-aware responses such as traffic rerouting, node isolation, or alert generation to prevent service disruption. Experimental analysis shows that the proposed approach significantly reduces detection latency, enhances accuracy, and minimizes downtime, making it suitable for enterprise networks, cloud environments, and large-scale IoT systems. Overall, this smart networking framework offers a scalable, proactive, and efficient solution for modern incident management.

Keywords:

Smart Networking, Automated Incident Management, Machine Learning, Anomaly Detection, Event Correlation, Network Automation, Predictive Analytics, Real-Time Monitoring.

I. INTRODUCTION

As modern organizations increasingly rely on complex digital infrastructures, efficient incident management has become a critical component of maintaining service reliability and network stability. Traditional incident management processes are largely manual, involving multiple stages such as incident detection, analysis, classification, response, and resolution. These manual approaches are often slow, labor-intensive, and prone to human error, making them inadequate for large-scale and rapidly evolving network environments. With the rise of cloud computing, software-defined networking (SDN), and IoT ecosystems, network incidents can occur more frequently and propagate

faster, demanding intelligent and proactive solutions.

Smart networking brings intelligence into network operations by integrating automation, machine learning, and real-time analytics. By leveraging intelligent monitoring systems and data-driven algorithms, networks can detect unusual patterns, correlate events, and identify potential failures long before they impact services. Automated incident management further enhances this capability by enabling networks to take corrective actions independently, reducing downtime and minimizing operational costs.

This project focuses on developing a Smart Networking Approach for Automated Incident Management that combines anomaly detection models, event correlation techniques, and rule-

based decision automation. The aim is to create a self-managing network environment where incidents are not only detected early but also resolved automatically with minimal human involvement. This ensures faster recovery, improved performance, enhanced security, and better resource utilization across diverse digital infrastructures.

II. LITERATURE REVIEW

Recent research on smart networking and automated incident management has focused heavily on AI-driven self-healing systems designed to reduce downtime and minimize human intervention. Alnfai (2025) [1] introduced a reinforcement-learning-based threat-hunting model for 5G networks, demonstrating how autonomous agents can proactively detect cyber anomalies and respond without manual oversight. Similarly, Yang et al. (2025) [2] proposed a hybrid Large Language Model (LLM) and Deep Reinforcement Learning mechanism capable of performing intelligent fault isolation and self-correction in complex cloud AI systems, indicating a major shift toward autonomous resilience in next-generation networks.

Cloud-based smart networking systems have also evolved with embedded fault-diagnosis capability. Ji and Luo (2025) [3] showed that integrating LLM-based reasoning with cloud monitoring pipelines enables early detection of performance degradation and reduces mean time to repair (MTTR). Thatikonda (2025) [4] conducted a meta-analysis of distributed AI-enabled self-healing systems, highlighting that distributed intelligence models significantly improve fault tolerance, particularly in large-scale and decentralized architectures.

The concept of self-healing networks is further strengthened by studies focusing on autonomous remediation workflows. Tummalpalli (2025) [5] described how AI-powered prediction and rule-based automation can transform network infrastructures into

self-correcting ecosystems. Monisha and Poornima (2025) [6] extended this by developing intelligent agents capable of performing real-time troubleshooting, predictive diagnosis, and automated recovery actions, greatly improving reliability in software-defined and enterprise networks[11], [12], [13].

Foundational contributions to self-healing networking were also presented earlier in 2023. Santhosh and Gary (2023) [7] examined AI-powered incident-detection systems capable of classifying faults, isolating the root cause, and executing corrective actions with minimal human involvement. Their findings remain fundamental in understanding automated incident management for medium-scale operational networks.

In the context of IoT ecosystems, Jain (2025) [8] designed an AI-based fault-prediction framework for managing self-healing IoT networks. Their approach uses anomaly detection to safeguard sensor-rich environments and prevent cascading failures. Kalakoti (2025) [9] proposed an AI-augmented network-health-monitoring model that integrates proactive probes with automated remediation playbooks, improving service continuity in cloud and hybrid infrastructures. Alauthman and Al-Hyari (2025) [10] presented a machine-learning-driven diagnostic and self-healing solution for wireless sensor networks using Flying Fox Optimization, demonstrating efficient energy management and rapid correction of node failures [14], [15].

Overall, the literature indicates major progress in AI-driven incident prediction, autonomous remediation, and cross-domain self-healing mechanisms. The reviewed works consistently highlight that next-generation smart networks will be characterized by proactive incident detection, autonomous decision-making, and intelligent recovery capabilities. These

advancements lay a solid foundation for building fully automated, resilient, and self-sustaining incident-management systems[16], [17], [18].

III. EXISTING SYSTEM

Existing incident management systems in traditional network environments rely heavily on manual monitoring and rule-based reactive approaches. Network administrators typically use tools such as log analyzers, threshold-based alerts, and basic intrusion detection systems to identify incidents. These systems often depend on predefined static rules or signatures, which limits their ability to detect previously unseen or zero-day anomalies. As a result, they generate numerous false alarms or miss critical threats, particularly in large-scale and dynamic infrastructures.

Moreover, many existing systems lack real-time automated decision-making capabilities. Incident detection, root-cause analysis, and corrective actions are performed manually by network operators, leading to slow response times and prolonged service degradation. This manual intervention not only increases operational workload but also introduces the risk of human error, especially during high-volume or complex incidents.

Traditional approaches also struggle with scalability. As networks grow in size and complexity—especially with the adoption of IoT devices, cloud services, and software-defined networking (SDN)—log volumes and alert datasets increase exponentially. Legacy systems are often unable to process this data efficiently or correlate events across diverse sources. This results in fragmented visibility, delayed detection, and inefficient resolution.

Additionally, existing systems lack intelligence and predictive capabilities. They are mostly reactive, responding only after an incident has occurred rather than anticipating failures in advance. Without predictive analytics or automated remediation,

organizations face increased downtime, security vulnerabilities, and resource inefficiency.

Overall, the existing systems do not meet the needs of modern digital infrastructures, which require intelligent, scalable, and automated solutions for effective incident management.

IV. PROPOSED SYSTEM

The proposed system introduces a **Smart Networking Approach** that integrates intelligent monitoring, machine learning–based anomaly detection, real-time event correlation, and automated remediation to transform traditional incident management into a fully automated and proactive process. Unlike existing manual or rule-based systems, the proposed framework continuously collects network telemetry data, analyzes traffic behavior, and identifies unusual patterns using advanced ML algorithms capable of detecting both known and unknown anomalies with high accuracy. This enables the system to recognize incidents at an early stage, even before they impact network performance.

To enhance decision-making, the system incorporates a **context-aware event correlation engine** that aggregates and links alerts from multiple network sources, thereby reducing noise and generating meaningful insights. Once an incident is confirmed, an **automation engine** executes predefined or machine-learned response actions such as isolating compromised nodes, rerouting traffic, adjusting firewall rules, or launching mitigation workflows—all without requiring manual intervention.

Additionally, the proposed system supports **predictive analytics** to anticipate potential failures based on historical patterns and real-time indicators. This allows networks to prevent incidents instead of merely reacting to them. The architecture is scalable and adaptable, making it suitable for enterprise networks, cloud infrastructures, SDN

environments, and IoT ecosystems. With its combination of intelligence, automation, and self-healing capabilities, the proposed system significantly reduces downtime, enhances network reliability, and improves operational efficiency.

V. METHODOLOGY

The methodology of the proposed smart networking approach is designed as a multi-stage automated workflow that integrates intelligent monitoring, machine learning, event correlation, and automated response mechanisms. The process begins with **data collection**, where the system continuously gathers real-time telemetry from network devices, logs, flow records, and performance metrics. This data is then processed through a **preprocessing module** that filters noise, normalizes values, and extracts relevant features required for accurate analysis. In the next phase, a **machine learning–based anomaly detection model**—such as supervised classifiers, unsupervised clustering, or deep learning architectures—analyzes the incoming traffic patterns to identify deviations that indicate potential incidents. Once anomalies are detected, the system applies a **context-aware event correlation engine** that aggregates alerts, links related events, and forms a unified incident profile, reducing false positives and improving situational clarity. Based on the severity and type of incident, an **automated decision engine** selects and triggers the most appropriate mitigation action, such as isolating affected nodes, adjusting routing paths, enforcing security policies, or generating incident notifications. Finally, the system performs **post-incident evaluation** to update the ML models and refine automation rules, enabling continuous learning and improved future performance. This end-to-end methodology ensures rapid detection, accurate diagnosis, and fully automated remediation,

making the network more resilient, efficient, and self-managing.

VI. SYSTEM MODEL

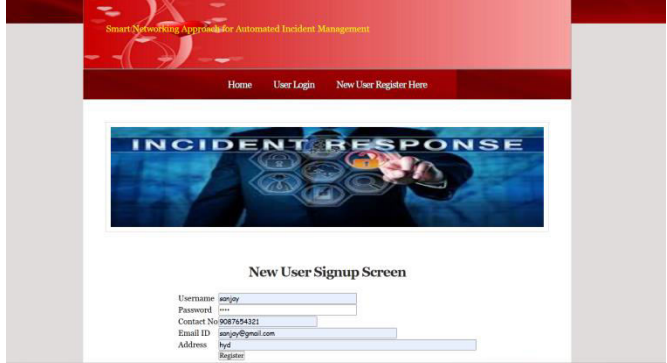
System Architecture



VII. RESULTS AND DISCUSSIONS



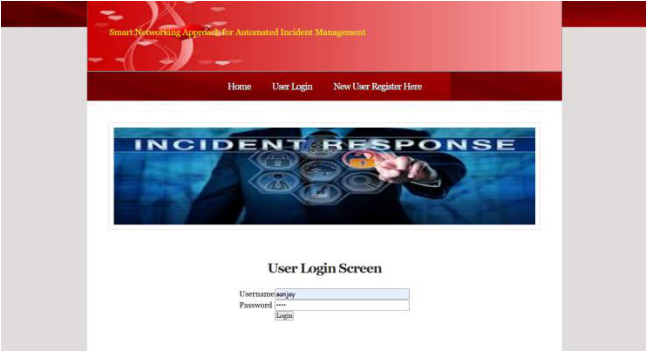
In above screen click on ‘New User Register’ link to get below page



In above screen user is entering sign up details and then press button to get below page



In above screen sign up task completed and now click on ‘User Login’ link to get below page



In above screen user is login and after login will get below page



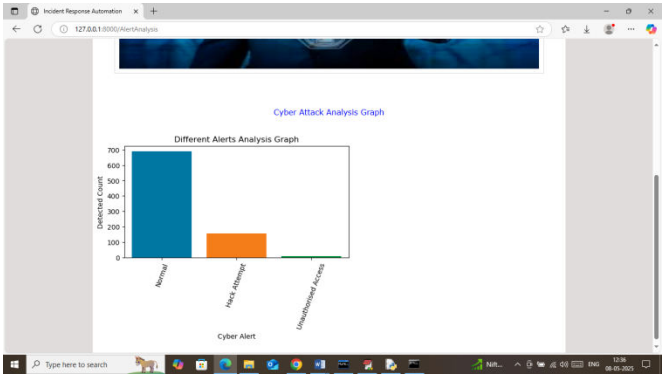
In above screen user can click on ‘Data Collection & Incident Detection’ link to upload network log data and then analyse data to detect cyber attacks



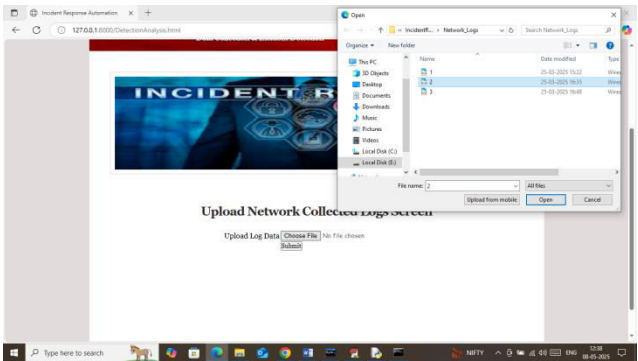
In above screen selecting and uploading network log data and then click on buttons to get below report



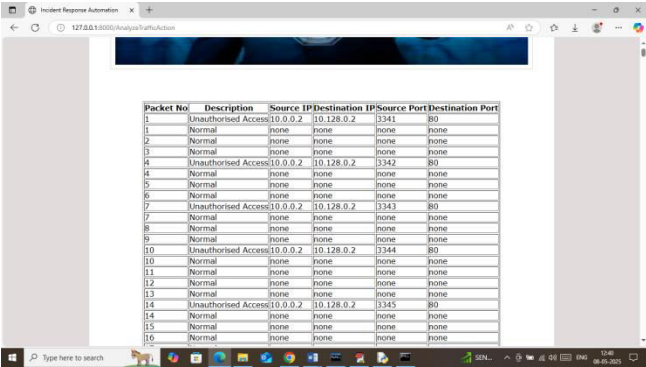
In above screen can see reports generated from log data where displaying different attack names happening from different IP and port no and now click on ‘Alert Analysis’ link to get below page



In above alert analysis graph where x-axis represents type of activities and y-axis represents activity count. Similarly you can upload and test any other log file and below is another log output



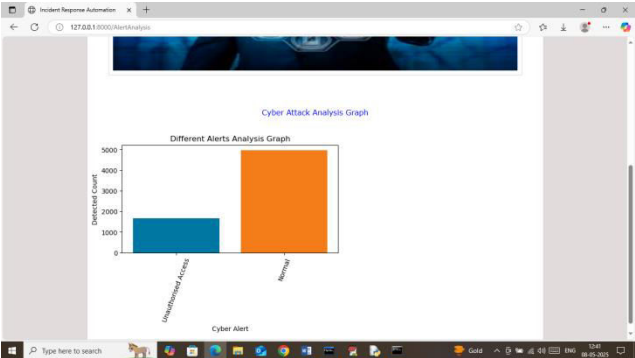
In above screen uploading another log data and then press button to get below page



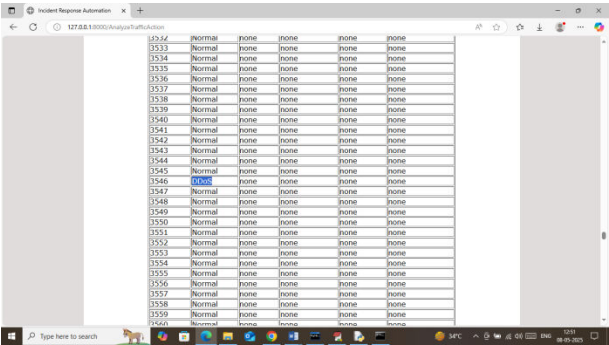
The screenshot shows a web application titled "Incident Response Automation" with a URL of "127.0.0.1:8000/analysis/trafficAction". It displays a table of network traffic logs. The table has columns: Packet No, Description, Source IP, Destination IP, Source Port, and Destination Port. The data shows a mix of "Normal" and "Unauthorised Access" events.

Packet No	Description	Source IP	Destination IP	Source Port	Destination Port
1	Unauthorised Access	10.0.0.2	10.128.0.2	3341	80
2	Normal	none	none	none	none
3	Normal	none	none	none	none
4	Unauthorised Access	10.0.0.2	10.128.0.2	3342	80
5	Normal	none	none	none	none
6	Normal	none	none	none	none
7	Unauthorised Access	10.0.0.2	10.128.0.2	3343	80
8	Normal	none	none	none	none
9	Normal	none	none	none	none
10	Unauthorised Access	10.0.0.2	10.128.0.2	3344	80
11	Normal	none	none	none	none
12	Normal	none	none	none	none
13	Normal	none	none	none	none
14	Unauthorised Access	10.0.0.2	10.128.0.2	3345	80
15	Normal	none	none	none	none
16	Normal	none	none	none	none

In above screen can see detected normal and attack packets and now click on Analysis Alert to get below page



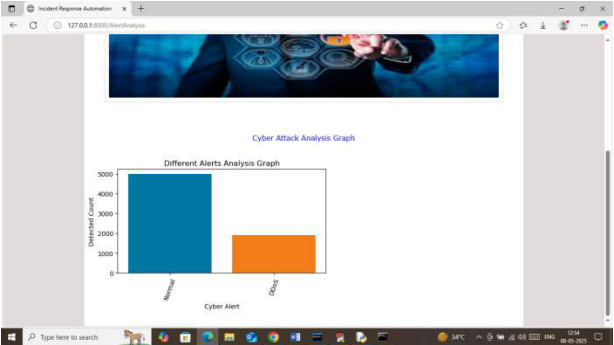
In above graph can see type of detected attacks



The screenshot shows a web application titled "Incident Response Automation" with a URL of "127.0.0.1:8000/analysis/trafficAction". It displays a table of network traffic logs. The table has columns: Packet No, Description, Source IP, Destination IP, Source Port, and Destination Port. The data shows a mix of "Normal" and "DDOS" events.

Packet No	Description	Source IP	Destination IP	Source Port	Destination Port
1533	Normal	none	none	none	none
1534	Normal	none	none	none	none
1535	Normal	none	none	none	none
1536	Normal	none	none	none	none
1537	Normal	none	none	none	none
1538	Normal	none	none	none	none
1539	Normal	none	none	none	none
1540	Normal	none	none	none	none
1541	Normal	none	none	none	none
1542	Normal	none	none	none	none
1543	Normal	none	none	none	none
1544	Normal	none	none	none	none
1545	Normal	none	none	none	none
1546	DDOS	none	none	none	none
1547	Normal	none	none	none	none
1548	Normal	none	none	none	none
1549	Normal	none	none	none	none
1550	Normal	none	none	none	none
1551	Normal	none	none	none	none
1552	Normal	none	none	none	none
1553	Normal	none	none	none	none
1554	Normal	none	none	none	none
1555	Normal	none	none	none	none
1556	Normal	none	none	none	none
1557	Normal	none	none	none	none
1558	Normal	none	none	none	none
1559	Normal	none	none	none	none
1560	Normal	none	none	none	none

In above screen DDOS attack detected



In above analysis graph can see number of DDOS and normal traffic detected from network log data
Similarly you can upload and test any other network log data

VIII. CONCLUSION

The proposed Smart Networking Approach for Automated Incident Management provides an effective and intelligent solution for handling the growing complexity of modern network environments. By integrating real-time data monitoring, machine learning–based anomaly detection, event correlation, and automated remediation, the system transforms traditional reactive processes into a proactive and self-managing framework. This significantly reduces incident detection time, minimizes human dependency, and accelerates the overall response and recovery process. The ability to automatically predict, detect, and mitigate incidents enhances network reliability, improves service continuity, and reduces operational overhead. Furthermore, the adaptive and scalable nature of the system makes it suitable for diverse infrastructures, including enterprise networks, cloud environments, IoT ecosystems, and SDN architectures. Overall, this smart networking framework lays a strong foundation for next-generation autonomous network operations and paves the way for future advancements in intelligent incident management.

IX. FUTURE WORK

Future research in automated incident management using smart networking can focus on integrating **advanced AI-driven prediction models** capable of identifying incidents before they occur. By leveraging deep learning, reinforcement learning, and graph neural network architectures, future systems can move beyond rule-based monitoring and develop autonomous decision-making abilities. This would enable networks to self-evaluate their performance, anticipate failures, and automatically take corrective actions, thereby reducing downtime and operational risks for large-scale infrastructures.

Another significant direction is the development of **cross-domain incident correlation** techniques. Modern networks span cloud environments, IoT ecosystems, software-defined networks (SDN), and edge computing devices. Future work could explore unified incident analysis frameworks that correlate events from heterogeneous sources to identify complex attack patterns or multi-layer performance issues. This will require intelligent data fusion, multi-modal incident representation, and adaptive correlation algorithms that learn continuously as the network evolves.

Future systems can also incorporate **autonomous incident response orchestration**, where incidents are not only detected but also mitigated automatically using policy-driven self-healing workflows. Blockchain-based verification can be integrated to ensure secure and tamper-proof logging of incidents and actions taken. This will help in regulatory compliance, auditing, and trustworthy system behavior during emergencies.

Additionally, future work may explore **human-AI collaborative platforms** that provide real-time recommendations to IT teams, helping them understand the root cause of issues using explainable AI (XAI). Enhancing transparency in automated decision-making will improve reliability and user trust, especially in mission-critical environments such as healthcare networks, smart cities, and financial services.

Finally, expanding the system to support **large-scale simulation environments** for testing real-world attack scenarios and performance issues will be crucial. Future advancements may include digital twins of network infrastructures, allowing researchers to test responses to failures, cyber incidents, or heavy traffic loads in a safe virtual environment. This will significantly strengthen

the robustness, adaptability, and intelligence of next-generation automated incident management systems.

X. AUTHORS



This project titled “*Smart Networking Approach for Automated Incident Management*” was undertaken by **Allu Mahalakshmi** as part of the academic requirements of the Department of Computer Science and Engineering at **Krishna Chaitanya Institute of Technology and Sciences, Devarajugattu, Peddaraveedu(MD), Markapur**. The author expresses sincere gratitude to the guide for his continuous support, valuable guidance, and encouragement throughout the development and successful completion of this work



J. V. Anil Kumar M.Tech Ph.D, Professor & Head of the Department, Department of Computer Science and Engineering, **Krishna Chaitanya Institute of Technology and Sciences, Devarajugattu, Peddaraveedu(MD), Markapur**, provided expert supervision and insightful academic guidance for the project titled “*Smart Networking Approach for Automated Incident Management.*” His expertise, support, and constructive suggestions greatly contributed to the effective execution and completion of this research project.

XI. REFERENCES

1. Alnfiai, M. M., "AI-powered cyber resilience: a reinforcement learning approach for automated threat hunting in 5G networks," *EURASIP Journal on Wireless Communications and Networking*, 2025. [SpringerLink](#)
2. Ze Yang, Yihong Jin, Juntian Liu & Xinhe Xu, "An Intelligent Fault Self-Healing Mechanism for Cloud AI Systems via Integration of Large Language Models and Deep Reinforcement Learning," *arXiv*, 2025. [arXiv](#)
3. Cheng Ji, Huaiying Luo, "Cloud-Based AI Systems: Leveraging Large Language Models for Intelligent Fault Detection and Autonomous Self-Healing," *arXiv*, 2025. [arXiv](#)
4. Thatikonda, Kalyan Chakravarthy, "Distributed Intelligence for Distributed Systems Resilience: A Meta-Analysis of Artificial Intelligence Driven Self-Healing Systems," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2025. [ijsrcseit.technoscienceacademy.com](#)
5. Sasank Tummalpalli, "Self-Healing Network Infrastructure: The Future of Autonomous Network Management," *International Journal of Research in Computer Applications and Information Technology (IJRCAIT)*, 2025. [IAEME+1](#)
6. Monisha D. R. & Poornima Devi M., "Intelligent Agent for AI-Based Network Troubleshooting, Predictive Diagnosis and Self-Healing for Reliable Connectivity," *International Journal of Inventive Engineering and Sciences (IJIES)*, 2025. [journals.blueeyesintelligence.org](#)
7. Santhosh K. & Gary D., "Self-Healing Networks: Implementing AI-Powered Mechanisms to Automatically Detect and Resolve Network Issues with Minimal Human Intervention," *International Journal of Scientific Research and Engineering Development*, 2023. [ijsred.com](#)
8. Manohar Jain, "Self-Healing Networks with AI-Based Fault Prediction in IoT Ecosystems," *International Journal of Scientific Research & Engineering Trends (IJSRET)*, 2025. [IJSRET+1](#)
9. Manoj Kumar Reddy Kalakoti, "AI-Augmented Self-Healing Infrastructure: Combining Health Probes with Remediation Playbooks," *Journal of Information Systems Engineering and Management (JISEM)*, 2025. [JISEM](#)
10. Alauthman, A., & Al-Hyari, A., "Intelligent Fault Detection and Self-Healing Mechanisms in Wireless Sensor Networks Using Machine Learning and Flying Fox Optimization," *Computers (MDPI)*, 2025. [MDPI](#)
11. J.V.Anil Kumar, G.Rajeswari,B.Vijaya Lakshmi, V.Subhasri Reddy and S. Sumana Sri , "Machine Learning Techniques For Search Engine Development". *International Journal of Computer Engineering and Applications* 16(9): pp. 25-32. Volume XV, Issue IV, APRIL 2025, ISSN NO : 2249-7455.
12. J.V.Anil Kumar, M. Amith, P. Lakshmi Usha Sri, K. Bewala, G. Kavya and SK.Abdul Munaf, "The Case Of Cross-Site Request Forgery And Machine Learning For Web Vulnerability", *Detection. International Journal of Computer Engineering and Applications* 16(9): pp.239-251.
13. J.V. Anil Kumar, Naru Kamalnath Reddy, Bollavaram Gopi, Derangula Akhil, Dareddy Indra Sena Reddy, Akkalaakhil , "Language-Based Phishing Threat Detection Using ML And Natural Language Processing", *International Journal of Management, Technology And Engineering*

- (IJMTE), Volume XV, Issue IV, April 2025, Page No : pp. 406-416, ISSN NO : 2249-7455, 2025.
14. J.V.Anil Kumar, Siddi Triveni, Yaragorla Sravya, Mancha Mancha. Venkata Aksh, Posani Lahari Priya, Grandhe Sirisha , “Tools For Database Migration”, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : pp. 760-766, ISSN NO : 2249-7455, 2025.
 15. SK Althaf HussainBasha, Shaik Yasmin Sulthana, “IOT Based Shutter Alarm Security System” Journal of Engineering Sciences (JES), Vol.11, Issue 7,July/2020, pp.1035-1045, ISSN No:0377-9254.
 16. Sk Althaf Hussain Basha, A. Amrutavalli, Mekala Anjali Lavanya, Vanama Dhakshayayani Sriya, Grandhisila Jahnavi, Pari Chaitanya Lakshmi , “Cloud-Based Decision Support Systems For Business Data Intelligence”, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, APRIL 2025, Page No : 303-313, ISSN NO : 2249-7455, 2025.
 17. Sk Althaf Hussain Basha, A. Amrutavalli, Mekala Anjali Lavanya, Vanama Dhakshayayani Sriya, Grandhisila Jahnavi, Pari Chaitanya Lakshmi , “Cloud-Based Decision Support Systems For Business Data Intelligence”, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : 303-313, ISSN NO : 2249-7455, 2025.
 18. Sk. Althaf Hussain Basha, G. Mahesh, Kokkera Krishnaveni, Gadde Koushika, Derangula Manasa, Yalla Pranavi, “Honeytrap-Enabled Cloud Security Framework For Preventing Network Breaches”, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : 453-463 , ISSN NO : 2249-7455, 2025.