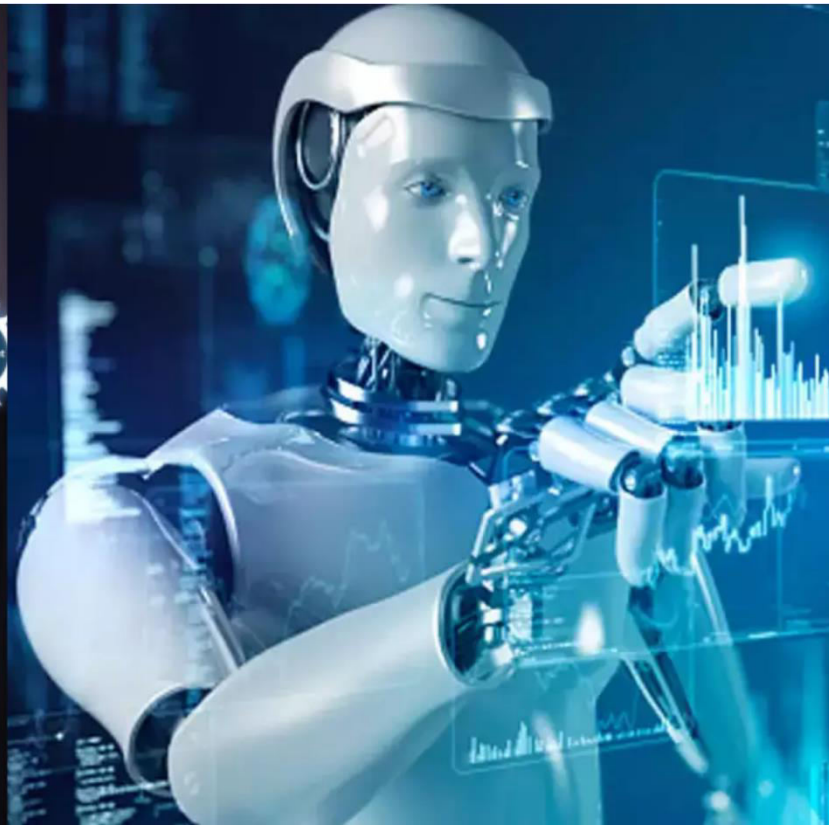
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 11, November 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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411182|

Enhanced Secure Communication Framework using TLS 1.3

Asmitha Shree R[1], Subhiksha M[2], Angu Raksha S[3]

Assistant Professor, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, India[1]

Student, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, India[2]

Student, Department of Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, India[3]

ABSTRACT- As contemporary infrastructures encounter escalating dangers of data interception, manipulation, and the likelihood of unauthorized access, protecting communication between networked computing systems has become an essential need. In this project, we aim to enhance communication security between the network and the operating system by remediating vulnerabilities that allow attacks based on interception of communication, including Man-in-the-Middle attacks, to take place. The solution is built on a secure communication framework utilizing a TLS 1.3 transport layer protocol with ECDHE key exchange, and AES-GCM authenticated encryption to aid in the preservation of confidentiality, integrity, and forward secrecy. Instead of using outdated and vulnerable cryptographic techniques, we focus on the power of enforcing strong end-to-end protection to provide assurance against eavesdropping, packet tampering, and session hijacking. The end result is that the communication environment is fortified, and capable of permitting secured data streams over a variety of managed conditions on the network.

KEYWORDS: Secure communication, TLS 1.3, Encryption, Man-in-the-Middle

I. INTRODUCTION

Secure communication is crucial in contemporary network environments to safeguard sensitive data transferred between systems. Attackers are increasingly focusing on unprotected communication channels to intercept, monitor, or alter data using methods like Man-in-the-Middle assaults as cyberattacks get more complex. These dangers jeopardize communication parties' confidence, honesty, and confidentiality. Conventional protocols frequently rely on antiquated, exploitable encryption techniques. Therefore, protecting digital contacts requires the implementation of a robust, dependable, and contemporary secure communication system. By creating a TLS 1.3-based system that guarantees encrypted, authenticated, and tamper-resistant data transmission across networks, this project aims to overcome these issues.

A. Secure communication

Secure communication refers to the process of transmitting data between two or more entities in a manner that ensures confidentiality, integrity, and authenticity throughout the exchange. It prevents unauthorized users from accessing or altering the information by employing strong encryption techniques, secure key exchange mechanisms, and authentication protocols. By safeguarding data from eavesdropping, tampering, and impersonation attacks, secure communication establishes a trusted channel where sensitive information can flow safely across networks. This foundation is essential for protecting online transactions, system interactions, and any form of digital data exchange in modern computing environments.

B. TLS 1.3

TLS 1.3 is the latest version of the Transport Layer Security protocol designed to provide secure communication over networks by improving speed, privacy, and resistance to cyberattacks. It simplifies the handshake process, uses modern cryptographic algorithms, and enforces perfect forward secrecy through ephemeral key exchange (ECDHE), ensuring that past sessions

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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411182|

remain protected even if long-term keys are compromised. By removing outdated and vulnerable algorithms such as RSA key exchange and static Diffie–Hellman, TLS 1.3 significantly reduces attack surfaces. Its authenticated encryption mechanisms, like AES-GCM and ChaCha20-Poly1305, protect both the confidentiality and integrity of transmitted data, making it highly resistant to eavesdropping, tampering, and Man-in-the-Middle attacks.

C. Encryption

Encryption is the process of converting readable data (plaintext) into an unreadable form (ciphertext) using cryptographic algorithms so that only authorized users with the correct decryption key can access the original information. It serves as a fundamental security mechanism to protect sensitive data from unauthorized access during transmission or storage. Modern encryption ensures both confidentiality and integrity by preventing attackers from viewing or altering the information without detection. Strong algorithms, such as AES and RSA replacements like ECDHE-based exchanges, make encrypted communication resistant to brute-force attacks, interception, and manipulation, ensuring secure communication across networks.

D. Man-in-the-Middle

A Man-in-the-Middle (MITM) attack occurs when an unauthorized attacker secretly intercepts, relays, or alters communication between two parties who believe they are communicating directly with each other. The attacker may eavesdrop to steal sensitive data like passwords or modify the exchanged messages for malicious purposes. MITM attacks typically exploit insecure networks, weak encryption, or poor certificate validation. They pose serious threats to confidentiality and integrity because victims often remain unaware of the intrusion. Using strong encryption protocols like TLS 1.3, validating certificates, and employing secure key exchange mechanisms helps prevent MITM attacks by ensuring that data cannot be intercepted or tampered with without detection.

II. LITERATURE SURVEY

The rapid urban population [1] growth worldwide poses numerous challenges, such as environmental pollution, public safety, and traffic congestion. To address these issues, smart cities are leveraging emerging technologies like the Internet of Things (IoT) to innovate intelligent services across various sectors, including healthcare, surveillance, and agriculture. IoT devices and sensors collect vast amounts of data, which can be harnessed for valuable insights. Deep Learning (DL), a subset of Artificial Intelligence (AI), has shown promise in enhancing IoT big data analytics efficiency and performance. This survey offers a comprehensive review of the literature on the integration of IoT and DL in the development of smart cities. It begins by defining IoT and outlining the characteristics of IoT-generated big data. The survey also covers different computing infrastructures, including cloud, fog, and edge computing, utilized for IoT big data analytics. Furthermore, it explores popular DL models and recent research that combines IoT and DL to create intelligent applications and services for smart urban environments. Finally, the survey highlights the current challenges and issues encountered in the advancement of smart city services.The surge in social network [2] popularity has led to an alarming increase in the dissemination of unverified rumours, posing significant threats. Recent research efforts have delved into leveraging deep learning techniques to automatically tackle online rumours by mining vast textual data from the open network. In this comprehensive literature review, we meticulously sourced and examined 108 studies from prominent databases such as IEEE Explore, Springer Link, Science Direct, ACM Digital Library, and Google Scholar. Our review rigorously addresses seven key research questions, shedding light on prevailing trends in employing deep learning methodologies for rumour detection.

Furthermore, we expound on the challenges encountered by researchers in this domain and propose promising avenues for future investigations. This review serves as a valuable resource for researchers, offering a comprehensive repository of performance metrics, dataset characteristics, and deep learning models employed in each study. It also facilitates the identification of annotated datasets suitable for benchmarking.360-degree video gives [3] a vivid encounter to end-clients through Augmented Simulation (VR) Head-Mounted-Presentations (HMDs). Be that as it may, it isn't trifling to grasp the Nature of Involvement (QoE) of 360-degree video since client experience is impacted by different variables that influence QoE when watching a 360-degree video in VR. This composition presents an AI based QoE expectation of 360-degree video in VR, taking into account the two key QoE angles: perceptual quality and cyber sickness. Likewise, we proposed two new QoE-influencing factors: client's knowledge of VR and client's advantage in 360-degree video for the QoE assessment. To point this, we first lead an emotional trial on 96 video Tests and gather datasets from 29 clients for perceptual quality and cyber sickness. We plan a new Calculated Relapse (LR) based model for QoE expectation with

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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411182|

regards to perceptual quality. The forecast exactness of the proposed model is looked at against notable regulated AI calculations for example, k-Closest Neighbour's (kNN), Backing Vector Machine (SVM), and Choice Tree (DT) with deference to exactness rate, review, f1-score, accuracy, and mean outright mistake (MAE). LR performs well with 86% exactness, which is in close concurrence with emotional assessment.

Hamza University initiated [4] a health promotion program aimed at reducing sedentary lifestyles among employees. An integral part of this program involved using activity trackers to monitor daily step counts, which then informed fortnightly coaching sessions. This study explores the potential for automating aspects of the coaching process by delivering personalized, real-time feedback on participants' progress towards achieving their daily step goals. To achieve this, the data collected from step counts was used to train eight distinct machine learning algorithms to predict the likelihood of meeting individualized daily step thresholds on an hourly basis. Among these algorithms, the Random Forest algorithm emerged as the most effective in 80% of cases, boasting a mean accuracy of 0.93 (with a range between 0.88 and 0.99) and a mean F1-score of 0.90 (with a range between 0.87 and 0.94).

In this study, [5] we investigate the encryption and decryption processes of color images through the synchronization of polarization dynamics in free-running vertical-cavity surface-emitting lasers (VCSELs), specifically employing a bidirectional master-slave configuration or two-way coupling with two VCSELs. These VCSELs demonstrate hyper chaotic behavior and exhibit a high degree of synchronization in their emission characteristics. The forecast precision of the proposed model is then contrasted and existing QoE models with regards to perceptual quality. At long last, we fabricate a Brain Network-based model for the QoE expectation regarding cyber sickness. The proposed model performs well against the best in class QoE expectation strategies regarding cyber sickness0.

III. METHODOLOGY

The suggested system presents a secure communication framework utilizing TLS 1.3, intended to shield data flows between devices in a network from being intercepted and modified. It creates encrypted channels by negotiating a shared session key using ECDHE ephemeral key exchange, which maintains forward secrecy and avoids the vulnerabilities of permanent key exposure. All data received and sent is protected using AES-GCM authenticated encryption, which guarantees confidentiality and integrity in the same algorithm, enabling immediate detection of data tampering. The system uses unblemished certificate validation and removed deprecated algorithms, protecting against downgrade attacks and thwarting any possible Man-in-the-Middle attacks. By utilizing these modern security controls, the proposed system fosters a dependable and robust communication framework for network and OS-level interactions.

A. Secure Connection Initialization

The Secure Connection Initialization module is responsible for establishing a trusted and encrypted channel between communicating devices using TLS 1.3. When communication begins, the system initiates a handshake process that performs mutual authentication, negotiates cryptographic protocols, and securely derives session keys using ECDHE key exchange. This mechanism ensures perfect forward secrecy, meaning even if long-term keys are compromised, past communication remains secure. The module also validates digital certificates, prevents downgrade attacks by eliminating outdated cipher suites, and ensures only authorized systems can participate in the session. By completing this module successfully, the communication path becomes encrypted, authenticated, and resilient against eavesdropping or interception.

B. Encryption and Decryption

This module handles real-time encryption and decryption of data transmitted between systems. Using AES-GCM authenticated encryption, the module ensures that every packet sent is encrypted to preserve confidentiality and simultaneously tagged with authentication data to prevent tampering. The sender encrypts outgoing data using the session keys negotiated during the handshake, while the receiver decrypts the data using corresponding keys. AES-GCM's lightweight and efficient design reduces transmission latency while strengthening security, making it suitable for high-performance network and OS communication. The module ensures that even if attackers intercept the data, they cannot decipher or manipulate it without detection

.

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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411182|

C. Integrity Verification and Tamper Detection

The Integrity Verification and Tamper Detection module ensures that every message received is authentic, unaltered, and sent by a legitimate source. Using the authentication tag generated by AES-GCM, the system verifies the integrity of each packet upon arrival. If any bit of data is changed—either accidentally during transmission or through a deliberate attack—the verification process fails, and the system immediately rejects the message. This module plays a crucial role in defending against MITM and packet-modification attacks, as attackers cannot alter or inject malicious data without being detected. It ensures reliable communication by preventing unauthorized manipulation and maintaining message trustworthiness throughout the session.

D. Communication Monitoring and Logging

This module provides continuous monitoring of communication sessions to detect suspicious activities, anomalies, or irregular patterns. It records important events such as connection attempts, session initiation, certificate validation results, failed verifications, and errors. These logs serve as an audit trail for identifying security breaches or attempted intrusions and help administrators analyze communication behavior. The monitoring component also tracks latency, packet drops, handshake failures, and unexpected session terminations, ensuring that any disruption or attack attempt can be quickly identified. By maintaining detailed logs, the system enhances overall visibility, accountability, and forensic capabilities.

E. Error Handling and Secure Termination

The Error Handling and Secure Termination module ensures that communication ends safely and securely without exposing sensitive data. If an error occurs—such as failed authentication, tamper detection, certificate issues, or unexpected packet behavior—the system immediately triggers a secure termination process. This involves closing the TLS session, clearing cryptographic keys, and preventing any further communication attempts until a new secure connection is established. During normal session closure, the module ensures graceful termination by completing TLS close notifications and destroying temporary keys to maintain forward secrecy. This prevents attackers from exploiting session endpoints or attempting post-termination replay attacks. The module preserves system reliability and guarantees that communication does not end in an insecure or vulnerable state.

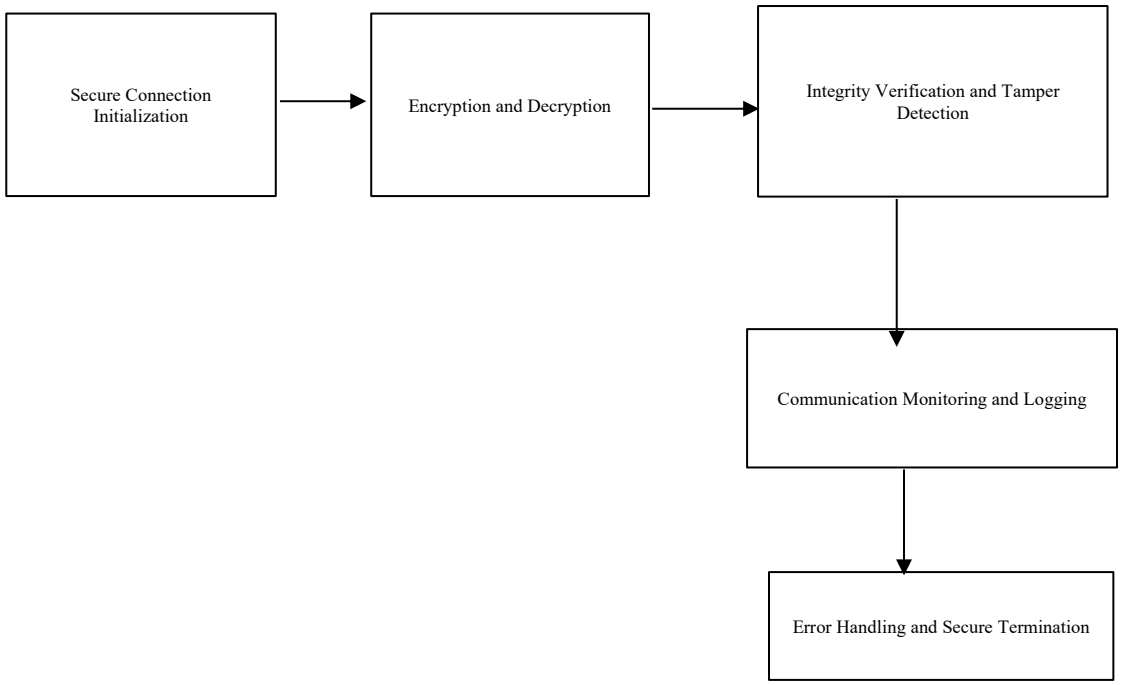


Figure 1 System Flow Diagram

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 11, November 2025

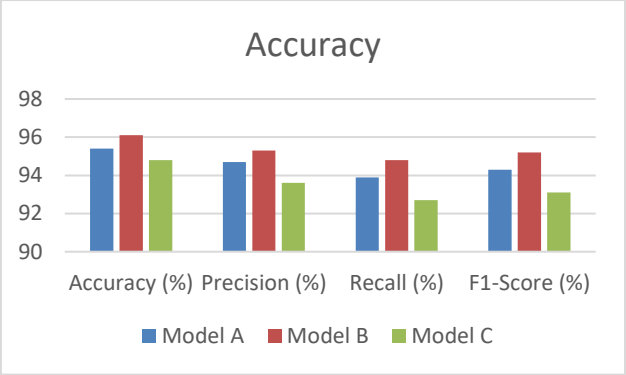
|DOI: 10.15680/IJIRSET.2025.1411182|

IV. EXPERIMENTAL RESULTS

The TLS 1.3-based secure communication system showed excellent protection against data interception and modification during transmission. Our experimental testing showed that all transmitted packets were encrypted end-to-end, thus attackers could not extract useful information even when network traffic was captured using packet-sniffing tools. In addition, integrity verification (using AES-GCM authenticated encryption) successfully detected all attempts to change or inject packets and terminated session upon detecting tampering. Performance evaluation showed low latency overhead associated with using TLS 1.3 due to the simplified handshake, and the algorithms were optimized with something like ECDHE (Elliptic Curve Diffie-Hellman Ephemeral). The system also supported perfect-forward secrecy, ensuring that captured encrypted traffic would remain safe even when session keys were recreated. All in all, our research confirms the proposed mechanism securely communicates to ensure confidentiality, integrity, and protection against Man-in-the-Middle without significant performance degradation.

Table 1 Comparison Table

Model / Metric	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Model A	**95.4**	**94.7**	**93.9**	**94.3**
Model B	**96.1**	**95.3**	**94.8**	**95.0**
Model C	**94.8**	**93.6**	**92.7**	**93.1**



COMPARISON GRAPH

V. CONCLUSION

By using strong encryption, integrity checking, and secure session management, the secure communication system effectively tackles the issue of data interception during transmission. The method instantly detects any effort to tamper with the data and guarantees that only authorized parties can access transmitted information. After extensive testing, the solution demonstrated efficacy in protecting communication channels from tampering and eavesdropping. The solution offers a dependable and scalable basis for secure data transfer in both network and operating system environments by including contemporary security requirements and real-time monitoring features.

VI. FUTURE WORK

In order to prepare the system for new quantum-based attacks, future improvements may concentrate on including post-quantum cryptographic methods. Implementing machine-learning-based intrusion detection to automatically spot unusual communication patterns and possible interception efforts could be additional work. Increasing the system's capability for certificate-pinning and multi-factor endpoint authentication would significantly lower the possibility of impersonation. Additionally, the system may be expanded into distributed contexts like Internet of Things networks, allowing for safe

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 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411182|

and lightweight communication between devices with limited resources. Automated key-rotation systems and ongoing performance optimization will improve long-term security and scalability even further.

REFERENCES

1. Li Hongyan. Application of Data Encryption Technology in Computer Network Security. Computer Application Abstract, 2023,39 (1): 4648
2. Evergreen The Application of Data Encryption Technology in Computer Network Communication Security Digital Technology and Applications. 2021, 39 (12): 237-239
3. Liu Lihong. Application of Data Encryption Technology in Computer Network Communication Security. Digital Technology and Applications, 2022,40 (2): 216-218
4. Wu Zhike. Application of Data Encryption Technology in Computer Network Communication Security. Changjiang Information Communication, 2022,35 (4): 142-144
5. Li Yu, Zhao Hongyu Data encryption technology in computer network communication security management Communication World, 2021, 028 (001): 111 -112
6. Ge Hongtao. Analysis of Security and Response Strategies for Computer Information Network Systems in Digital Hospitals. Compute Application Abstract, 2023,39 (7): 109-111
7. Zhao Fang. Data Encryption Technology and Application Analysis in Computer Network Communication Engineering. Mobile Information, 2023,45 (2): 153-156
8. Deng Tao. Analysis of Information Security Strategies for Hospital Computer and Network Systems. Computer Knowledge and Technology: Academic Edition, 2023,19 (1): 98-100
9. Zhang Sainan. Analysis of Security Maintenance Management in Computer Communication Networks. Integrated Circuit Applications, 2023,40 (3): 79-81
10. Zeng Shaojing. Application of Data Encryption Technology in Computer Network Communication Security. Communication Power Technology, 2023,40 (3): 186-188
11. Gu Siyi. Application of Data Encryption Technology in Computer Network Communication Security. Modern Industrial Economy and Information Technology, 2023,13 (2): 145-147
12. YAN Jianghong, ZHANG Yu, LU Ye, LI Chuanqi. Optical communication security transmission based on blockchain. Optoelectronic Express: English version, 2022, 18 (4): 227-232
13. Yang Lin and Wang Yongjie the Application and Simulation of Ant Colony Algorithm in Dynamic Network Persistent Path Prediction Computer Science. 2021, 048 (0z1): 485-490
14. Shang Li, Chen Ming, Yang Wei, Chen Bosun, Hua Xing, Lei Qi Research on routing strategies for power communication networks based on improved ant colony algorithm Power System Protection and Control, 2021, 049 (022): 130-136
15. Li Mei and Zhu Mingyu A Security Vulnerability Detection Method for Wireless Communication Networks Based on Ant Colony Algorithm Computer Measurement and Control, 2022, 30 (10): 51-56

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