iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81261

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Smart AI-Enabled Security Framework for IoT System

Mrs. Suvarna Potdukhe[1], Sarthak Pagar[2], Vivek Dake[3], Shashwat Deshmukh[4], Tushar Dalave[5]
Information Technology, Pune, India

Abstract: ***The rapid expansion of Internet of Things (IoT) systems has significantly improved automation, connectivity, and real-time monitoring across various domains. However, the increasing number of connected devices has also introduced critical security vulnerabilities, including unauthorized access, data manipulation, and replay attacks. Traditional security mechanisms are often insufficient due to their static nature and inability to adapt to evolving threats. This paper proposes a Smart AI-enabled security framework for IoT systems that integrates machine learning techniques for real-time anomaly detection and automated threat mitigation. The framework continuously monitors sensor data and network activity, identifying abnormal patterns using a trained AI model. Upon detecting suspicious behavior, the system triggers automated responses such as alert generation and access restriction. The proposed solution enhances detection accuracy, reduces response time, and improves overall system reliability. Experimental evaluation demonstrates the effectiveness of the framework in securing IoT environments against modern cyber threats.***

Keywords: Internet of Things (IoT), Artificial Intelligence, Cybersecurity, Anomaly Detection, Intrusion Detection System, Machine Learning, Smart Monitoring.

Problem Statement: In IoT-based systems, especially in critical environments like cold storage, the absence of robust security mechanisms makes them vulnerable to cyberattacks such as Denial of Service (DoS), Replay, and Data Poisoning, leading to manipulated sensor data, operational failures, and loss of reliability.

I. INTRODUCTION

The Internet of Things (IoT) has revolutionized modern computing by enabling seamless communication between devices, sensors, and cloud platforms. IoT systems are widely used in applications such as smart homes, healthcare, industrial automation, and environmental monitoring. Despite their benefits, IoT devices are highly vulnerable to cyber threats due to limited computational capabilities, lack of standardized security protocols, and large-scale deployment.

Security threats such as data injection, replay attacks, and unauthorized access can compromise system integrity and lead to significant operational failures. Traditional security approaches rely on static rules and predefined signatures, which are ineffective in detecting dynamic and evolving attack patterns. Artificial Intelligence (AI) offers a promising solution by enabling systems to learn from data and identify anomalies in real time. AI-based security frameworks can automatically adapt to new threats, improving detection accuracy and response efficiency. This paper presents a smart AI-enabled security framework that combines IoT monitoring with intelligent anomaly detection and automated mitigation strategies. The proposed system ensures secure data transmission, real-time threat detection, and improved reliability in IoT environments.

II. RELATED WORK

Recent research in IoT security has explored various approaches to address vulnerabilities in connected systems. Traditional methods such as encryption, authentication, and firewall-based protection provide basic security but are insufficient against advanced cyberattacks. Machine learning-based intrusion detection systems have gained attention due to their ability to analyze large volumes of data and detect anomalies. Techniques such as Support Vector Machines (SVM), Decision Trees, and Neural Networks have been applied for identifying malicious activities in IoT networks. These methods improve detection accuracy but often require high computational resources and lack real-time response mechanisms.

Several studies have proposed AI-driven frameworks for IoT security, focusing on anomaly detection and predictive threat analysis. These approaches demonstrate improved performance compared to conventional methods but still face challenges such as false positives, scalability issues, and delayed response.

The proposed framework addresses these limitations by integrating real-time monitoring, AI-based anomaly detection, and automated mitigation mechanisms, providing a comprehensive and efficient solution for IoT security.

III. LITERATURE SURVEY

[1] Gajjar et al. present a comprehensive survey on security challenges in the Internet of Things (IoT) ecosystem and explore the role of Machine Learning (ML) and Blockchain in mitigating these threats. The study analyzes security vulnerabilities across the perception, network, and application layers, including attacks such as DoS, replay attacks, node capture, and malware injection. The authors highlight blockchain's capability to ensure data integrity and decentralized trust, while ML techniques improve anomaly detection and intrusion prevention. Although the paper provides a broad taxonomy of IoT threats and solutions, it lacks in-depth technical implementation details.

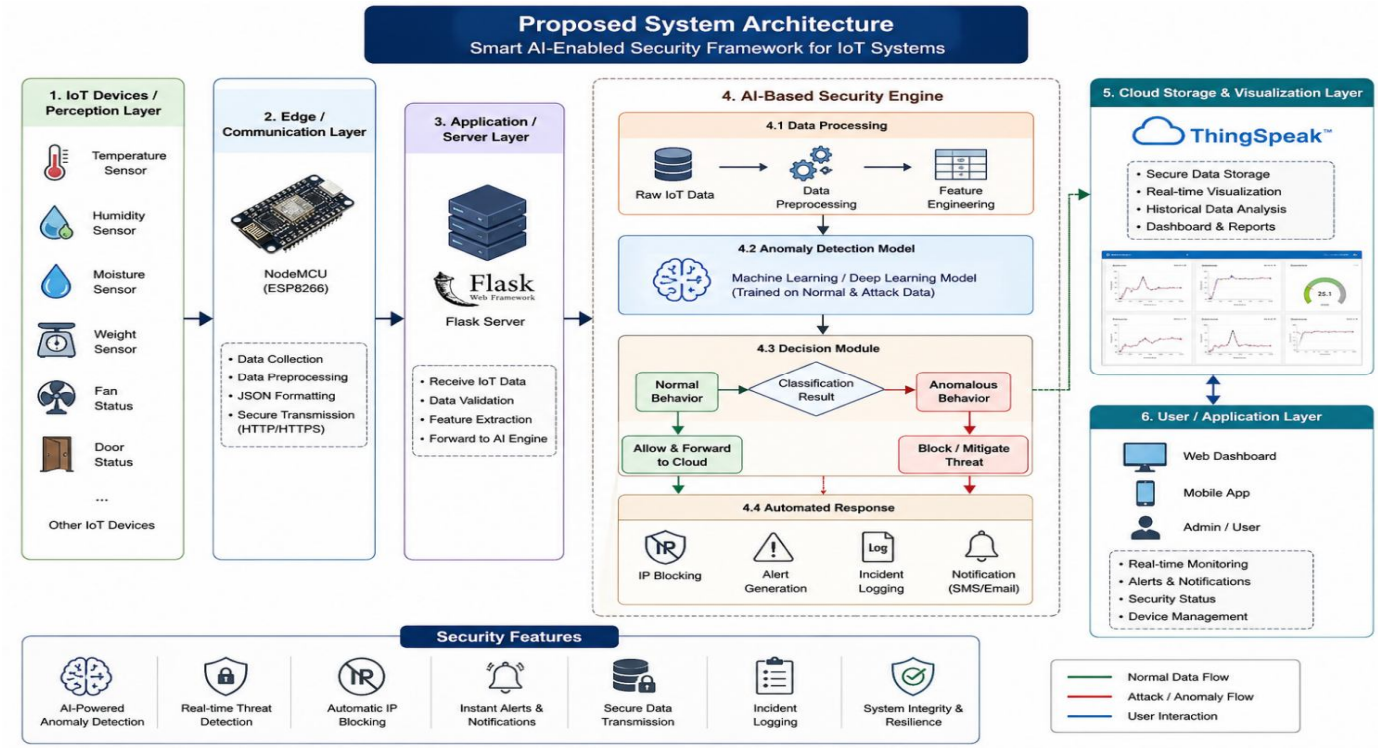
[2] Menon et al. examine the integration of Artificial Intelligence with IoT, commonly referred to as AIoT, focusing on improvements in security, efficiency, and automation. The survey discusses how ML and Deep Learning (DL) enhance IoT systems by enabling intelligent decision-making and adaptive security mechanisms across domains such as healthcare, smart cities, and industrial automation. The study emphasizes AI-driven analytics for real-time monitoring and threat detection, highlighting the transformative impact of AI on large-scale IoT deployments.

[3] Gilbert and Gilbert investigate AI-driven threat detection mechanisms in IoT environments, emphasizing the limitations of traditional security approaches. The paper identifies major vulnerabilities such as insecure boot processes, unauthorized access, and data leakage, supported by statistical analysis of reported IoT security incidents. The authors propose the use of ML, DL, and Reinforcement Learning (RL) models to enable adaptive and real-time threat detection, demonstrating the potential of AI-based frameworks in enhancing IoT security resilience.

[4] Prabhakar et al. provide an extensive survey of IoT security challenges, threats, and emerging countermeasures across different architectural layers. The study highlights physical attacks and node tampering at the perception layer, communication-based attacks at the network layer, and data privacy issues at the application layer. The authors emphasize the need for scalable and adaptive security solutions, reviewing cryptographic, authentication, and intrusion detection mechanisms suited for resource-constrained IoT environments.

[5] Raj and Kamble review the role of Artificial Intelligence in strengthening IoT security, focusing on Machine Learning and Deep Learning-based approaches. The paper discusses the shortcomings of traditional security mechanisms and demonstrates how AI-based models can detect anomalies, identify zero-day attacks, and automate security responses. The study concludes that AI-driven security solutions are essential for handling the dynamic and heterogeneous nature of modern IoT networks.

Proposed System Architecture



The proposed AI-powered IoT security monitoring system consists of four major layers:

1) Sensor Layer - Includes temperature, humidity, moisture, and weight sensors deployed inside the cold storage unit.

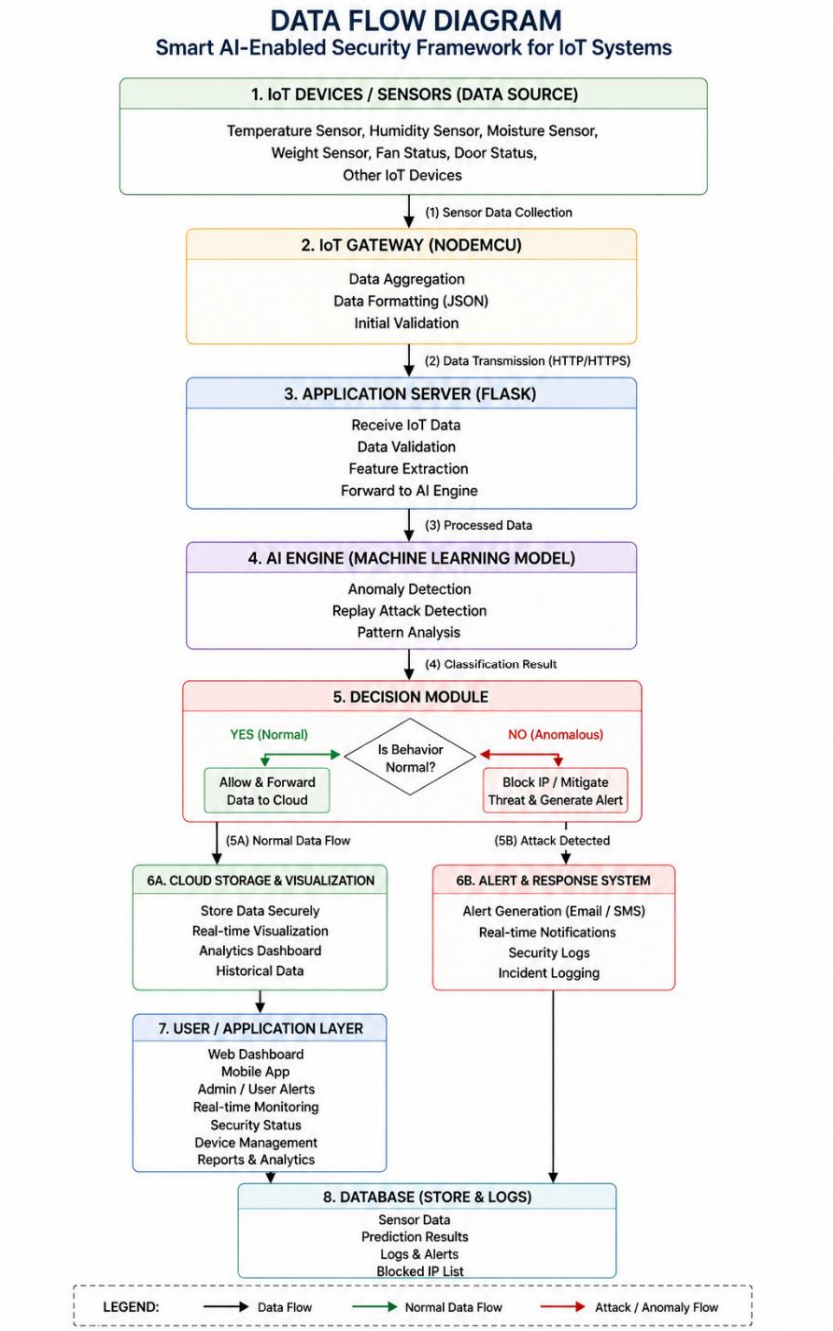
2) IoT Device Layer - NodeMCU (ESP8266) collects sensor data, converts it into JSON format, and transmits it to the server using HTTP protocol.

3) Server and AI Layer - A Flask server receives sensor data and forwards it to a pre-trained machine learning model. The model analyzes the data to detect anomalies and replay attacks.

4) Cloud and User Layer - Valid data is uploaded to the ThingSpeak cloud platform for visualization. In case of attacks, alerts are generated and malicious IPs are blocked automatically.

This layered architecture ensures scalability, security, and real-time monitoring.

Flow Chart



IV. ALGORITHM & RESULT

The proposed AI-powered IoT security monitoring system follows a structured algorithm to ensure secure data acquisition, anomaly detection, and automated mitigation in a smart cold storage environment.

Step 1: Initialize all sensors, NodeMCU (ESP8266), Flask server, and the pre-trained AI anomaly detection model.

Step 2: Periodically collect environmental data from sensors deployed in the cold storage unit.

Step 3: Convert sensor readings into JSON format and transmit the data to the Flask server using the HTTP protocol.

Step 4: Preprocess the received data by normalizing values and extracting relevant features.

Step 5: Apply the trained AI model to classify incoming data as normal or anomalous.

Step 6: If the data is classified as normal, forward it to the ThingSpeak cloud platform for storage and visualization. If the data is classified as anomalous (replay attack or fake data injection), block the source IP address, generate an alert, and log the incident.

Step 7: Control actuators such as cooling fan and door mechanism based on predefined thresholds and system logic.

Step 8: Repeat the process continuously for real-time monitoring and security enforcement.

The AI-based anomaly detection model successfully distinguished between normal sensor behavior and malicious activity. Replay attacks were detected based on repeated timestamps and identical sensor patterns. Fake temperature injection attacks were identified through abnormal deviations from learned normal behavior. The system demonstrated fast response time, ensuring that malicious data did not reach the cloud dashboard. Automatic IP blocking prevented repeated attack attempts from the same source.

V. CONCLUSION

This paper presents a smart AI-enabled security framework designed to enhance the protection of IoT systems against modern cyber threats. By leveraging machine learning techniques, the proposed system effectively detects anomalies and suspicious activities in real time. The integration of automated response mechanisms, such as alert generation and access control, further strengthens system security and reduces human intervention. The experimental results demonstrate that the framework improves detection accuracy, minimizes false positives, and ensures faster response to potential threats. The system is scalable and adaptable, making it suitable for various IoT applications. Future work will focus on incorporating advanced deep learning models, improving detection precision, and integrating emerging technologies such as blockchain for enhanced security and data integrity.

VI. ACKNOWLEDGEMENT

The authors would like to thank their institution and project guide for their support and guidance throughout this research work.

REFERENCES

[1] N. Sharma and P. Dhiman, “A Survey on IoT Security: Challenges and Their Solutions Using Machine Learning and Blockchain Technology,” Cluster Computing, Springer Nature, vol. 28, pp. 1–19, Apr. 2025. doi: 10.1007/s10586-025-05208-0.

[2] V. Menon U., V. B. Kumaravelu, V. Kumar C., R. A., S. Chinnadurai, R. Venkatesan, H. Hai, and P. Selvaprabhu, “AI-Powered IoT: A Survey on Integrating Artificial Intelligence with IoT for Enhanced Security, Efficiency, and Smart Applications,” IEEE Access, vol. 13, pp. 22844–22879, Mar. 2025. doi: 10.1109/ACCESS.2025.3551750.

[3] C. Gilbert and M. A. Gilbert, “AI-Driven Threat Detection in the Internet of Things (IoT): Exploring Opportunities and Vulnerabilities,” International Journal of Research Publication and Reviews, vol. 5, no. 11, pp. 219–236, Nov. 2024. doi: 10.2139/ssrn.5259702.

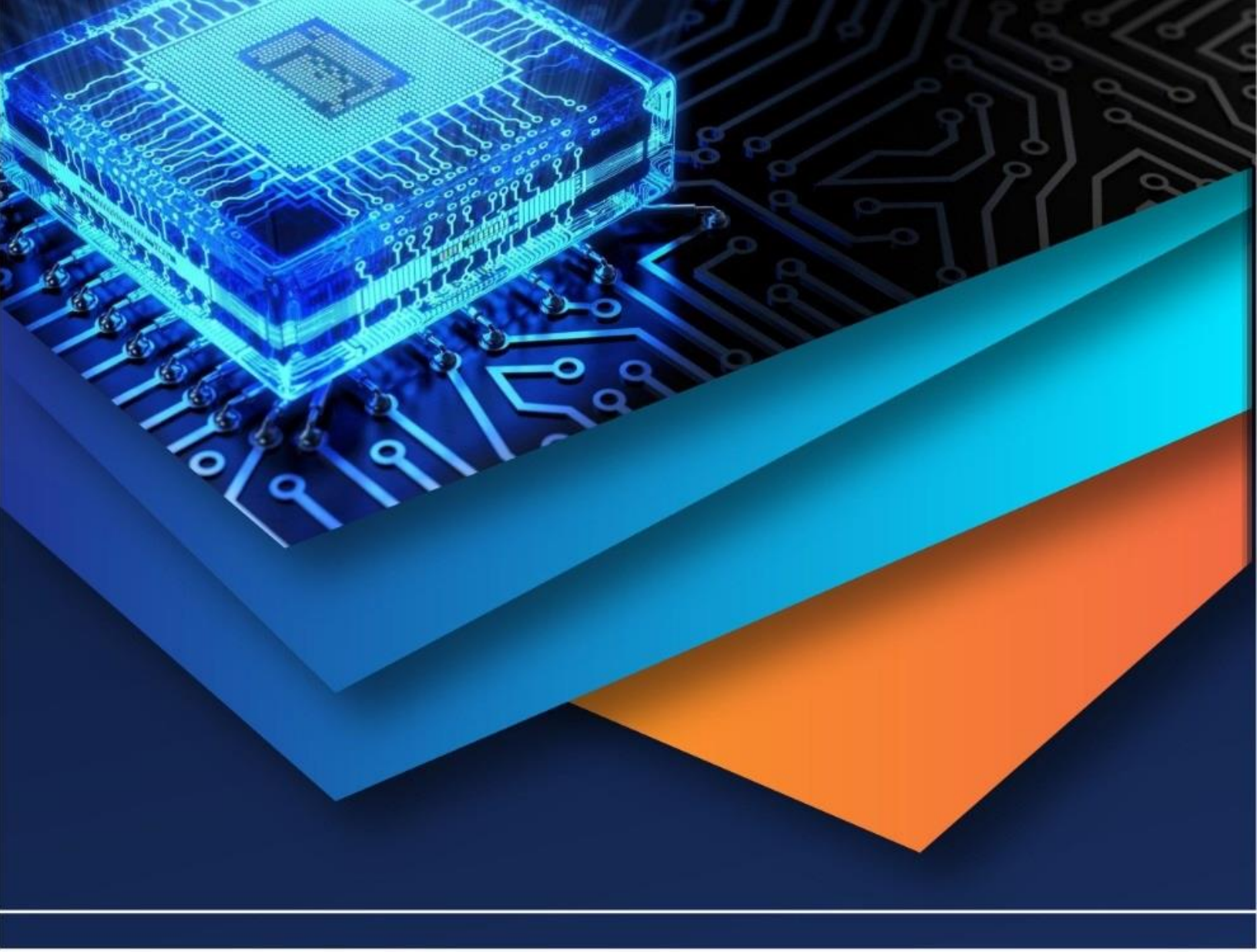
[4] M. Prabhakar, S. Selvarani, S. Manikandan, M. Preethika, and N. Suganya, “A Comprehensive Survey on IoT Security Challenges, Threats, and Emerging Countermeasures,” International Journal of Recent Technology and Engineering (IJRTE), vol. 12, issue 4, Apr. 2024.

[5] Y. Raj and S. D. Kamble, “A Survey on the Role of Artificial Intelligence in Enhancing IoT Security,” International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), vol. 12, no. 11, Nov. 2023.

[6] T. Mazhar, D. B. Talpur, T. A. Al Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, K. Ouahada, and H. Hamam,“Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence,” Brain Sciences, MDPI, vol. 13, no. 4, p. 683, Apr. 2023. doi: 10.3390/brainsci13040683.

[7] A. Imran and W. Shah, “AI-Powered Cyber Security for IoT: Enhancing Network Resilience and Privacy,” ResearchGate Preprint, Dec. 2023. doi: 10.13140/RG.2.2.35571.03363.

[8] F. Zaheer, “AI-Powered Cybersecurity for IoT Systems: Threat Detection and Privacy Preservation,” International Journal of Advanced Research in Computer Science and Engineering, Dec. 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY