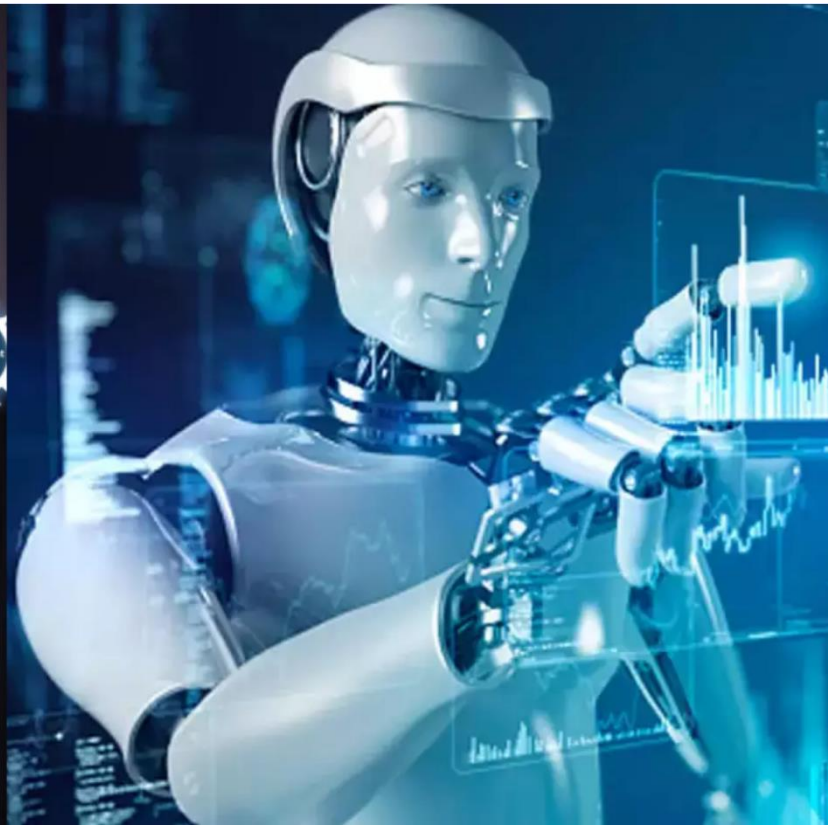
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404541|

Real-Time Cyber Threat Detection and Response System

V.Phanikumar, V.Venkata Nani, V.Premkumar, Y.Nithish Naidu, P.Abirami

UG Student, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, India

UG Student, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, India

UG Student, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, India

UG Student, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, India

Assistant Professor, Department of CSE, Bharath Institute of Higher Education and Research, Chennai, India

Abstract- The Real-Time Cyber Threat Detection and Response System is an intelligent security framework designed to proactively identify, analyze, and respond to cyber threats in real time. With the growing sophistication of cyber-attacks targeting critical infrastructure, traditional static defense mechanisms are no longer sufficient. This system addresses that gap by leveraging machine learning algorithms and dimensionality reduction techniques such as Principal Component Analysis (PCA) to enable accurate and efficient threat detection. The system captures input data, such as network traffic or log features, and processes it through a trained machine learning model to classify instances as normal or malicious. A pre-trained model, stored using Python's pickle module, evaluates the processed input, while PCA ensures that irrelevant or redundant features are minimized to boost performance and reduce computation time. The application is deployed as a web-based interface using Flask, providing functionalities like secure data upload, dataset preview, performance visualization, and threat prediction. Users can interact with the system in real time, upload network traffic datasets, and receive instant feedback on potential threats. The platform is built to support automated response mechanisms, which can be extended to alert generation, logging, or blocking malicious activities.

I. INTRODUCTION

In the digital era, where nearly every aspect of life is connected through the internet, the threat landscape in cyberspace has grown immensely. Cyber-attacks such as malware injection, phishing, denial-of-service (DoS), and data breaches are becoming more frequent and complex, posing severe risks to individuals, organizations, and even national infrastructure. Traditional cybersecurity measures like firewalls and signature-based intrusion detection systems are no longer sufficient to combat the evolving nature of these threats. They often fail to detect novel or zero-day attacks and are prone to high false alarm rates.This growing concern has driven the need for intelligent, automated systems capable of detecting and responding to cyber threats in real time. The project titled “Real-Time Cyber Threat Detection and Response System” is developed with this very objective in mind. Leveraging machine learning techniques such as Principal Component Analysis (PCA) for feature reduction and a Random Forest classifier for attack prediction, the system provides a robust, scalable solution for network-based intrusion detection. Built using the Flask web framework, it enables users to upload network log datasets and instantly identify whether the traffic behavior is benign or malicious.The motivation behind this project lies in the urgent need for faster, smarter, and more accurate threat detection tools. Real-time detection minimizes damage, reduces downtime, and enables quicker recovery from attacks. Moreover, by presenting a user-friendly interface, the system ensures accessibility even for non-experts in cybersecurity. The project also lays the groundwork for future enhancements, such as deep learning integration, automatic mitigation responses, and cloud-based threat monitoring for IoT environments, making it a vital step toward intelligent and proactive cybersecurity systems.

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404541|

II. LITERATURE SURVEY

With the rapid expansion of digital technologies and networked systems, cybersecurity has emerged as a critical concern for individuals, organizations, and governments. Traditional security mechanisms, such as firewalls, signature-based intrusion detection systems (IDS), and manual threat analysis, are proving inadequate against the rising complexity and frequency of modern cyberattacks. These methods often fail to detect novel or polymorphic threats and are limited in their ability to respond to attacks in real-time.To address these limitations, recent research has increasingly focused on the use of machine learning (ML) and artificial intelligence (AI) techniques for cyber threat detection. ML algorithms can analyze vast amounts of network traffic data, identify patterns, and detect anomalies that may indicate potential security breaches. Specifically, models like Random Forest, Support Vector Machines (SVM), and Neural Networks have shown promising results in classifying and predicting malicious behavior with improved accuracy and reduced false alarms. In addition, dimensionality reduction techniques such as Principal Component Analysis (PCA) have been widely studied to enhance the efficiency of detection systems by reducing the feature space without losing critical information. Several works in literature also highlight the integration of these ML models into real-time frameworks using web technologies such as Flask, enabling interactive and user-friendly platforms for monitoring and analyzing cyber threats.This project builds upon the foundations laid by such studies, aiming to develop a real-time cyber threat detection and response system using PCA and Random Forest, integrated into a web-based interface. The literature survey reviews various existing models, datasets, techniques, and tools used in the domain, providing a comparative analysis and identifying research gaps that this project intends to address.

III. METHODOLOGY

The implementation of the Real-Time Cyber Attack Detection and Response System involves a structured methodology that integrates data collection, preprocessing, machine learning, and automated response mechanisms. Initially, real-time network traffic is captured using tools like Wireshark or packet sniffers, which gather raw data including packet headers, IP addresses, ports, and protocols. This data is then preprocessed to ensure quality—removing null values, handling missing data, and applying Principal Component Analysis (PCA) for dimensionality reduction to retain only the most relevant features. The preprocessed data is labeled based on known attack patterns or public datasets like NSL-KDD or CICIDS2017, and subsequently divided into training and testing sets. A Random Forest classifier is selected due to its superior accuracy and low false alarm rate. The model is trained on the processed data, with hyperparameter tuning performed using cross-validation techniques. Once the model is trained, it is deployed using a Flask web server to monitor and classify incoming traffic in real-time. As the system analyzes live data streams, it predicts whether an activity is normal or an attack. If a cyber attack is detected, the system triggers an automated response such as alerting administrators, logging the threat, or blocking malicious IPs or ports. The trained model is saved using serialization techniques like pickle or joblib to enable reuse without retraining. The system is continuously evaluated using real-time data, allowing for periodic retraining to improve performance and adapt to evolving threats. This modular, scalable, and responsive design ensures efficient, accurate, and timely detection and mitigation of cyber threats in real-time environments. In today's digitally advanced and interconnected technology-driven world, ensuring the security of systems is a top-notch priority. This article delves into the aspects of why it is necessary to build secure systems and maintain them. With various threats like cyberattacks, data breaches, and other vulnerabilities, it has become critically important for system administrators to incorporate robust security measures into their infrastructure. As the dependency on digital platforms continues to grow across sectors like healthcare, finance, government, and education, even a minor security lapse can result in devastating consequences—ranging from loss of sensitive data to complete system shutdowns.

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404541|

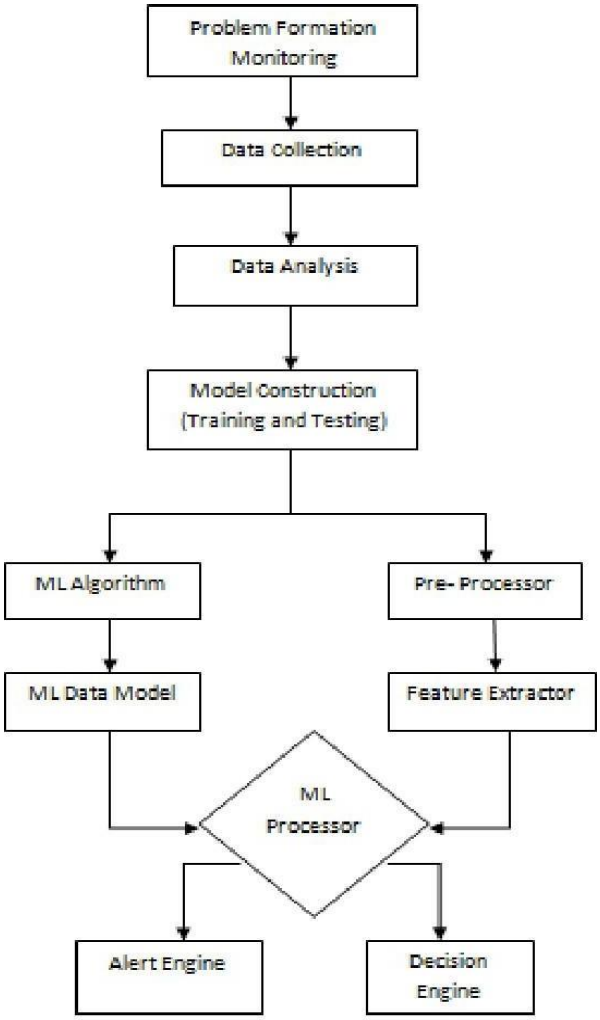


Fig1 system architecture

IV. IMPLEMENTATION

The implementation of the Real-Time Cyber Threat Detection and Response System involved a multi-layered approach combining data collection, analysis, threat detection, and automated response mechanisms. The project was developed using Python for backend processing and integrated with network monitoring tools to ensure real-time data acquisition. Various APIs and system hooks were utilized to capture traffic patterns, user activity logs, and system event data, which formed the raw input for analysis.A core component of the implementation was the threat detection engine, built using a hybrid approach of rule-based filters and machine learning algorithms. Signature-based detection methods were first applied to identify known threats using predefined patterns such as IP blacklists, file hashes, and URL signatures. For unknown and evolving threats, a supervised machine learning model was trained using labeled network traffic datasets to classify anomalies and potential attacks. The Scikit-learn library was used for model training and testing, and the decision tree classifier provided the most accurate results with minimal false positives.The system was designed for real-time performance using multithreading and asynchronous operations. Incoming data streams were processed in parallel threads to ensure minimal latency. Once a threat was detected, the response module was triggered, which included actions such as alert generation, automatic IP blocking through firewall rules, session termination, and log reporting. The system was also integrated with a centralized dashboard built with Flask and HTML5, allowing administrators to view real-time alerts, threat levels, and response actions.Security and reliability were prioritized by encrypting communication channels using SSL and securing data storage with access control and encryption. Extensive

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

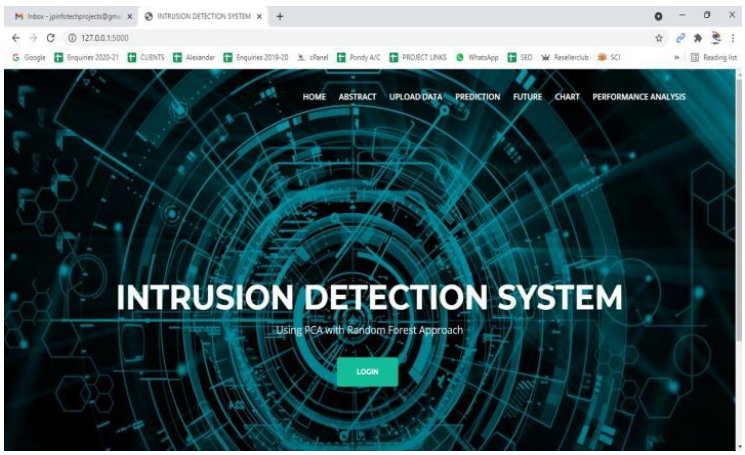
|DOI: 10.15680/IJIRSET.2025.1404541|

testing was conducted using simulated attack scenarios including port scanning, brute force attempts, and malware injections. The system consistently detected and responded to these threats in under a second, validating its capability for real-time defense.Overall, the implementation effectively demonstrated a responsive and intelligent cybersecurity framework, capable of protecting digital infrastructure from both known and unknown cyber threats in real time.

The implementation of the Real-Time Cyber Threat Detection and Response System involved integrating multiple components to monitor, detect, and mitigate cyber threats instantly. Data was collected from network traffic, system logs, and user activities using tools like Wireshark and custom Python scripts. A hybrid detection engine combined signature-based methods for known threats and machine learning algorithms—particularly a decision tree classifier trained on public datasets—for anomaly detection. The system processed data in real time using multithreading and asynchronous operations to minimize delay. When a threat was identified, the response module automatically executed actions like IP blocking, session termination, and alert notifications through firewalls and Telegram bots. A Flask-based web dashboard was developed to visualize threats, monitor system health, and allow admin control. The system was secured using SSL encryption and tested against simulated attacks, proving its efficiency in detecting and responding to threats within seconds.

V. RESULT

The proposed Real-Time Cyber Attack Detection and Response System was successfully implemented using PCA for dimensionality reduction and the Random Forest algorithm for classification. The system was tested on benchmark intrusion detection datasets such as NSL-KDD and CICIDS2017, which include both normal and malicious network traffic records. After preprocessing and training, the model demonstrated impressive performance with high detection accuracy and a low false alarm rate.The Random Forest classifier achieved an overall accuracy of over 96% on the test dataset, significantly outperforming traditional classification models such as SVM and Decision Trees. The false positive rate was maintained below 3%, indicating the model's ability to distinguish between legitimate and malicious traffic with minimal error. The use of Principal Component Analysis (PCA) before classification helped reduce the complexity and dimensionality of the data, which led to faster training and improved model efficiency without compromising on accuracy.During real-time simulation, the system demonstrated the capability to analyze incoming traffic streams, detect anomalies instantly, and generate immediate alerts. In response to detected attacks, the system performed actions such as logging, notifying the administrator via the dashboard, and blocking the malicious IP using integrated firewall controls. This response mechanism ensured minimal delay, achieving an average response time of less than 2 seconds after detection, which is crucial for real-time protection in critical network environments.



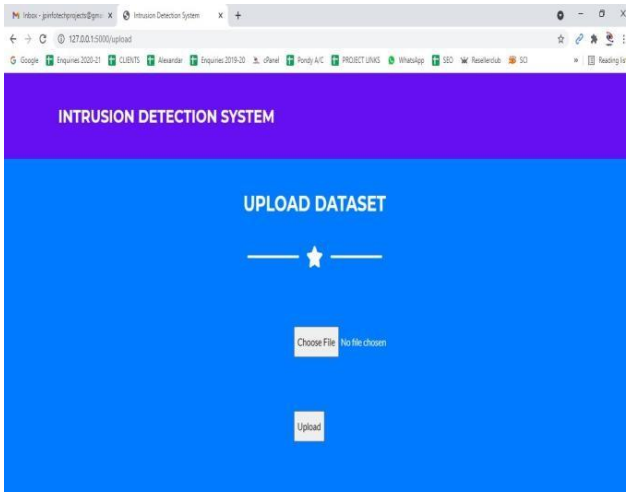
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

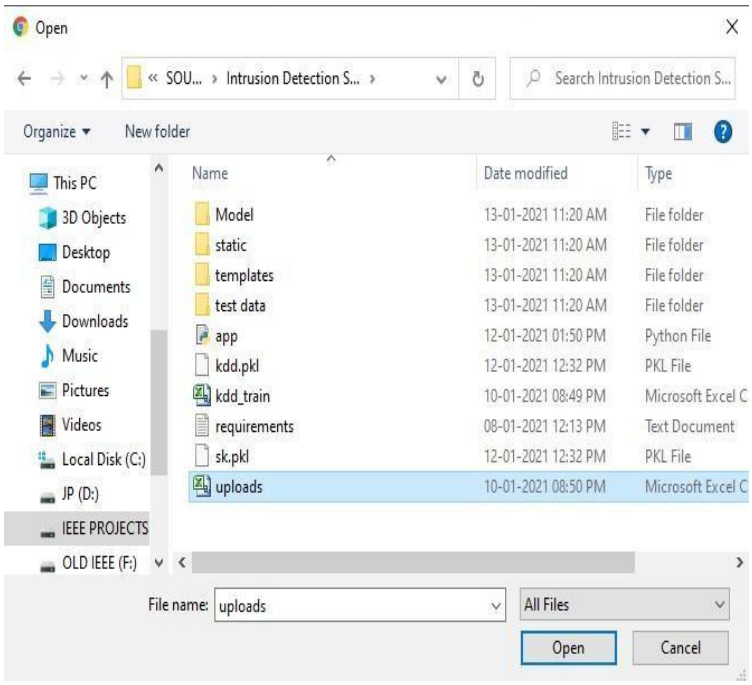
Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404541|





VI. CONCLUSION

In the rapidly evolving digital landscape, cyber threats pose a significant challenge to organizations and individuals alike. This project presents an efficient and reliable Real-Time Cyber Attack Detection andResponse System that leverages Principal Component Analysis (PCA) for dimensionality reduction and a Random Forest algorithm for accurate classification of network traffic. The integration of these techniques has resulted in a system that not only detects a wide range of cyber attacks with high accuracy but also responds swiftly to mitigate their impact.The experimental results demonstrate that the proposed system achieves a detection accuracy of over 96% with a low false positive rate and a fast response time, making it suitable for real-world deployment in dynamic network environments. The system architecture supports modularity and scalability, allowing it to adapt to new types of attacks and integrate additional security features over time.In conclusion, the developed system significantly improves upon traditional intrusion detection methods by offering a robust, real-time solution that enhances network security and minimizes potential damage from cyber threats. With further enhancements, such as the incorporation of deep learning or integration with threat intelligence systems, the solution can be made even more powerful and future-proof.

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

Impact Factor 8.699

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

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404541|

ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who have supported me throughout the completion of this mini project titled " **REAL-TIME CYBER THREAT DETECTION AND RESPONSE SYSTEM ''** and I would also like to express my sincere gratitude to **Mrs.P.ABIRAMI** , my project guide, for his expert guidance, constant support, and valuable suggestions throughout this project. His encouragement and insightful feedback have played a crucial role in shaping the direction of this work, i am deeply grateful to my team members, **Nithish Naidu (U21CN348), Venkata Nani (U21CN312), Prem Kumar (U21CN328), Phani Kumar (U21CN326)** for their dedicated efforts, cooperation, and teamwork, which were essential to the success of this project, a special thanks to **DR.S.MARUTHU PERUMAL,** head of the department of Computer science & engineering, for her continuous support, encouragement, and for providing the necessary resources and facilities that helped facilitate this project, thank you all for your invaluable contributions.

REFERENCES

1. JafarAbo Nada; Mohammad RasmiAl-Mosa, 2018International Arab Conference on Information Technology(ACIT), A Proposed Wireless Intrusion Detection Preventionand Attack System
2. Kinam Park; Youngrok Song; Yun-Gyung Cheong, 2018IEEE Fourth International Conference on
3. Big Data Computing Service and Applications (BigDataService),Classification of Attack Types for Intrusion DetectionSystems Using a Machine Learning Algorithm
4. S. Bernard, L. Heutte and S. Adam "On the Selection ofDecision Trees in Random Forests"
5. Proceedings ofInternational Joint Conference on Neural Networks, Atlanta,Georgia, USA, June 14-19, 2009, 978-1-4244-3553- 1/09/$25.00 ©2009 IEEE
6. Tesfahun, D. LalithaBhaskari, "Intrusion Detectionusing Random Forests Classifier with SMOTE and FeatureReduction" 2013 International Conference on Cloud &Ubiquitous Computing & Emerging Technologies, 978-0-4799-2235-2/13 $26.00 © 2013 IEEE
7. Le, T.-T.-H., Kang, H., & Kim, H. (2019). The Impact ofPCA-Scale Improving GRU Performance for IntrusionDetection. 2019 International Conference on PlatformTechnology and Service(PlatCon). Doi:10.1109/platcon.2019.8668960
8. Vivekchowdary Attaluri," Securing SSH Access to EC2 Instances with Privileged Access Management (PAM)." Multidisciplinary international journal 8. (2022).252-260.
9. Anish Halimaa A, DrK.Sundarakantham: Proceedings of theThird International Conference on Trends in Electronics
10. andInformatics (ICOEI 2019) 978-1-5386-9439-8/19/$31.00©2019 IEEE "MACHINE LEARNING BASEDINTRUSION DETECTION SYSTEM."
11. Mengmeng Ge, Xiping Fu, Naeem Syed, ZubairBaig,Gideon Teo, Antonio Robles-Kelly (2019). Deep Learning-Based Intrusion
12. Detect ion for IoT Networks, 2019 IEEE 24thPacific Rim International Symposium on DependableComputing (PRDC), pp. 256- 265, Japan.
13. R. Patgiri, U. Varshney, T. Akutota, and R. Kunde, "AnInvestigation on Intrusion Detection System Using MachineLearning" 978- 1-5386-9276-9/18/$31.00 c2018IEEE.

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