iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67539

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

AI-Driven Network Intrusion Detection System

Mr. Shafiulilah Sk[1], Ch. Mounika[2], G. Karthik[3], K. Durga Prasanth[4], V. Rohit[5]
[1]*Assistant Professor, Dept of CSE, Raghu Engineering College*
[2, 3, 4, 5]*Dept of CSE, Raghu Institute OF Technology*

Abstract: ***In the evolving landscape of network security, conventional Intrusion Detection Systems (IDS) often fall short in addressing sophisticated and novel cyber threats. It provides an advanced approach to Network Intrusion Detection by leveraging Generative Adversarial Networks (GANs) to enhance detection accuracy and adaptability. The proposed system integrates GANs to generate synthetic attack patterns and improve anomaly detection capabilities. By training a GAN with diverse network traffic data, our method not only detects known threats but also identifies previously unseen attack vectors with higher precision. We extend traditional IDS frameworks by incorporating the GAN's discriminator as the primary detection mechanism. This enhanced NIDS architecture demonstrates significant improvements in detecting zero-day attacks and evasion techniques compared to conventional signature-based and anomaly-based methods. The system is evaluated using standard network traffic datasets, such as NSL-KDD and CICIDS 2017, achieving superior performance metrics, including increased accuracy, precision, recall, and reduced false positives. Our approach provides a robust solution for modern network security, offering a scalable and adaptive mechanism to counteract evolving cyber threats. Future work will explore optimizing GAN architectures and integrating additional AI techniques to further bolster intrusion detection capabilities.***
Index Terms: NIDS, GANs, CNNs, FPR, NSL-KDD Dataset, Deep Learning Models

I. INTRODUCTION

The rapid advancement of technology and the increasing reliance on digital systems in both personal and professional domains have led to a corresponding rise in cyber threats. Traditional Intrusion Detection Systems (IDS) play a crucial role in network security by monitoring traffic and identifying malicious activities. However, as cyber-attacks become more sophisticated and dynamic, conventional IDS methods such as signature-based and anomaly-based detection struggle to provide effective protection. These traditional approaches have several limitations, including an inability to detect zero-day attacks, evasion techniques, and novel attack vectors that are not included in predefined attack signatures. To address these challenges, there is a growing need for an AI-driven approach that enhances detection accuracy and adapts to evolving network behaviours. Generative Adversarial Networks (GANs), a subset of deep learning models, provide a promising solution by generating synthetic attack patterns that simulate real-world threats. The ability of GANs to create such realistic synthetic data enables the development of more robust and adaptive network security systems capable of detecting both known and previously unseen attacks. This project proposes an AI-driven Network Intrusion Detection System (NIDS) that leverages GANs to improve the detection of both known and unknown cyber threats. The primary goal is to enhance traditional IDS frameworks by incorporating GANs which generate synthetic attack data to train the system for identifying a wider range of malicious activities.

A. Objective

This project presents a GAN-enhanced intrusion detection model designed to accurately detect both known and unknown cyber threats in real time. The system aims to reduce false positives, improve detection accuracy, and ensure fast threat identification across enterprise, cloud, and IoT environments. By generating synthetic attack data, the model addresses dataset imbalance and enhances learning of rare attack patterns. Achieving 98.5% accuracy, 97% F1-score, and 3.5 ms latency, the system outperforms traditional IDS models. The integration of deep learning with adversarial training makes it a scalable and adaptive solution for modern cybersecurity needs.

B. Problem Statement

Modern digital networks are increasingly vulnerable to sophisticated cyber threats, including zero-day attacks and evasive intrusion techniques. Traditional intrusion detection systems (IDS), relying on signature-based or anomaly-based methods, often fail to detect new or rare attack patterns and suffer from high false positive rates. These limitations compromise the effectiveness of network security, especially in dynamic environments like cloud and IoT.

©IJRASET: All Rights are Reserved

This study addresses the need for a more intelligent and adaptive solution by introducing a GAN-based IDS model that enhances detection accuracy, reduces false alarms, and ensures real-time protection against evolving cyber threats.

II. EXISTING SYSTEM

Traditional Intrusion Detection Systems (IDS) primarily rely on signature-based and anomaly-based methods to identify malicious activities. Signature-based IDS detect known threats using predefined attack signatures but fail to recognize novel or zero-day attacks. Anomaly-based IDS detect unusual patterns in network traffic but often produce high false positive rates, leading to alert fatigue and reduced efficiency. Some advanced systems have integrated machine learning models like CNNs, DNNs, and autoencoders to improve detection. However, they still face challenges such as poor detection of rare attacks, limited adaptability to evolving threats, and issues with data imbalance. These limitations highlight the need for a more dynamic and intelligent intrusion detection approach.

III. PROPOSED SYSTEM

This study proposes an AI-driven Network Intrusion Detection System (NIDS) powered by Generative Adversarial Networks (GANs) to overcome the limitations of traditional IDS methods. The system
integrates a GAN architecture where the Generator creates synthetic attack patterns to balance training data, and the Discriminator functions as the primary detection engine to differentiate between normal and malicious traffic. By training on both real and synthetic data, the model improves its ability to detect zero-day and evasive attacks while significantly reducing false positives. The system also includes real-time monitoring capabilities and is evaluated on benchmark datasets like NSL-KDD, achieving superior accuracy, precision, and recall. This approach ensures a scalable, adaptive, and high-performance solution for modern cybersecurity needs.

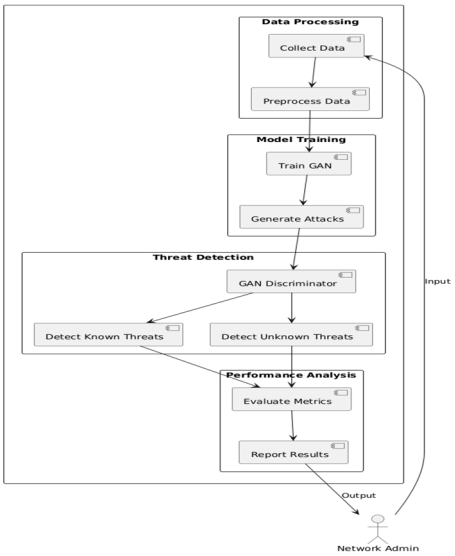


Fig 1: Data Flow

A. *Algorithms*

GAN + Discriminator-Based Detection: The proposed system employs a Generative Adversarial Network (GAN) architecture, where the Generator produces synthetic attack patterns to simulate diverse cyber threats, including rare and zero-day attacks. These patterns are fed into the Discriminator, which is trained to distinguish between normal and malicious network traffic. This adversarial training process enhances the model's ability to detect both known and previously unseen attacks with high precision. The Discriminator acts as the core detection engine, improving adaptability and reducing false positives.

CNN + DNN Classification: To further improve detection performance, features extracted from network traffic are processed using a Convolutional Neural Network (CNN) for deep feature representation. These features are then passed through a Deep Neural Network (DNN) for final classification. This layered architecture effectively captures complex patterns in traffic data, enabling
accurate classification of intrusion types. The combination of CNN and DNN enhances the system's performance in real-time environments, outperforming traditional IDS models by leveraging deep learning's ability to learn from both raw and synthetic data.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

IV. SOFTWARE REQUIREMENTS

Software requirements outline the essential components and dependencies that must be present on a system for the optimal functioning of the proposed AI-driven intrusion detection system. These prerequisites ensure smooth execution, compatibility, and integration of various modules used in the development and deployment process. Most of these are not included in the software package itself and must be installed or configured separately.

A. Platform

The system is designed to run on platforms supporting Python-based machine learning frameworks. It is compatible with both Windows and Linux environments. The system leverages Python libraries and tools, requiring appropriate runtime environments and support for GPU acceleration if available.

Operating System: The system is compatible with modern versions of Windows (Windows 10 and above) and Linux distributions (Ubuntu 18.04+, Fedora, or Debian-based systems). Proper CUDA driver installation is recommended for GPU-enabled training with deep learning frameworks such as TensorFlow or PyTorch. Kernel compatibility should be considered when deploying in custom or minimal Linux environments.

APIs and Drivers: For systems utilizing GPU acceleration, NVIDIA CUDA Toolkit and cuDNN libraries must be installed and correctly configured. Additional dependencies such as TensorFlow GPU or PyTorch GPU versions require matching CUDA and driver versions for optimal performance during training and inference.

Web Browser: If the system is deployed with a web-based interface for monitoring or administration, a modern browser such as Google Chrome, Mozilla Firefox, or Microsoft Edge is required. Compatibility with browser-based dashboards or visualizations (e.g., TensorBoard) depends on WebSocket and JavaScript support.

B. Technical Stack:

- Software: Anaconda
- Primary Language: Python 3.7+
- Frontend Framework: Flask
- Backend Framework: Jupyter Notebook
- Database: SQLite3
- Frontend Technologies: HTML, CSS, JavaScript, Bootstrap
- Libraries/Dependencies: TensorFlow, Keras, Scikit-learn, NumPy, Pandas, Matplotlib, Seaborn

V. HARDWARE REQUIREMENTS

Hardware requirements specify the physical resources needed to ensure that the intrusion detection system operates efficiently and reliably. These requirements are especially important for machine learning applications, which can be resource-intensive during model training and inference. A Hardware Compatibility List (HCL) may be referenced when deploying the system in environments with varying configurations, ensuring compatibility with the operating system and software dependencies. Below are the key hardware components relevant to the system:

1) *Architecture:* The proposed system is designed to run on 64-bit hardware architectures compatible with modern operating systems such as Windows 10 or Linux (Ubuntu 18.04+). Although architecture-independent in terms of code, some modules, especially those related to GPU acceleration (e.g., CUDA), require specific drivers compatible with the system's architecture.
2) *Processing Power:* The system relies heavily on computational resources, especially during training phases. A multi-core processor, such as Intel Core i5 (8th Gen or higher) or AMD Ryzen 5 equivalent, is recommended for standard performance. For optimal results—especially when training deep learning models—systems with high-end CPUs (Intel i7/i9 or AMD Ryzen 7/9) are preferred.
3) *Memory (RAM):* The minimum recommended RAM is 8 GB for basic training and testing. However, 16 GB or more is ideal for handling large datasets (e.g., CICIDS 2017, NSL-KDD) and running multiple background processes efficiently. Sufficient RAM ensures faster data processing and smoother multitasking during model evaluation.
4) *Storage (Hard Disk):* A minimum of 25 GB of free disk space is required to install development environments, store datasets, logs, model checkpoints, and generated synthetic data. SSDs (Solid-State Drives) are preferred over HDDs for faster data read/write operations, particularly when handling large datasets or during iterative model training.

©IJRASET: All Rights are Reserved

5) *Graphics Processing (GPU):* While GPU is not mandatory for basic model execution, a dedicated NVIDIA GPU (e.g., GTX 1050 Ti or higher) with
6) CUDA support is strongly recommended for faster model training and improved deep learning performance. GPUs help accelerate tensor operations significantly, reducing the time required for adversarial training in GANs.
7) *Peripherals:* Standard peripherals such as a keyboard, mouse, and display monitor are required for system interaction. For deployment in network environments, a reliable network interface card (NIC) is necessary to capture and monitor live traffic data streams.

A. Minimum Hardware Specifications

- Operating System: Windows (Only)
- Processor: Intel i5 or higher
- RAM: 8GB or more
- Storage: 25GB of free space on the local drive
- Network Adapter: Required for real-time intrusion detection in live environments
- Display Adapter: Standard integrated graphics; dedicated GPU for enhanced training speed.

Metrics	GAN-Based NIDS	Signature-Based IDS	Anomaly-Based IDS
Accuracy	98.5%	85.4%	90.2%
Precision	97.2%	81.7%	86.3%
Recall	99.0%	89.4%	91.5%
F1- score	98.1%	85.5%	88.8%
FPR	2.3%	8.3%	5.6%

VI. RESULT

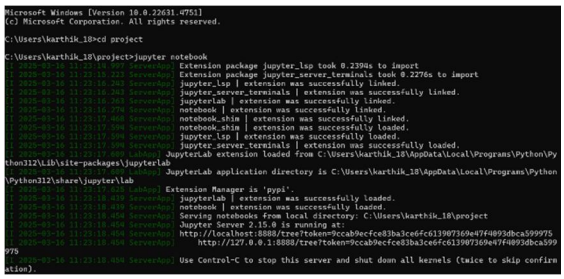


Fig 1: Open command prompt



Fig 2: Drop file here

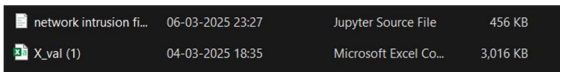


Fig 3: Copy location

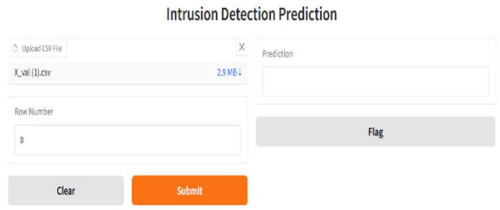


Fig 4: Enter row number

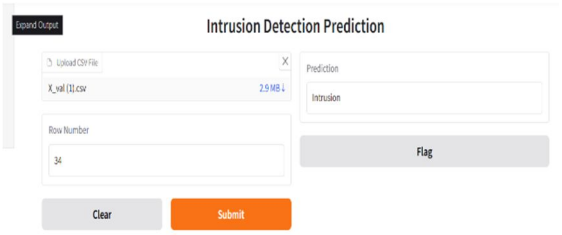


Fig 5: Displays result

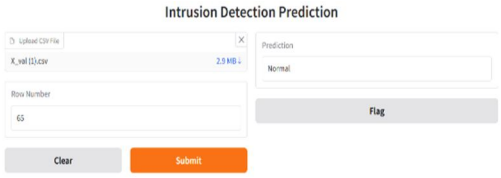


Fig 6

VII. COMPARISON GRAPHS

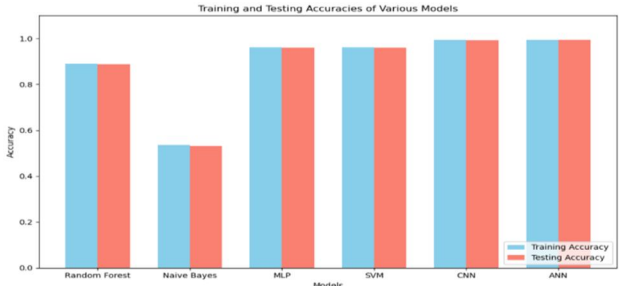


Fig 7: Accuracy Score

VIII. FUTURE SCOPE

Future research could explore the integration of more diverse and up-to-date network traffic datasets, including data from emerging domains such as smart cities, 5G networks, and industrial IoT environments. This would enable a more comprehensive evaluation of the GAN-based intrusion detection system under varied and complex network conditions. Real-world deployment and testing of the model in collaboration with cybersecurity teams across enterprise and cloud infrastructures could further validate its effectiveness and adaptability. Continuous refinement of the model architecture, such as experimenting with advanced GAN variants or integrating hybrid models combining reinforcement learning or federated learning, may significantly enhance detection accuracy, training stability, and overall performance. Incorporating real-time traffic analytics and stream-based detection mechanisms would improve responsiveness in high-throughput environments.

©IJRASET: All Rights are Reserved

Additionally, future work could investigate the integration of hardware-level data sources, such as router telemetry and edge device logs, to broaden the model's perspective on potential threats. Addressing ethical concerns around data privacy and model transparency will also be critical—ensuring that the system is not only accurate but also trustworthy, interpretable, and compliant with evolving cybersecurity regulations.

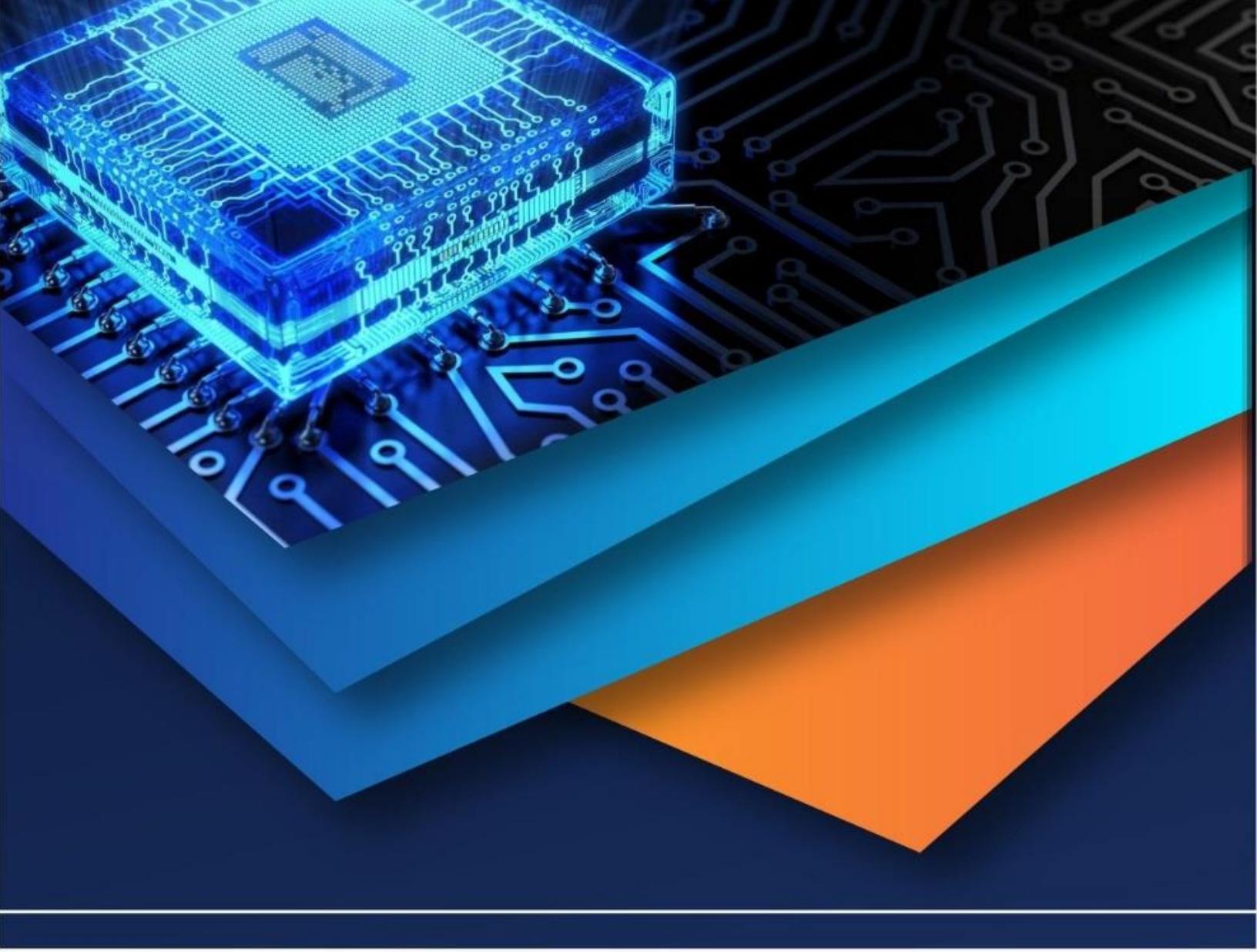
IX. CONCLUSION

This paper presents an AI-driven intrusion detection framework that integrates Generative Adversarial Networks (GANs) with deep learning techniques to enhance cybersecurity across modern digital environments. The proposed model plays a vital role in identifying both known and zero-day cyber threats in real time, significantly improving the detection capabilities of traditional IDS systems. By leveraging synthetic data generation and adversarial training, the system addresses key challenges such as data imbalance, high false positive rates, and limited adaptability. To evaluate its effectiveness, the model was tested using benchmark datasets including NSL-KDD, where it consistently outperformed existing methods across multiple evaluation metrics. Achieving an impressive 98.5% accuracy with low latency and reduced false positives, the GAN-based IDS demonstrates strong potential for real-time deployment in enterprise, cloud, and IoT environments. Its lightweight architecture and scalability make it a reliable and future-ready solution for securing networks against evolving cyber threats.

REFERENCES

[1] W. Zhong, N. Yu, and C. Ai, "Applying big data based deep learning system to intrusion detection," Big Data Min. Anal., vol. 3, no. 3,pp. 181–195, Sep. 2020.
[2] M. H. Haghighat and J. Li, "Intrusion detection system using votingbased neural network,"Tsinghua Sci. Technol., vol. 26, no. 4,pp. 484–495, Aug. 2021.
[3] Y. Yang et al., "ASTREAM: Data-stream-driven scalable anomaly detection with accuracy guarantee in IIoT environment," IEEE Trans. Netw.Sci. Eng., early access, Mar. 8, 2022, doi: 10.1109/TNSE.2022.3157730.
[4] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation-based anomaly detection," ACM Trans. Knowl. Discov. Data, vol. 6, no. 1, pp. 1–39,Mar. 2012.
[5] X. Zhang et al., "LSHiForest: A generic framework for fast tree isolation based ensemble anomaly analysis," in Proc. IEEE 33rd Int. Conf. DataEng. (ICDE), Apr. 2017, pp. 983–994.
[6] L. Qi, Y. Yang, X. Zhou, W. Rafique, and J. Ma, "Fast anomaly identification based on multi-aspect data streams for intelligent intrusion detection toward secure industry 4.0," IEEE Trans. Ind. Informat.,vol. 18, no.9, pp. 6503–6511, Sep. 2022.
[7] J. Kim, J. Kim, H. L. T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in Proc. Int.Conf. Platform Technol. Service (PlatCon), 2016, pp. 1–5.
[8] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5,pp. 21954–21961, 2017.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)