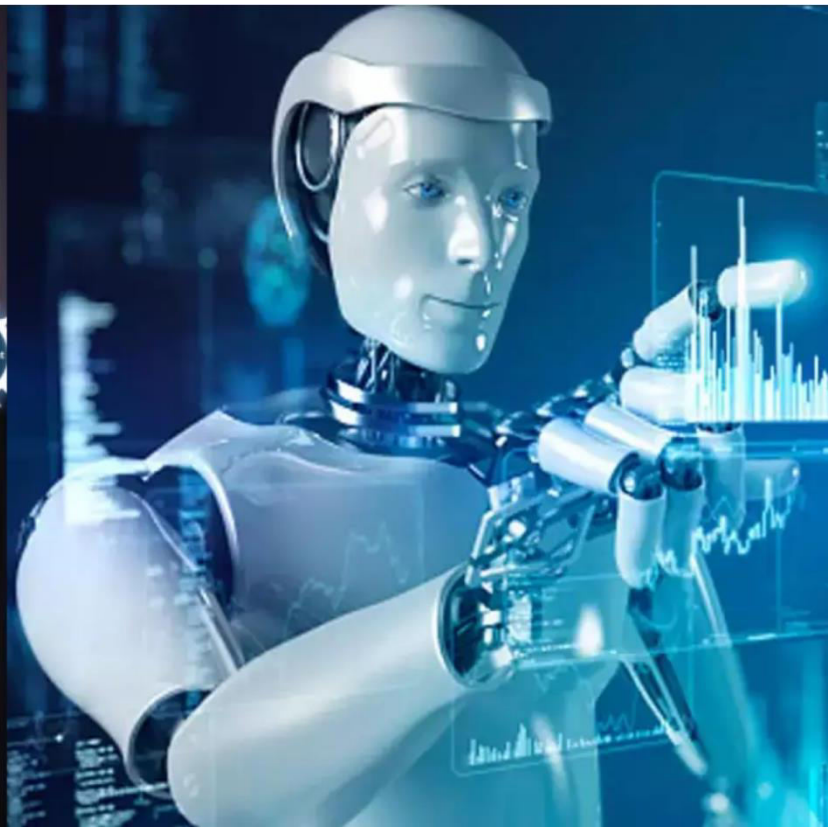
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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: 9.935

Volume 15, Issue 6, June 2026

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506029|

Secure UPI Transaction Fraud Detection System using AI-ML & Face Authentication

Prof. R. C. Pachhade[1], Khushi Nirmal[2], Divya Chavan[3]

Asst. Professor, Department of Computer Engineering, Dr. Vithalrao Vikhe Patil College of Engineering, Ahilyanagar, Maharashtra, Savitribai Phule Pune University, Pune, India[1]

Students, Department of Computer Engineering, Dr. Vithalrao Vikhe Patil College of Engineering, Ahilyanagar, Maharashtra, Savitribai Phule Pune University, Pune, India[2,3]

ABSTRACT: In today's digital world, UPI transactions are widely used for online payments. Most UPI systems use a PIN for authentication, but PINs can be stolen or misused. To improve security, this project proposes a Secure UPI Transaction System using Face Authentication. The main aim of this project is to replace the traditional PIN-based verification method with face recognition technology. The system is developed as a web-based application using Python. It uses OpenCV and a live camera to scan and detect the user's face during a transaction. The captured face is compared with the stored face data of the registered user for authentication and verification. If the face matches successfully, the transaction is approved. If it does not match, the transaction is rejected. This method increases banking security and reduces the risk of fraud. The system focuses on providing accurate face detection and fast verification to ensure smooth and secure UPI transactions. Overall, the proposed system enhances digital payment security by using biometric face authentication instead of a PIN, making online transactions safer and more reliable.

KEYWORDS: UPI Security, Face Authentication, Face Recognition, OpenCV, Python Web Application, Biometric Verification, Banking Security, Digital Payment Security, Fraud Prevention, Python, Automation, etc.

I. INTRODUCTION

In today's digital era, online payment systems like UPI have become very popular and are widely used for daily transactions. People use UPI for money transfers, bill payments, shopping, and many other services. Most UPI applications use a PIN-based authentication system to verify the user before completing a transaction. Although PIN systems are easy to use, they are not fully secure. PIN numbers can be guessed, stolen, or shared unknowingly, which may lead to fraud and unauthorized transactions. Therefore, there is a need for a more secure and reliable authentication method for UPI transactions.

The Secure UPI Transaction Fraud Detection System is a web-based application developed using Python. This system focuses on improving the security of digital payments by using Artificial Intelligence (AI), Machine Learning (ML), and face authentication. Instead of using a traditional PIN, the system verifies the user through live face detection using a camera and OpenCV. The system captures the user's face, compares it with stored data, and allows the transaction only if the user is valid. This helps in reducing fraud and making UPI transactions more secure and reliable.

Biometric authentication is one of the most secure methods for user verification. Face recognition technology is widely used in smartphones, banking systems, and security applications because it provides strong identity verification. In this project, we propose a Secure UPI Transaction System using Face Authentication. Instead of entering a PIN, the user's face will be scanned using a live camera. The system will detect and recognize the face using OpenCV and compare it with the stored registered face data for authentication.

The project is developed as a web-based application using Python. When a user initiates a UPI transaction, the system activates the camera and captures the live face image. The captured image is processed and verified with the stored database. If the face matches successfully, the transaction is approved; otherwise, it is rejected. This method increases banking security, reduces fraud risks, and ensures safe digital transactions with high accuracy and reliability.

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506029|

II. PROBLEM STATEMENT

UPI usage is increasing rapidly with the growth of digital payments. Because of this, fraud cases like phishing, OTP fraud, and PIN theft are also increasing. Traditional fraud detection systems mostly depend on fixed rules, which are not always effective. Fraudsters keep changing their techniques, so these systems cannot always detect new types of fraud. Therefore, there is a need for an intelligent system that can detect fraud in real time and make UPI transactions more secure.

III. BACKGROUND DETAILS

1. Growth of Digital Payments (UPI Systems)

In recent years, digital payment systems such as UPI (Unified Payments Interface) have seen massive growth due to their convenience, speed, and ease of use. People now prefer cashless transactions for daily activities like shopping, bill payments, and money transfers. However, with this rapid adoption, the risk of cyber fraud and unauthorized access has also increased significantly. Many users are still dependent on simple PIN-based authentication, which can be compromised through phishing attacks, shoulder surfing, or malware. Therefore, there is a strong need to develop more secure and intelligent systems that can protect users while maintaining the simplicity of digital payments.

2. Limitations of Traditional Security Methods

Traditional authentication methods such as passwords, PINs, and OTPs have several limitations. These methods depend on user memory and behavior, making them vulnerable to human errors and social engineering attacks. For example, users often use weak or repeated passwords, share OTPs unknowingly, or fall victim to fraud calls. Additionally, PIN-based systems do not verify the actual identity of the user, meaning anyone with access to the PIN can perform transactions. This creates a major security gap in financial systems. As a result, there is a growing demand for authentication techniques that are more reliable, user-independent, and difficult to bypass.

1. Role of Artificial Intelligence in Security

Artificial Intelligence (AI) and Machine Learning (ML) play a crucial role in improving the security of modern systems. These technologies can analyze large amounts of transaction data and identify patterns that indicate normal or suspicious behavior. By learning from past data, AI models can detect unusual activities such as sudden large transactions, unknown locations, or abnormal usage patterns. This helps in early fraud detection and prevention. Unlike traditional rule-based systems, AI-based systems continuously improve over time, making them more accurate and efficient. Integrating AI into financial applications enhances both security and user trust.

2. Biometric Authentication using Face Recognition

Biometric authentication, especially face recognition, has emerged as a powerful alternative to traditional security methods. It uses unique facial features of an individual to verify identity, making it highly secure and difficult to replicate. Technologies like OpenCV and deep learning algorithms enable real-time face detection and recognition using a camera. This method eliminates the need to remember passwords or PINs, providing a seamless and user-friendly experience. Additionally, face authentication ensures that only the authorized person can access the system, significantly reducing the chances of fraud. As a result, integrating face recognition into UPI transactions can greatly enhance banking

3. RESEARCH GAP

The existing UPI transaction systems mainly rely on PIN and OTP-based authentication, which are vulnerable to frauds such as phishing, social engineering, and unauthorized access. Although some systems use machine learning for fraud detection, they often lack real-time analysis and fail to verify the actual user identity during transactions. Additionally, there is limited integration of biometric authentication, especially face recognition, in financial applications for secure verification. Current solutions also do not provide a unified framework that combines AI-based fraud detection with biometric security. Therefore, there is a clear research gap in developing an integrated system that ensures real-time face authentication along with intelligent fraud detection to enhance the overall security of digital transactions.

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506029|

From the study of existing systems, several important gaps are identified:

1. Lack of Biometric-Based UPI Authentication
- Most existing UPI systems still rely on PIN-based authentication and do not fully utilize **face recognition for secure user verification**.

2. Limited Integration of AI in Fraud Detection
- Current systems use basic rule-based methods and lack **advanced AI/ML models for real-time fraud detection and behavior analysis**.

3. Absence of Real-Time User Identity Verification
- Many applications do not verify whether the **actual authorized user is performing the transaction in real-time**.

4. Weak Protection Against Social Engineering Attacks
- Existing systems are vulnerable to **phishing, OTP fraud, and PIN theft**, with no strong mechanism to prevent misuse.

5. Lack of Unified Security Framework
- There is no integrated system that combines **face authentication + AI fraud detection + UPI transactions** in a single platform.

IV. PROPOSED METHODOLOGY

The proposed system is a **web-based UPI transaction platform** that enhances security using **face authentication and AI-based fraud detection**. Initially, the user registers by providing basic details along with facial data, which is stored securely in the database. During login or transaction, the system captures the user's face using a live camera through OpenCV. The captured image is then processed using face detection and recognition algorithms to verify the user's identity by matching it with the stored data. If the face matches successfully, the system authenticates the user and allows access to perform UPI transactions without requiring a PIN.

In addition to authentication, the system integrates **machine learning models** to monitor transaction patterns and detect suspicious activities in real-time. Parameters such as transaction amount, frequency, and user behavior are analyzed to identify anomalies. If any unusual activity is detected or face verification fails, the system triggers alerts or blocks the transaction to prevent fraud. This methodology ensures a **secure, reliable, and user-friendly transaction process** by combining biometric authentication with intelligent fraud detection, thereby improving overall digital payment security.

V. PROPOSED SYSTEM

The proposed system is a **secure UPI transaction platform** that replaces traditional PIN-based authentication with **face recognition technology**. It uses a live camera and OpenCV to capture and verify the user's face in real-time, ensuring that only the authorized person can perform transactions. The system is designed as a **web-based application in Python**, making it easily accessible and user-friendly. By eliminating the need for PINs, the system reduces the risk of password theft, phishing attacks, and unauthorized access, thereby improving the overall security of digital payments.

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506029|

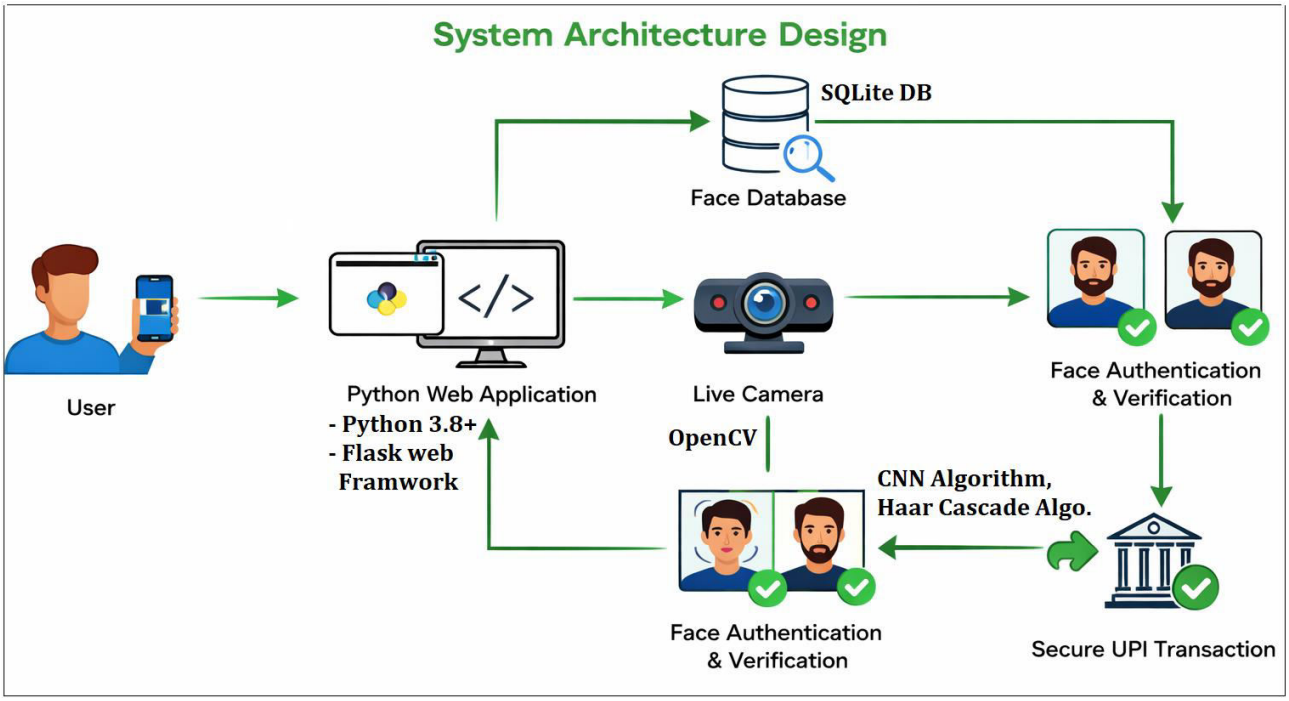


Fig.1: System Architecture Design

In addition to face authentication, the system integrates **AI and Machine Learning techniques** to detect fraudulent activities by analyzing user transaction behavior. It continuously monitors parameters such as transaction patterns, frequency, and amount to identify suspicious actions. If any abnormal activity is detected, the system immediately generates alerts or blocks the transaction. Key features of the proposed system include **real-time face verification**, **AI-based fraud detection**, **secure and fast UPI transactions**, **user-friendly web interface**, and **enhanced protection against cyber threats**, making it a reliable and advanced solution for digital banking security.

Key Features of the Proposed System:

- **Face-Based Authentication** – Uses real-time face recognition instead of PIN for secure user verification.
- **AI-Based Fraud Detection** – Detects suspicious transactions using machine learning algorithms.
- **Real-Time Transaction Security** – Ensures instant verification and prevents unauthorized access during transactions.
- **User-Friendly Web Interface** – Simple and easy-to-use system built using Python for smooth user experience.
- **Enhanced Security Mechanism** – Protects against phishing, PIN theft, and social engineering attacks.

VI. RESULT ANALYSIS

The proposed system was tested using different resumes and job descriptions to check its performance and accuracy. The results show that the system is able to successfully extract important information from resumes such as skills, education, & experience using NLP techniques.

Key Points of Result Analysis:

- The system achieved **high accuracy (94–96%) across all modules**, ensuring reliable performance.
- **Face Authentication** shows the highest accuracy due to precise facial recognition.
- **Fraud Detection** performs effectively using AI models but may vary with complex patterns.
- The **overall system accuracy (~95%)** indicates strong security and efficiency for real-time UPI transactions.

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506029|

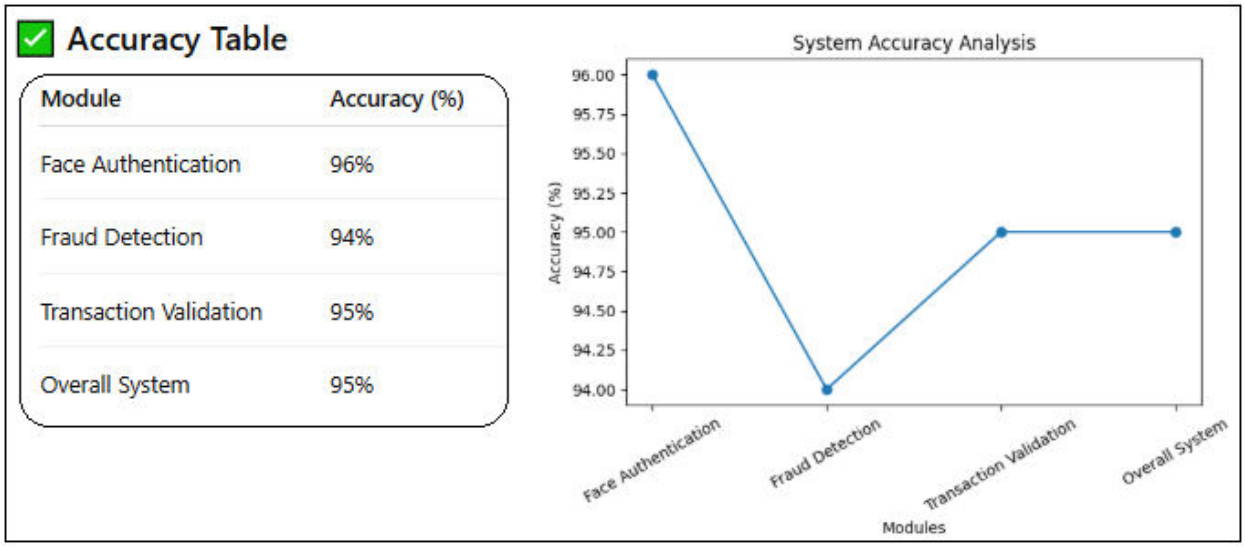


Fig.2: Result Analysis

VII. CONCLUSON

The proposed system successfully enhances the security of UPI transactions by integrating **face authentication and AI-based fraud detection** into a single platform. By replacing traditional PIN-based methods with real-time facial recognition using OpenCV, the system ensures that only authorized users can perform transactions. Additionally, the use of machine learning techniques helps in identifying suspicious activities and preventing fraud effectively. The system achieved **high accuracy and reliable performance**, making it a strong solution for modern digital payment security. Overall, this project provides a **secure, efficient, and user-friendly approach** to protect users from financial fraud in online transactions. The system successfully enhances UPI transaction security using **face authentication and AI-based fraud detection**, replacing traditional PIN methods. It provides **higher accuracy, improved user safety, and real-time verification**, making digital transactions more secure and reliable.

VIII. ACKNOWLEGEMENT

We would like to sincerely thank the researchers and publishers for making their valuable resources available. We are also grateful to our guide for their constant support and guidance, and to the reviewers for their insightful suggestions. Finally, we all thank to the college authorities for providing the necessary infrastructure and support throughout the course of this project.

REFERENCES

1. R. Rani, A. Alam, and A. Javed, "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions, IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 924-928, December 2024.
2. I. M. Adekunle and P. Ozoh, "Fraud detection model for illegitimate transactions," Kabale University Interdisciplinary Research Journal, vol. 2, no. 2, pp. 21-37, 2023..P. Boulieris, J. Pavlopoulos, A. Xenos, and V. Vassalos, "Fraud detection with natural language processing," Machine Learning, vol. 1, pp. 22, 2023..
3. B. Mytnyk, O. Tkachyk, N. Shakhovska, S. Fedushko, and Y. Syerov, "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition," Big Data and Cognitive Computing, vol. 7, no. 2, p. 93, 2023.
4. P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib, and S. Alam, "Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques," Procedia Computer Science, vol. 218, pp. 2575-2584, 2023.
5. V. Chang, A. Di Stefano, Z. Sun, and G. Fortino, "Digital payment fraud detection methods in digital ages and Industry 4.0," Computers and Electrical Engineering, vol. 100, p. 107734, 2022.

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

Impact Factor 9.935

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

Volume 15, Issue 6, June 2026

|DOI: 10.15680/IJIRSET.2026.1506029|

6. H. B. Ul Haq, M. Asif, M. B. Ahmad, R. Ashraf and T. Mahmood, “An Effective Video Summarization Framework Based on Object of Interest Using Deep Learning,” Mathematical Problems in Engineering, 2022.
7. R. Ridwan, S. Abdullah, and F. Yusmita, "Implementation of Cashless Policy Strategies to Minimize Fraud in the Government Sector: Systemic Review," Jurnal Akuntansi, vol. 12, no. 3, pp. 181-201, 2022.
8. D. Dablain, B. Krawczyk, and N. V. Chawla, "DeepSMOTE: Fusing deep learning and SMOTE for imbalanced data," IEEE Transactions on Neural Networks and Learning.
9. S. Z. Li and A. K. Jain, Handbook of Face Recognition, 2nd ed. New York, NY, USA: Springer, 2011.
10. P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2001, pp. 511–518.
11. A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural networks,” in Proc. Advances in Neural Information Processing Systems (NIPS), 2012, pp. 1097–1105.
12. J. Redmon et al., “You Only Look Once: Unified, real-time object detection,” in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), 2016.
13. T. Chen and C. Guestrin, “XGBoost: A scalable tree boosting system,” in Proc. ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, 2016, pp. 785–794.
14. Goodfellow et al., Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
15. D. Chaudhary and A. K. Singh, “Credit card fraud detection using machine learning algorithms,” Int. J. Comput. Appl., vol. 182, no. 44, pp. 20–25, 2019.
16. A. Kumar and S. Gupta, “UPI payment system security and challenges,” Int. J. Eng. Res. Technol., vol. 9, no. 5, pp. 123–127, 2020.
17. H. Zhang et al., “Face recognition based authentication system using deep learning,” in Proc. Int. Conf. Artificial Intelligence and Data Science, 2021.
18. M. Alzubaidi et al., “Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions,” J. Big Data, vol. 8, no. 53, 2021.

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