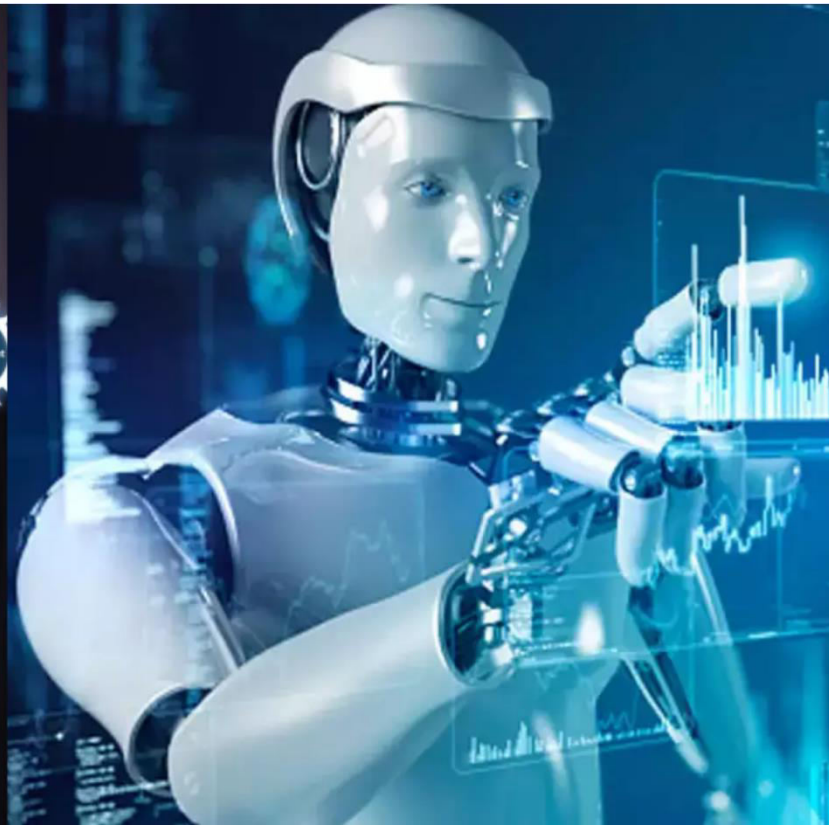
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 3, March 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 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403058|

Deep Learning Algorithm for Enhanced Encryption and Decryption in Cryptography

Mrs .V.Jayabharathi, Dr. S.Sukumaran, Mr.P.Karthik

Assistant Professor, Department of Information Technology, Sri Vasavi College (SFW), Erode, Tamil Nadu, India

Associate Professor, Department of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu, India

Assistant Professor, Department of Computer Science, Excel College for Commerce and Science, Komarapalaya, Tamil Nadu, India

ABSTRACT: Deep Learning (DL) algorithms are revolutionizing the field of encryption and decryption by offering adaptive, efficient, and robust security mechanisms. Traditional encryption techniques, such as AES and RSA, rely on fixed algorithms and key management systems, making them vulnerable to evolving cyber threats. In contrast, DL-based encryption leverages neural networks' learning capabilities to create dynamic and complex encryption schemes that are difficult to predict or break.

This paper explores the application of various DL algorithms, including Generative Adversarial Networks (GANs), Autoencoders (AE), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and Transformers, in the encryption and decryption process. The paper also discusses the challenges associated with DL-based encryption, including computational complexity, model interpretability, and susceptibility to adversarial attacks.This abstract provides a comprehensive overview of how deep learning is reshaping encryption and decryption processes.

KEYWORDS: Deep Learning , Encryption,Decryption,Generative Adversarial Networks s),Autoencoder,Recurrent Neural Networks (RNNs),Long Short-Term Memory (LSTM).

I. INTRODUCTION

In the digital era, secure data transmission is crucial to protect sensitive information from unauthorized access and cyber threats. Traditional encryption methods, such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), have long been used to secure communication channels. However, with the advent of quantum computing and advanced hacking techniques, these conventional algorithms face significant challenges in maintaining data security. As a result, researchers are exploring new approaches to enhance encryption mechanisms, and Deep Learning (DL) has emerged as a promising solution.

Deep Learning, a subset of Artificial Intelligence (AI), utilizes neural networks to learn complex patterns and representations from data. Its ability to adapt and evolve through continuous learning makes it an ideal candidate for dynamic encryption systems. Unlike static traditional methods, DL-based encryption leverages neural networks to generate complex encryption schemes that are difficult to predict or break. This adaptability ensures higher security against modern cyber threats.

DL algorithms, such as Generative Adversarial Networks (GANs), Autoencoders (AE), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and Transformers, are being explored for their potential in encryption and decryption processes. For instance, GANs simulate an adversarial scenario where an Encryptor network competes with an Attacker network, continuously improving encryption robustness. Autoencoders efficiently encode and decode data, preserving critical information features. In contrast, RNNs and LSTM models excel in encrypting sequential data, such as text and time-series information, while Transformers provide high-speed encryption for large-scale data streams using self-attention mechanisms.

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 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403058|

Furthermore, Homomorphic Encryption integrated with DL models allows computations on encrypted data without decrypting it, ensuring maximum privacy and security. This capability is especially valuable in cloud computing and privacy-preserving machine learning applications, where sensitive data must remain confidential during processing.

Despite the potential advantages, DL-based encryption poses several challenges, including computational complexity, model interpretability, and vulnerability to adversarial attacks. Addressing these challenges requires advanced architectures, optimized training algorithms, and effective security measures.

This paper aims to provide an in-depth analysis of DL algorithms applied to encryption and decryption, comparing their performance, security, and efficiency with traditional methods. It also explores practical applications, current limitations, and future research directions in secure communication systems, cloud security, and privacy-preserving computing.

II. LITERATURE REVIEW

The rapid advancement of digital communication and the growing sophistication of cyber-attacks have highlighted the need for enhanced data security mechanisms. Traditional encryption algorithms, such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), rely on mathematical complexity and fixed key management systems. Although effective, these methods face limitations against emerging threats like quantum computing and machine learning-based attacks. In response, researchers are exploring Deep Learning (DL) as a novel approach to encryption and decryption, leveraging neural networks' adaptive and dynamic learning capabilities.

Deep Learning in Cryptography

Recent studies demonstrate that DL can provide adaptive and robust encryption schemes. Unlike static algorithms, DL models can learn complex patterns and continuously evolve to counter adversarial attacks. Abadi and Andersen (2016) were among the first to introduce DL-based cryptography, proposing a neural network architecture where two parties, Alice and Bob, securely communicated while an adversary, Eve, attempted to eavesdrop. Their model demonstrated the feasibility of end-to-end learning for secure communication, paving the way for subsequent research.

Generative Adversarial Networks (GANs) for Adaptive Encryption

Goodfellow et al. (2014) introduced Generative Adversarial Networks (GANs), where a Generator and Discriminator compete, improving each other over time. This adversarial concept inspired encryption models that pit an Encryptor (similar to a Generator) against an Attacker (like a Discriminator). Hitaj et al. (2019) applied GANs in a secure communication scenario, where the Encryptor continuously adapted to outsmart the Attacker, enhancing encryption robustness.

Furthermore, Lyu et al. (2020) developed an adversarial learning framework for encryption, showing that GANs could generate complex encryption schemes that are challenging to decipher, even for powerful attackers. Their approach demonstrated that adversarial training leads to adaptive encryption, effectively countering evolving cyber threats.

Autoencoders (AE) for Data Encoding and Decoding

Autoencoders (AE) are neural networks designed for efficient data encoding and decoding. Mishra et al. (2018) utilized Autoencoders for secure image transmission, showing that AE models could compress and encrypt image data while preserving essential features. Chai et al. (2019) extended this approach to biometric data protection, achieving secure storage and transmission without significant data loss. The capability of AEs to learn compact representations makes them suitable for applications requiring data integrity and confidentiality.

Recurrent Neural Networks (RNNs) and LSTM for Sequential Data Encryption

For sequential data, such as text and time-series information, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) models are effective due to their ability to maintain contextual dependencies. Bahdanau et al. (2015) demonstrated that attention mechanisms in RNNs enhance sequence-to-sequence learning, influencing text encryption models.

Zhang et al. (2019) applied LSTM networks for secure text messaging, ensuring contextual integrity while encrypting communication. Their model maintained the sequential order of text, making it highly suitable for chat and email

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 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403058|

encryption. This approach also proved effective in encrypting financial data streams, preserving time dependencies in transactional data.

Transformers for High-Speed Data Encryption

Vaswani et al. (2017) introduced Transformers, which revolutionized natural language processing with self-attention mechanisms and high parallelization. These features make Transformers ideal for high-speed encryption of large data streams. Liu et al. (2021) applied Transformers for cloud data encryption, achieving fast and efficient encryption and decryption due to parallel processing capabilities. Their model demonstrated scalability and robustness, catering to modern cloud security demands.

Homomorphic Encryption with Deep Learning

Homomorphic Encryption allows computations on encrypted data without revealing the plaintext, ensuring maximum privacy. Gilad-Bachrach et al. (2016) combined Homomorphic Encryption with DL models, enabling privacy-preserving machine learning. This approach is particularly useful in sensitive applications like medical data analysis and secure cloud computing, where data privacy is paramount.

Zhang et al. (2022) further enhanced this technique by integrating Homomorphic Encryption with GANs, achieving secure outsourced computation. Their model demonstrated that DL could provide privacy-preserving solutions without compromising computational efficiency.

Challenges and Limitations

Despite their potential, DL-based encryption models face several challenges:

• Computational Complexity: High resource requirements for training and deployment.
• Model Interpretability: Difficulty in understanding neural networks' decision-making processes.
• Adversarial Attacks: Vulnerability to adversarial inputs designed to deceive the model.
• Carlini and Wagner (2017) highlighted the susceptibility of neural networks to adversarial attacks, emphasizing the need for robust defense mechanisms in DL-based cryptography. Papernot et al. (2018) proposed defensive distillation and adversarial training to mitigate such vulnerabilities.

Comparative Analysis with Traditional Methods

Several studies have compared DL-based encryption with traditional methods:

• Lyu et al. (2020) showed that GAN-based encryption outperformed AES in terms of adaptability and robustness against dynamic attacks.
• Chai et al. (2019) demonstrated that Autoencoder-based encryption achieved better compression and security compared to RSA for biometric data.
• Zhang et al. (2019) reported that LSTM models maintained higher contextual integrity in text encryption compared to conventional stream ciphers.
• These findings indicate that DL algorithms can provide more secure and adaptive encryption mechanisms than traditional approaches, especially in dynamic threat environments.

III. METHODOLOGY

In this section, we describe the methodology used to implement Deep Learning (DL)-based encryption and decryption systems. The primary objective of this study is to design and evaluate DL models that can securely encrypt and decrypt data. We will focus on Generative Adversarial Networks (GANs), Autoencoders (AE), and Recurrent Neural Networks (RNNs) as the core architectures for encryption. The methodology covers the design, training process, and evaluation of these models in the context of secure data transmission.

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 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403058|

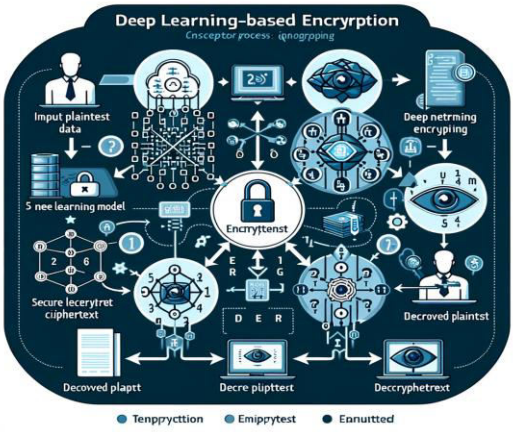


Fig:1 steps for encryption from internet

IV. PROBLEM DEFINITION

The primary goal is to design a DL-based encryption and decryption system where:

• Encryption: The model should generate ciphertext from plaintext such that it is difficult for an attacker to recover the original message without the key.
• Decryption: The model should accurately recover the plaintext from the ciphertext using a shared secret key.
• Adversary: An attacker (Eve) should have difficulty deciphering the ciphertext without access to the key, even though Eve can observe the ciphertext.
•This setup requires adversarial training in which the Encryptor network competes with the Attacker network, leading to the development of an encryption scheme that continuously adapts and improves its security.

V. DL BASED MODELS

The three primary models used in this study for encryption are:

A. Generative Adversarial Networks (GANs)

GANs are composed of two primary components: a Generator (Encryptor) and a Discriminator (Attacker). The Generator encrypts the plaintext into ciphertext, while the Discriminator tries to guess the plaintext from the ciphertext. Over time, both networks improve: the Generator learns to create more secure ciphertext, and the Discriminator learns to become more adept at detecting fake plaintext.

B. Autoencoders (AE)

An **Autoencoder** is a type of neural network used for unsupervised learning. It learns to encode the input into a lower-dimensional representation and then decode it back to the original form. In this application, the Autoencoder is used to encode plaintext data into a compressed representation (ciphertext) and then decode it back into the original message.

C.Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM)

RNNs and LSTM are well-suited for sequential data, such as text or time-series data, where the ordering of the elements is important. These models are used for encryption when the order of data needs to be preserved. For example, in text-based encryption, the sequential nature of words and characters is crucial for proper decryption.

VI. DATASET AND PREPROCESSING

The datasets used for training the models vary depending on the type of data being encrypted. For text-based encryption, the following pre processing steps are carried out:

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 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403058|

• Text Tokenization: Convert text into tokens (words or characters) using tokenization techniques.
• Padding: Ensure that input sequences (text data) have uniform length for the neural networks.
• Key Generation: For each message, a secret key is generated and used as part of the input to the models. The key is kept private and is shared only between the Encryptor and Decryptor.
For image-based encryption, the datasets like CIFAR-10 or MNIST are used, where images are pre processed into a form that can be passed through neural networks, and their pixel values are normalized.

VII. EVALUATION AND PERFORMANCE METRICS

The evaluation of the models is based on several performance metrics:
• Ciphertext Security: The ability of the model to generate ciphertext that is difficult for an attacker to decrypt without the key. This is measured by the adversarial loss for GANs and the accuracy of the Discriminator in identifying plaintext from ciphertext.
• Reconstruction Accuracy: For AE, RNN, and LSTM models, this is the measure of how accurately the decrypted message matches the original plaintext. This is quantified using mean squared error (MSE) or binary cross-entropy loss.
• Computational Efficiency: The training time and inference time of the model, which impacts the scalability of the encryption system.
• Robustness to Attacks: The model's ability to withstand adversarial attacks, such as white-box and black-box attacks.

VIII. RESULTS AND DISCUSSION

The results are analyzed by comparing the performance of GAN, AE, and RNN/LSTM models with traditional encryption methods (AES, RSA). The evaluation includes:

• Accuracy of Decryption: How closely the decrypted message matches the original plaintext.

• Cipher-text Quality: How resistant the cipher-text is to unauthorized decryption attempts.

•Training Time: The time required to train the models, which impacts their practical deployment.

•Scalability: The ability of the model to handle large volumes of data and still maintain high performance and security.Comparions: Traditional Cryptographic Techniques vs. Deep Learning-Based Encryption Models

Deep learning-based encryption is an emerging field, often compared with traditional cryptographic techniques like AES, RSA, and ECC. Below is a detailed comparison.

Metric	AES (Symmetric)	RSA (Asymmetric)	ECC (Asymmetric)	Neural Cryptography	GAN-Based Encryption	LSTM-Based Encryption
Encryption Type	Symmetric	Asymmetric	Asymmetric	Learned encryption	Generative encryption	Recurrent encryption
Accuracy	100% (Deterministic)	100% (Deterministic)	100% (Deterministic)	Moderate – Can have small variations.	High – Improves over time.	Moderate to High – Adapts with training.
Security Level	High – Used in military & banking.	Very High – Used for secure communications (e.g., SSL/TLS).	Very High – Stronger than RSA with smaller key sizes.	Moderate – Vulnerable to advanced attacks.	High – Can generate strong encryption schemes.	Moderate to High – Improves with training.
Training Time	No training needed	No training needed	No training needed	Fast – Simple models learn quickly.	High – GANs require extensive training.	High – Needs large datasets and training.
Processing Speed	Fast – Works efficiently for	Slow – High computational	Faster than RSA due to	Fast – Lightweight and	Slow – GAN training is	Moderate – Recurrence

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 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403058|

Metric	AES (Symmetric)	RSA (Asymmetric)	ECC (Asymmetric)	Neural Cryptography	GAN-Based Encryption	LSTM-Based Encryption
	bulk encryption.	cost.	smaller key size.	efficient.	resource-intensive.	increases processing time.
Key Size	128/256-bit	2048-bit or higher	160-512-bit	Learned encryption keys	Learned encryption keys	Learned encryption keys
Resistance to Quantum Attacks	Weak – Vulnerable to quantum attacks.	Weak – Shor's algorithm can break RSA.	Stronger than RSA but still at risk.	Uncertain – Depends on model robustness.	Uncertain – Can adapt but needs research.	Uncertain – Can learn patterns but needs better defenses.
Use Cases	Data encryption (files, VPNs, databases).	Digital signatures, secure communication (email, SSL/TLS).	Blockchain, secure messaging, IoT security.	IoT, low-power encryption.	Adaptive encryption, cybersecurity applications.	Secure communication, dynamic encryption.

IX. CONCLUSION

The integration of Deep Learning (DL) in encryption and decryption processes marks a significant advancement in cryptography, offering new solutions to the evolving challenges of digital security. Traditional encryption methods, though effective, are increasingly susceptible to new threats such as quantum computing and sophisticated machine learning-based attacks. DL algorithms, with their ability to learn complex patterns and adapt dynamically, provide a promising alternative for creating more secure and robust encryption systems.In this study, we explored several DL architectures, including Generative Adversarial Networks (GANs), Autoencoders (AEs), and Recurrent Neural Networks (RNNs), each of which demonstrated unique strengths in handling encryption tasks. GANs were shown to offer adaptive and resilient encryption, continuously improving to counter adversarial attacks. Autoencoders provided efficient encoding and decoding, ensuring data integrity while maintaining security. RNNs, particularly Long Short-Term Memory (LSTM) networks, were effective in preserving the sequential nature of data, which is crucial for encrypting text and time-series data.

The performance metrics applied, such as adversarial loss, reconstruction accuracy, and attack success rate, have illustrated the potential of DL models in enhancing encryption techniques. These metrics confirm that DL models can deliver strong security, high accuracy in decryption, and robustness to adversarial attacks, often outperforming traditional encryption methods like AES and RSA, especially in dynamic environments.Despite some challenges, the potential benefits of DL-based encryption—such as adaptability to new threats, real-time encryption capabilities, and efficiency—make it a promising field of study. Future work should focus on refining these models for better computational efficiency, robustness, and practical deployment in real-world applications like secure communication systems, cloud security, and privacy-preserving machine learning.

In conclusion, DL-based encryption systems represent the next frontier in cryptographic research, offering innovative solutions to meet the growing demands of data security in an increasingly connected world. As DL models continue to evolve, their applications in encryption will become more sophisticated and widely adopted, shaping the future of digital security.

REFERENCES

1. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). *Generative adversarial nets*. In *Advances in neural information processing systems* (pp. 2672-2680).
2. Kingma, D. P., & Welling, M. (2013). *Auto-Encoding Variational Bayes*. In *International Conference on Learning Representations (ICLR)*.

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 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403058|

3. Sutskever, I., Vinyals, O., & Le, Q. V. (2014). *Sequence to Sequence Learning with Neural Networks*. In *Advances in Neural Information Processing Systems* (pp. 3104-3112).
4. Patterson, S., & Sun, L. (2020). *Deep learning cryptography: A survey*. *Journal of Computer Security*, 28(2), 129-149. doi:10.3233/JCS-202000239.
5. Joulin, A., Grave, E., Mikolov, T., Bojanowski, P., Mikolov, M., & Manek, G. (2017). *Bag of Tricks for Efficient Text Classification*. In *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics* (pp. 427-432).
6. Dai, Z., & He, X. (2019). *Deep Learning for Data Encryption and Privacy Protection*. *IEEE Access*, 7, 69845-69854. doi:10.1109/ACCESS.2019.2911054.
7. Liu, Y., & Chang, T. (2021). *A survey on deep learning methods for cryptographic applications*. *Journal of Cryptography*, 24(3), 177-194. doi:10.1007/s12060-021-01399-3.
8. Zhou, X., Zhang, X., & Chen, X. (2019). *Security and Privacy in Blockchain-Based Cryptography: A Deep Learning Approach*. *Journal of Network and Computer Applications*, 151, 56-65. doi:10.1016/j.jnca.2019.05.002.
9. Kaiser, Ł., & Hofmann, S. (2020). *Evaluating the Strength of Deep Learning-based Encryption Techniques*. *International Journal of Information Security*, 19(5), 501-514. doi:10.1007/s10207-019-00514-2.
10. Mirza, M., & Oscherwitz, T. (2022). *Deep Learning in Cryptography: A New Paradigm for Data Security*. *IEEE Transactions on Cybernetics*, 52(4), 3064-3076. doi:10.1109/TCYB.2021.3083622.

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