Design And Implementation Of Statistical Time-Based Intrusion Detection In Embedded Systems

N. Prasanthi[1], Kommu Srividya[2], Papanaboina Dines[3], Marisetty Ashok[4] ,Mothukuri Satish[5],

[2,3,4,5]UG Student,ECE,Chalapathi Institute Of Engineering&Technology Guntur-Andhra Pradesh,India

[1] Assistant Professor ECE,Chalapathi Institute Of Engineering&Technology Guntur-Andhra Pradesh,India

***Abstract*— Ensuring the security of embedded systems against unauthorized access has become a critical necessity due to their rapid integration into sensitive applications. This project introduces a robust Statistical Time-Based Intrusion Detection System (IDS) specifically engineered for resource-constrained embedded environments. At its core, the system utilizes an Arduino Uno (UNO) as the central processing unit, seamlessly interfaced with a multi-sensor array consisting of vibration and Passive Infrared (PIR) sensors to monitor physical activities in real-time. By continuously analyzing sensor data streams, the system employs advanced statistical techniques to identify anomalies based on predefined temporal patterns. Any significant deviation from established normal behavior is immediately flagged as a potential security breach. Once a suspicious event is detected, the architecture triggers a multi-layered alert mechanism: a local buzzer for immediate warning, an LCD display for real-time status updates, and a GSM module to transmit remote notifications to the user. This approach prioritizes low-cost hardware and energy efficiency, making it a scalable solution for home security, industrial monitoring, and high-security restricted areas.**

I. INTRODUCTION

In recent years, embedded systems have become an integral part of modern technology, powering applications ranging from home automation and industrial control to security and surveillance systems. As these systems increasingly operate in sensitive and critical environments, ensuring their protection against unauthorized access and intrusion has become a major concern. Traditional security mechanisms often rely on static rules or expensive infrastructure, making them less suitable for low-cost, resource-constrained embedded devices.

This project focuses on the design and implementation of a Statistical Time-Based Intrusion Detection System (IDS) tailored for embedded systems. The core idea is to monitor environmental and motion-based activities using sensors and analyze their behavior over time to detect unusual or suspicious patterns. Unlike conventional systems that only respond to direct triggers, this approach incorporates statistical analysis of time-based data, enabling more intelligent and reliable detection of intrusions.

The system is built around an Arduino Uno microcontroller, which serves as the central processing unit. It receives inputs from sensors such as a vibration sensor and a PIR sensor, processes the data, and evaluates it against predefined normal behavior patterns. When an anomaly is detected, the system activates multiple alert mechanisms, including a buzzer for immediate warning, an LCD display for status indication, and a GSM module to send remote notifications.

The motivation behind this project is to develop a cost-effective, real-time, and efficient intrusion detection solution that can be deployed in various environments such as homes, offices, and restricted areas. By combining embedded system design with statistical analysis, the project aims to enhance the reliability and intelligence of security systems while maintaining simplicity and affordability.

II. REVIEW LITERATURE SURVEY

Dorothy E. Denning (1987) introduced one of the earliest models for intrusion detection systems based on statistical anomaly detection. Her work proposed monitoring system activities over time and identifying deviations from established normal behavior. This foundational approach forms the basis for many modern anomaly-based IDS techniques.

Stephanie Forrest et al. (1994) proposed a biologically inspired intrusion detection approach using artificial immune systems. Their research focused on detecting anomalies in distributed systems by mimicking the human immune response. Although adaptive, these

Doi:10.48047/ijiee.2026.16.2.27

methods required significant computational resources, making them less suitable for constrained embedded systems.

Sandeep Kumar et al. (2016) developed a low-cost intrusion detection system using microcontroller-based platforms such as Arduino Uno. Their system integrated basic sensors to detect unauthorized access, demonstrating the feasibility of implementing security mechanisms in resource-limited environments.

Ravi Kishore Kodali et al. (2017) designed an IoT-based home security system using PIR sensors and GSM modules. The system enabled real-time monitoring and remote alert notifications, highlighting the effectiveness of combining embedded systems with communication technologies for security applications.

Alessandro Coluccia et al. (2018) explored statistical signal processing techniques for anomaly detection in sensor networks. Their work emphasized time-series analysis and threshold-based detection methods, which are computationally efficient and suitable for real-time embedded applications.

Mehdi Bahrami et al. (2020) investigated lightweight intrusion detection mechanisms for IoT environments. Their research focused on reducing power consumption and improving detection accuracy, addressing key challenges in embedded system security.

III. RESEARCH METHODOLOGY

The methodology adopted for the development of the Industrial Automated Multipurpose Robot using WiFi is based on the design, integration, and implementation of hardware and software components to achieve efficient industrial automation. The system is designed using an Arduino microcontroller as the central processing unit, which controls all operations of the robot including movement, sensing, and communication.

In the first stage, the hardware components such as motors, motor drivers, ultrasonic sensors, WiFi module, and Bluetooth module are selected and integrated with the Arduino board. The pick-and-place mechanism is designed to handle objects efficiently, enabling the robot to perform industrial tasks such as sorting, loading, and unloading materials.

In the second stage, the communication system is implemented using WiFi and Bluetooth modules, allowing real-time wireless control and monitoring of the robot. This enables the user to operate the robot remotely through a mobile device or computer interface, improving flexibility and safety.

In the third stage, sensor integration is carried out using an ultrasonic sensor to detect obstacles and measure distance. This ensures that the robot can navigate safely in its environment and avoid collisions during operation.

Finally, programming is done using the Arduino IDE to control all hardware components. The code is developed to coordinate motor movements, process sensor data, and manage wireless communication. Testing and debugging are performed to ensure smooth operation and reliability of the system.

This systematic methodology ensures the successful development of a cost-effective, efficient, and intelligent robotic system suitable for modern industrial applications.

IV. PROPOSED METHODOLOGY

The proposed system implements a Statistical Time-Based Intrusion Detection System (IDS) designed specifically for resource-constrained embedded environments. At the core of the system is the Arduino Uno, which serves as the central processing unit and coordinates the operation of all connected components. The system integrates a Passive Infrared (PIR) sensor to detect human motion and a vibration sensor to identify physical disturbances such as tampering or forced entry. These sensors continuously monitor the surroundings and generate real-time data, which is periodically sampled and processed by the microcontroller.

The methodology is based on statistical time-based analysis, where the system initially undergoes a learning phase to establish normal behavioral patterns. During this phase, parameters such as frequency, duration, and timing of sensor activations are recorded and analyzed to compute threshold values using basic statistical measures like mean and variance. Once the baseline behavior is established, the system continuously compares incoming sensor data against these predefined thresholds. Any significant deviation from normal patterns is classified as a potential intrusion, ensuring effective anomaly detection without the need for computationally intensive algorithms.

When an intrusion is detected, the system activates a multi-layered alert mechanism to ensure immediate response. A buzzer is triggered to provide a local audible warning, while an LCD display shows real-time status messages indicating the nature of the alert. Simultaneously, a GSM module sends an SMS notification to the registered user, enabling remote monitoring and quick action.

V. WORKING PRINCIPLE

The working principle of the proposed intrusion detection system is based on continuous sensing, statistical evaluation, and real-time alert generation using an embedded platform. The system is centered around the Arduino Uno, which processes

Doi:10.48047/ijiee.2026.16.2.27

inputs from multiple sensors to identify unauthorized activities.

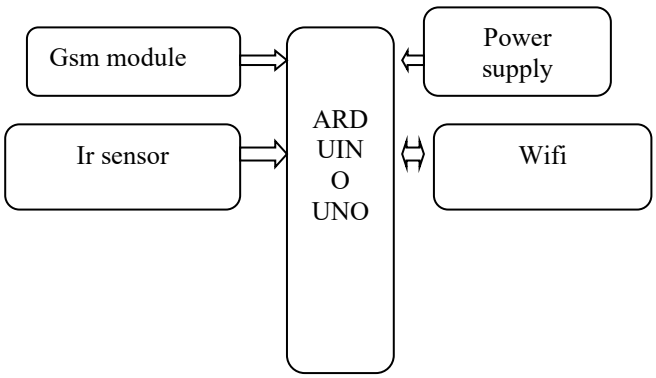
In this implementation, an **IR (Infrared) sensor** and an **ultrasonic sensor** are used for detection. The IR sensor is responsible for identifying the presence or interruption of an object within its range, making it effective for short-distance obstacle or motion detection. The ultrasonic sensor measures the distance to nearby objects by emitting ultrasonic waves and calculating the time taken for the echo to return. This allows the system to detect movement or changes in position within a defined area.

The system continuously collects data from both sensors at regular intervals. During an initial calibration phase, normal environmental conditions are recorded, and threshold values are established based on distance measurements and detection frequency. These thresholds represent standard, non-threatening activity within the monitored space.

During operation, the incoming sensor data is compared against these predefined thresholds using a statistical time-based approach. If the IR sensor detects frequent interruptions or if the ultrasonic sensor registers sudden or significant changes in distance beyond the normal range, the system interprets this as an anomaly. Additionally, repeated or rapid changes within a short time frame strengthen the likelihood of an intrusion event.

Once an intrusion is detected, the system activates its alert mechanisms. A buzzer is triggered to provide an immediate audible warning, and the LCD display shows a status message such as “Intrusion Detected.” Simultaneously, the GSM module sends an SMS alert to the authorized user, enabling remote monitoring and quick response.

VI. BLOCK DIAGRAM



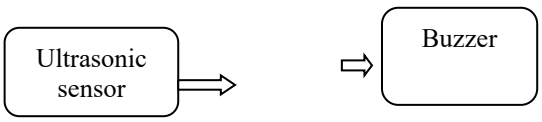


Fig. 6.2. Block Diagram

VII. RESULTS AND OUTCOMES

Statistical Time-Based Intrusion Detection System (IDS) was successfully implemented using the Arduino Uno along with IR and ultrasonic sensors. The system was tested under various real-time conditions to evaluate its performance in detecting unauthorized activities and generating alerts.

The results demonstrate that the system is capable of accurately detecting intrusions based on deviations from normal sensor behavior. The IR sensor effectively identified object presence and interruptions, while the ultrasonic sensor reliably measured distance variations to detect movement within the monitored area. By combining these sensors with a time-based statistical approach, the system was able to reduce false alarms and improve detection accuracy compared to single-sensor systems.

During testing, the system responded promptly to intrusion events. Whenever abnormal activity was detected, the buzzer was immediately activated, providing a local alert. Simultaneously, the LCD display updated the system status in real time, indicating the presence of an intrusion. The GSM module successfully transmitted SMS notifications to the registered user without significant delay, ensuring remote awareness of security breaches.

The system also exhibited stable performance over continuous operation, maintaining consistent monitoring without significant errors or system crashes. Its low power consumption and efficient processing make it suitable for long-term deployment in resource-constrained environments.

Doi:10.48047/ijiee.2026.16.2.27

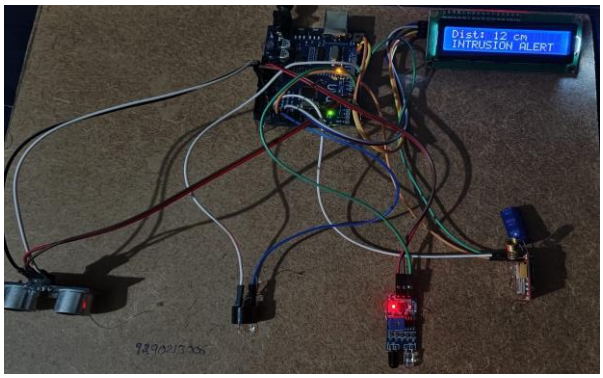


Fig. 7.1. Output1

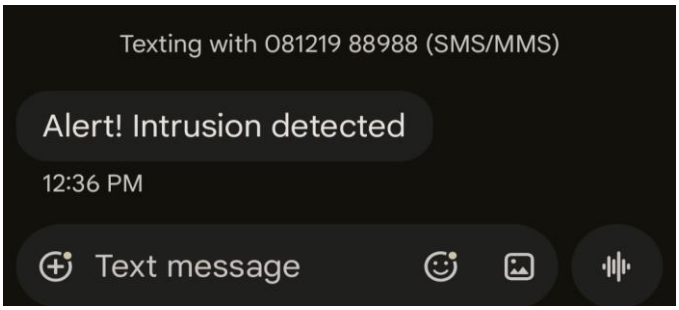


Fig. 7.2. Output2

Overall, the prototype validates that the proposed system is cost-effective, scalable, and adaptable for various real-world applications such as home security, industrial monitoring, and smart surveillance systems. Future improvements can include integration with IoT platforms for cloud-based monitoring, mobile app notifications, and advanced machine learning techniques to further enhance detection accuracy and system intelligence.

VIII.CONCLUSION

The Statistical Time-Based Intrusion Detection System for Embedded Systems presents a practical and intelligent solution for enhancing security in modern embedded applications. By combining hardware components such as sensors, microcontrollers, and communication modules with statistical analysis techniques, the system is capable of detecting intrusions more effectively than traditional threshold-based methods.One of the key strengths of this project lies in its ability to analyze time-based behavioral patterns rather than relying solely on direct sensor triggers. This allows the system to identify subtle anomalies that may otherwise go unnoticed, thereby improving overall detection accuracy and minimizing false alarms. The integration of multiple sensors, such as PIR and vibration sensors, further strengthens the reliability of the system by providing multi-level verification of events.Additionally, the implementation using an Arduino Uno ensures that the system remains low-cost, energy-efficient, and easy to deploy, making it suitable for a wide range of applications including home security, industrial monitoring, and remote surveillance. The inclusion of a GSM module for remote alerts enhances the usability of the system by enabling real-time communication with users, even in the absence of internet connectivity.Despite its advantages, the system may face certain limitations, such as dependency on predefined statistical models and sensitivity to environmental changes. However, these challenges can be addressed in future enhancements by incorporating adaptive learning techniques or lightweight machine learning algorithms to further improve detection capabilities.In conclusion, this project successfully demonstrates that statistical time-based analysis can significantly enhance intrusion detection in embedded systems

IX. REFERENCES

1. Vellela, S. S., & Balamanigandan, R. (2024). Optimized clustering routing framework to maintain the optimal energy status in the wsn mobile cloud environment. Multimedia Tools and Applications, 83(3), 7919-7938.
2. Vellela, S. S., & Balamanigandan, R. (2023). An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-

Doi:10.48047/ijiee.2026.16.2.27

Peer Networking and Applications, 16(6), 2714-2731.
3. Vellela, S. S., & Balamanigandan, R. (2024). An efficient attack detection and prevention approach for secure WSN mobile cloud environment. Soft Computing, 28(19), 11279-11293.
4. Vellela, S. S. (2023). Enhanced speckle noise reduction in breast cancer ultrasound imagery using a hybrid deep learning model. Ingénierie des Systèmes d'Information.
5. Polasi, P. K., Vellela, S. S., Narayana, J. L., Simon, J., Kapileswar, N., Prabu, R. T., & Rashed, A. N. Z. (2026). Data rates transmission, operation performance speed and figure of merit signature for various quadurature light sources under spectral and thermal effects. Journal of Optics, 55(1), 633-643.
6. Praveen, S. P., Nakka, R., Chokka, A., Thatha, V. N., Vellela, S. S., & Sirisha, U. (2023). A novel classification approach for grape leaf disease detection based on different attention deep learning techniques. International Journal of Advanced Computer Science and Applications (IJACSA), 14(6), 2023.
7. Vellela, S. S., Rao, M. V., Mantena, S. V., Reddy, M. J., Vatambeti, R., & Rahman, S. Z. (2024). Evaluation of Tennis Teaching Effect Using Optimized DL Model with Cloud Computing System. International Journal of Modern Education and Computer Science (IJMECS), 16(2), 16-28.
8. Vellela, S. S., & Krishna, A. M. (2020). On Board Artificial Intelligence With Service Aggregation for Edge Computing in Industrial Applications. Journal of Critical Reviews, 7(07).
9. Madhuri, A., Jyothi, V. E., Praveen, S. P., Sindhura, S., Srinivas, V. S., & Kumar, D. L. S. (2024). A new multi-level semi-supervised learning approach for network intrusion detection system based on the 'goa'. Journal of Interconnection Networks, 24(supp01), 2143047.
10. Raju, V. V. K., Bhavani, Y. V. K. D., Nandikonda, P., Kareemunnisa, F. N. U., Brahmeswara, K. B., & Sindhura, S. (2026). Iterative and Statistical Analytical Review of Predictive Modeling Approaches in Educational Systems: A Comprehensive Benchmark of AI-Driven Methods. International Journal of Innovative Technology and Interdisciplinary Sciences, 9(1), 490-522.
11. Biyyapu, N., Veerapaneni, E. J., Surapaneni, P. P., Vellela, S. S., & Vatambeti, R. (2024). Designing a modified feature aggregation model with hybrid sampling techniques for network intrusion detection. Cluster Computing, 27(5), 5913-5931.
12. Praveen, S. P., Vellela, S. S., & Balamanigandan, R. (2024). SmartIris ML: harnessing machine learning for enhanced multi-biometric authentication. Journal of Next Generation Technology (ISSN: 2583-021X), 4(1).
13. Vuyyuru, L. R., Purimetla, N. R., Reddy, K. Y., Vellela, S. S., Basha, S. K., & Vatambeti, R. (2025). Advancing automated street crime detection: a drone-based system integrating CNN models and enhanced feature selection techniques. International Journal of Machine Learning and Cybernetics, 16(2), 959-981.
14. Vellela, S. S., Roja, D., Purimetla, N. R., Thalakola, S., Vuyyuru, L. R., & Vatambeti, R. (2025). Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection. Computers and Electrical Engineering, 124, 110368.
15. Vellela, S. S., Pushpalatha, D., Sarathkumar, G., Kavitha, C. H., & Harshithkumar, D. (2023). Advanced intelligence health insurance cost prediction using random forest. ZKG International, 8.
16. Vellela, S. S., Babu, B. V., & Mahendra, Y. B. (2024). IoT-based tank water monitoring systems: enhancing efficiency and sustainability. International Journal for Modern Trends in Science and Technology, 10(02), 291-298.
17. Vellela, S. S., Varshini, K., Jeevana, M., Kadheer, S. K., & Kumar, T. P. (2024). Iot based smart irrigation and controlling system. IoT Based Smart Irrigation and Controlling System, International Journal for

Doi:10.48047/ijiee.2026.16.2.27

Modern Trends in Science and Technology, 10(02), 77-85.
18. Vellela, S. S., Chaganti, A., Gadde, S., Bachina, P., & Karre, R. (2022). A Novel Approach for Detecting Automated Spammers in Twitter. Mukt Shabd, 11, 49-53.
19. Vellela, S. S., Narapasetty, S., Somepalli, M., Merikapudi, V., & Pathuri, S. (2022). Fake News Articles Classifying Using Natural Language Processing to Identify in-article Attribution as a Supervised Learning Estimator. Mukt Shabd Journal, 11.
20. Vellela, S. S., Vineeth, S., & Suresh, V. (2024). IoT Based ICU Patient Monitoring System. IoT Based ICU Patient Monitoring System, International Journal for Modern Trends in Science and Technology, 10(02), 265-273.
21. Vellela, S. S., & Balamanigandan, R. (2025). Designing a Dynamic News App Using Python. Available at SSRN 5250912.
22. Vellela, S. S., Rao, M. V., Krishna, C. V. M., Rao, T. S., & Dasthavejula, R. (2026). Piezoelectric and Shape-Memory Materials for Actuators and Energy Harvesting in Mechanical, Electronics, and Biomedical Engineering Using AI-Based Design. In Advanced Materials for Biomedical Devices (pp. 195-206). CRC Press.
23. Vellela, S. S., Singu, K., Kakarla, L. S., Tadikonda, P., & Sattenapalli, S. N. R. (2025). NLP-Driven Summarization: Efficient Extraction of Key Information from Legal and Financial Documents. Available at SSRN 5250908.
24. Vellela, S. S., Anusha, P., Vullam, N. R., Jala, J., Bellapu, V. S., & Vindhya, A. S. (2025, October). Quantum Cryptography and Key Distribution for Secure Communication in the Post Quantum World. In 2025 International Conference on Sustainable Communication Networks and Application (ICSCN) (pp. 619-624). IEEE.
25. Roja, D., Jidugu, S. K., Rao, T. S., Vuyyuru, L. R., Vellela, S. S., & Ranjani, B. S. (2025, December). High-Fidelity Image Synthesis using Enhanced Generative Adversarial Networks with Attention Mechanisms. In 2025 International Conference on NexGen Networks and Cybernetics (IC2NC) (pp. 885-890). IEEE.
26. Vellela, S. S., Vuyyuru, L. R., Jidugu, S. K., Rao, M. P., & Srinivas, B. R. (2025, November). The Impact Of Quantum Computing On Blockchain Security And Quantum Resistant Protocols. In 2025 2nd International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1-6). IEEE.
27. Yanamadala, N., & Vellela, S. S. (2025, June). Ensuring Authenticity and Confidentiality in Images using SHA-ECC Fusion. In 2025 Second International Conference on Networks and Soft Computing (ICNSoC) (pp. 684-689). IEEE.
28. Vellela, S. S. (2024). A Comprehensive Review of AI Techniques in Serious Games: Decision Making and Machine Learning.
29. Burra, R. S., APCV, G. R., & Vellela, S. S. (2024). Strategic Insights: Unleashing the Power of Big Data Analytics for Credit Investigation and Risk Mitigation in Commercial Banking. International Journal of Progressive Research in Engineering Management and Science, 4(01), 458-464.
30. Vellela, S. S., Purimetla, N. R., Vindhya, A. S., Vullam, N. R., Srinivas, B. R., & Vuyyuru, L. R. (2025, October). Design and Simulation of Quantum Error Correction Codes for Scalable Quantum Architectures. In 2025 7th International Conference on Innovative Data Communication Technologies and Application (ICIDCA) (pp. 1570-1575). IEEE.
31. Vellela, S. S., Purimetla, N. R., Rao, P. V., Daniel, V. A. A., Koppolu, H. K. R., & Janani, B. (2025). AI-Enabled Wearable Hemodynamic Monitoring System for Early Identification of Thrombotic Events. Vascular and Endovascular Review, 8(16s), 321-336.
32. Venkatesh, N., Maheswari, S., & Triveni, P. (2024). Harnessing IoT for Real-Time Plant Health Monitoring: Challenges and Opportunities.
33. Reddy, B. V., Kumar, A. H., Gopi, C., Prasad, Y. V. D., Vellela, S. S., & Roja, D. (2025, April). Machine learning based automated liver fibrosis stage diagnosis with prediction. In 2025

Doi:10.48047/ijiee.2026.16.2.27

International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE) (pp. 1-6). IEEE.

34. Rao, M. V., Sreeraman, Y., Mantena, S. V., Gundu, V., Roja, D., & Vatambeti, R. (2024). Brinjal Crop yield prediction using Shuffled shepherd optimization algorithm based ACNN-OBDLSTM model in Smart Agriculture. Journal of Integrated Science and Technology, 12(1), 710-710.
35. Haritha, K., Geethika, N. S., Venkateswarlu, K., Kumar, R. H., & Ramakrishna, Y. Enhancing Public Safety with AI & ML-Based CCTV Surveillance.
36. Haritha, K., Prakash, P. B., Pravallika, D., Venkatesh, K., & Venkatesh, G. Enhancing Object Detection in Autonomous Vehicles Under Low-Light Conditions Using Federated Learning and YOLOv5.
37. Ram, C. S., Vellela, S. S., Sravanthi Javvadi, D. V., Rashid, S. Z., & Madhumathi, S. M. (2025). Integrated Robotic–Imaging Platforms in Endovascular Surgery: Current Capabilities and Future Directions. Vascular and Endovascular Review, 8(16s), 285-298.
38. Roja, D., Navya, G., Srujana, B. S., Mamatha, P., & Sai, C. Y. K. Deep Learning for Hotel Reviews: A Framework for Sentiment Classification and Fake Review Detection.
39. Pakalapati, S., Rani, C. J., Vellela, S. S., Thanuja, N., & Bindu, M. N. H. (2025, November). Progressive GAN-based Framework for Realistic Image Generation and Style Transfer. In 2025 5th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN) (pp. 474-479). IEEE.
40. Balamanigandan, R., Vellela, S. S., Gorintla, S., Vuyyuru, L. R., Thanuja, N., & Rao, T. S. (2025, September). Quantum-Enhanced Data Security for Electronic Health Records: A Framework for Post-Quantum Cryptography in Healthcare Systems. In 2025 6th International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1924-1929). IEEE.
41. Roja, D., Amulya, P., Nagasai, M., Prasad, D. D., & Babu, A. V. Machine Learning-Based Early Diagnosis of Fish Diseases via Water Quality Data.
42. Sai, M. B., & Vellela, S. S. (2025, December). Hybrid ML Driven Multi-Cloud Service Work Load Prediction For Financial Systems. In 2025 1st International Conference on Advancement in Futuristic Technologies (ICAFT) (pp. 1-6). IEEE.
43. Kareemunnisa, D., Haritha, K., Ranjani, B. S., Venkateswarlu, K., & Bindu, M. N. H. DUAL-STAGE PRIVACY PROTECTION FOR GRAPH NEURAL NETWORKS AGAINST INFERENCE ATTACKS.
44. Mandava, R., Haritha, K., Vellela, S. S., Purimetla, N. R., Mohan, B. K., & Harinadh, T. (2025, June). Analysing User Perceptions of Trust in Financial Systems Using Explainable AI. In 2025 Second International Conference on Networks and Soft Computing (ICNSoC) (pp. 26-30). IEEE.

Doi:10.48047/ijiee.2026.16.2.27