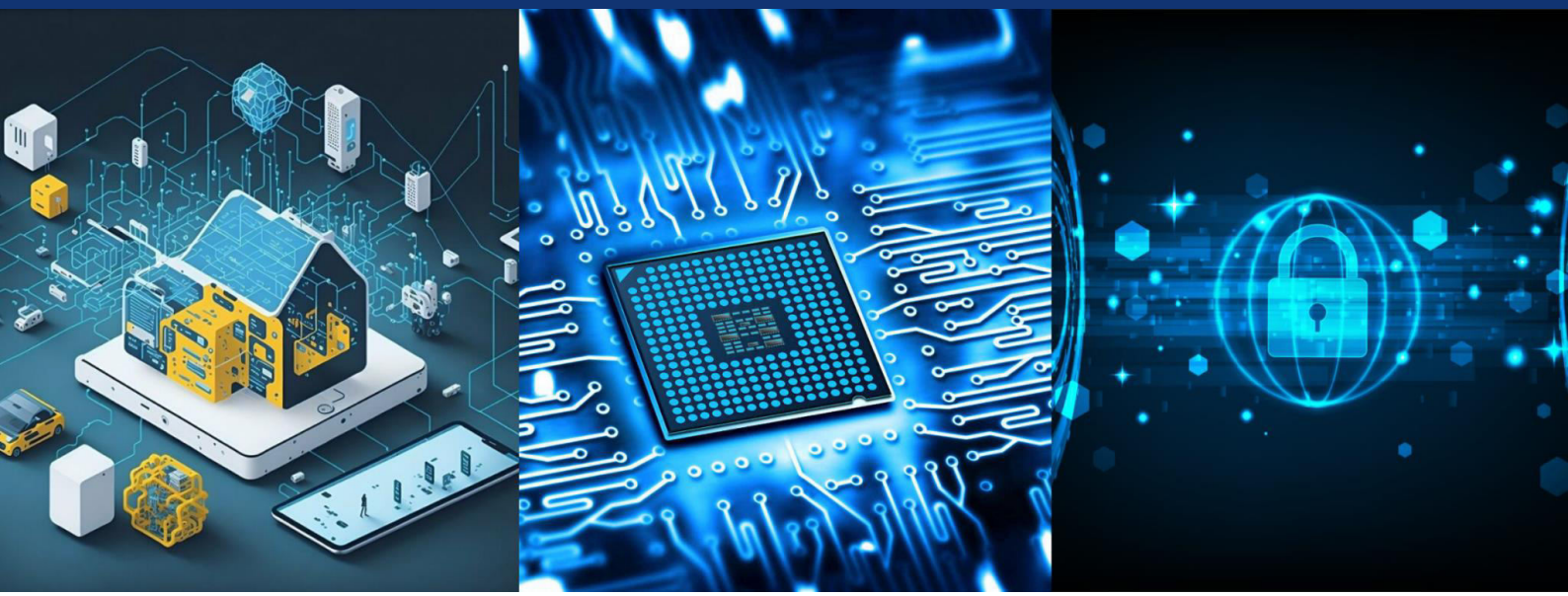
IJIRCCE

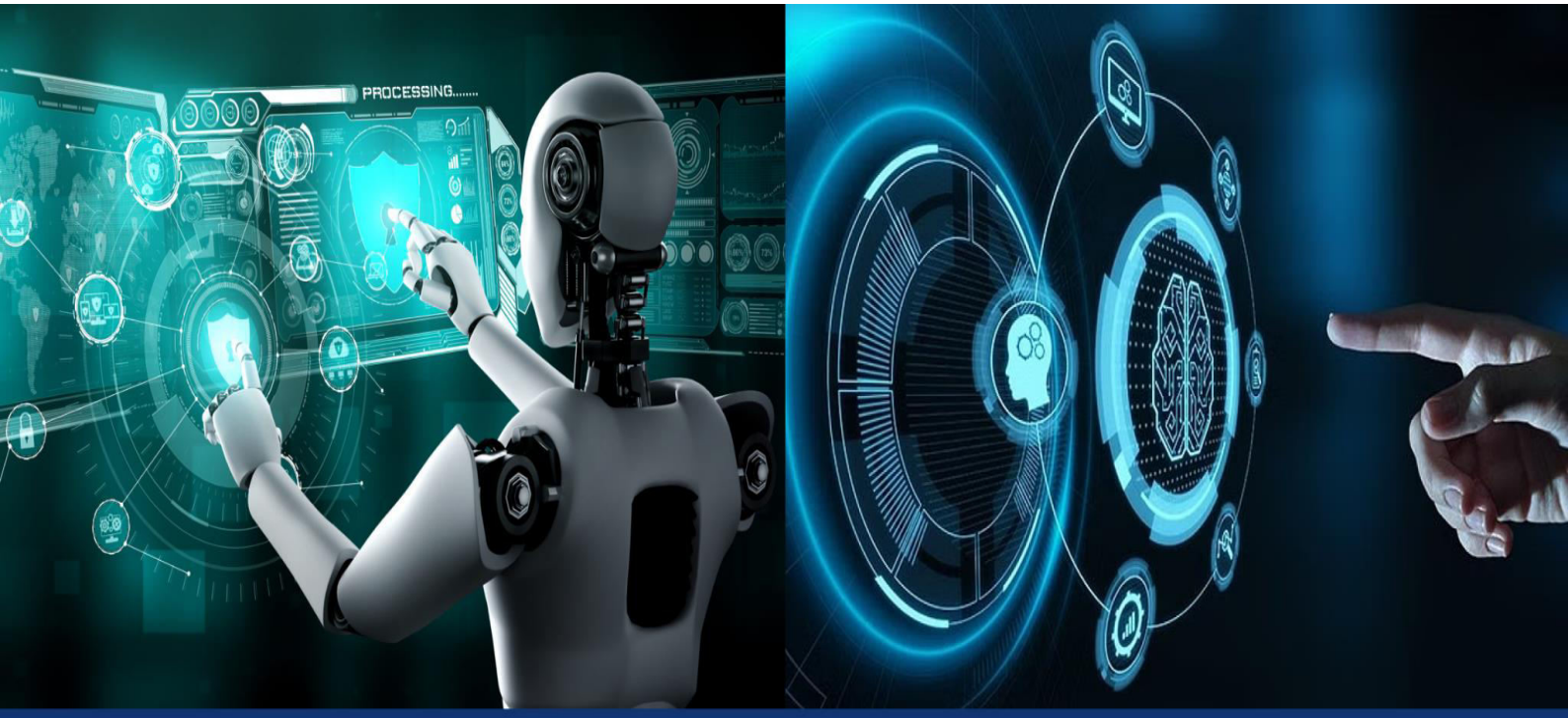
ISSN(O): 2320-9801

ISSN(P): 2320-9798



# International Journal of Innovative Research in Computer and Communication Engineering

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




**Impact Factor: 8.771**

**Volume 13, Issue 5, May 2025**

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305166

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

# On the Feasibility of Deep Learning in Sensor Network Intrusion Detection

**B Shanmuga Priya**

Assistant Professor, Dept. of AIDS, The Kavery Engineering College, Salem, Tamil Nadu, India

**Nishanth A, NithishKumar G, Naveen Kumar T, Jagadeesh R**

UG Student, Dept. of CSE, The Kavery Engineering College, Salem, Tamil Nadu, India

**ABSTRACT:** With the rapid growth of the internet, the security threats to computer networks have escalated significantly, making the reduction and prevention of cybercrime a top priority in the digital age. Sensor Netork Intrusion Detection Systems (NIDS) struggle with limitations in detection accuracy and real-time performance as attackers employ increasingly sophisticated techniques. In recent years, deep learning has emerged as a prominent solution in the NIDS field due to its powerful capabilities in feature extraction and classification. The existing Intrusion Detection System are thus facing challenges for improvement in Intrusion Detection, handling heterogeneous data sources is hard for discovering zero-day attacks in sensor networks. High volume, variety and high speed of data generated in the network have made the data analysis process to detect attacks by traditional techniques very difficult. To proposed Recurrent Neural Network (RNN) algorithm to detect the IDS. The data processed by the preprocessing module are compressed by the auto-encoder module to obtain a lower-dimensional reconstruction feature, and the classification result is obtained through the classification module. Compressed features of each traffic are stored in the database module which can both provide retraining and testing for the classification module and restore these features to the original traffic for post event analysis and forensics. We used KDD cup 99 to train and test the model. Through this way, could reduce the number of false rate and increase the accuracy of the designed intrusion detection system.

**KEYWORDS:** Intrusion Detection Systems, Network, sensor, Recurrent Neural Network, accuracy

## I. INTRODUCTION

Application systems and computer networks are essential for effective business processes in today's quickly evolving technology world. They enable the seamless exchange of resources, including data, processing power, storage, and information. As the need for automated systems that can quickly and efficiently accomplish organizational goals has grown, so has the use of application systems in networked environments. At the same time, privacy and security issues in application systems and networks have become more well-known, highlighting the necessity of strengthening security controls against the constantly changing threats in today's cyberspace. Within the larger framework of modern civilization, the Internet is a vital resource that promotes international communication and information sharing. The Internet is essential for exchanging important information among authorities or wirelessly transmitting basic photographs on social media. Even with significant progress, persistent problems, including vulnerability to cyberattacks and difficulties enforcing international protection rules, exist, necessitating proactive measures on the part of businesses to defend their interests from possible security breaches and incursions.

When paired with firewalls, intrusion detection systems (IDS) are among the essential security elements that can effectively handle a wide range of security risks. IDS techniques fall into two categories: Network Intrusion Detection Systems based on signatures and Anomaly Detection Systems based on anomaly detection. NIDS relies on signatures to identify intrusions and does so by comparing patterns across all the data they retrieve. On the other hand, anomaly-based alerts for intrusions detect any appreciable departures from the typical traffic pattern in the user behavior being monitored. Consequently, anomaly detection NIDS performs better when dealing with new attack patterns, while signature-based NIDS has a higher detection rate for recognized attack types. However, it frequently results in false alarms because of variations in intruder behavior. Finding abnormal patterns in the system audit record might aid in identifying security breaches.IDS solutions are one of the key security components that in combination with firewalls can effectively handle various types of security attacks. IDS schemes can be mainly classified as misuse detection schemes and anomaly detection schemes, which can be realized by using various machine learning techniques. Misuse

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

detection or signature-based systems heavily depend on the signature of the security attacks and malicious behaviors and support multi-class classification. However, they cannot detect the new attacks in which their signature is not available for the IDS . However, as an advantage, these schemes benefit from more accuracy in recognizing known malicious behaviors and their variants. On the other hand, the anomaly detection-based IDS approaches can detect new attacks by relying on the users' normal behavior profiles and only support binary classifications. Nonetheless, in dynamic organizations in which users' roles change occasionally, their profiles should be updated correspondingly. Also, anomaly detection schemes may suffer from the false positive problem. A large number of recent researches are conducted in both anomaly detection and misuse detection contexts using various machine learning techniques. Conventional machine learning techniques suffer from the lack of labeled training datasets and heavily rely on the extracted features by a human, which makes it difficult for deployment on large platforms. Deep learning is a novel paradigm in the machine learning field mainly established using RNNs or artificial neural networks and has a higher performance than the other conventional machine learning techniques.

## II. LITERATURE SURVEY

### 2.1 Network Intrusion Detection Based on Feature Image and Deformable Vision Transformer Classification

K. He et al (2024) defined as, Network intrusion detection technology has always been an indispensable protection mechanism for industrial network security. The rise of new forms of network attacks has resulted in a heightened demand for these technologies. Nevertheless, the current models' effectiveness is subpar. We propose a new Deformable Vision Transformer (DE-VIT) method to address this issue. DE-VIT introduces a new deformable attention mechanism module, where the positions of key-value pairs in the attention mechanism are selected in a data-dependent manner, allowing it to focus on relevant areas, capture more informative features, and avoid excessive memory and computational costs. In addition to using deformable convolutions instead of regular convolutions in embedding layers to enhance the receptive field of patches, a sliding window mechanism is also employed to utilize edge information fully. In Parallel, we use a layered focal loss function to improve classification performance and address data imbalance issues. In summary, DE-VIT reduces computational complexity and achieves better results.

### 2.2 Sensor and Decision Fusion-Based Intrusion Detection and Mitigation Approach for Connected Autonomous Vehicles

M. Moradi et al (2024) defined as, The safety of connected and autonomous vehicles (CAV) depends on the security of in-vehicle communication. The controller area network (CAN) bus holds a crucial position in ensuring in-vehicle security. Injecting attacks (e.g., increasing the speed) by hackers can affect drivers. This article proposes a fusion intrusion detection and resilient approach to maintain system performance against intrusion. The proposed system consists of two parts: sensor validation and sensor value estimation. In the sensor validation step, a new fusion approach uses three feature ranking approaches, autoencoder, and estimator-based detectors. Finally, Yager's rules are used to handle conflict between classifiers and enrich intrusion detection accuracy. Afterward, in the second part, if any intrusion is detected, the estimated values of that sensor which is under intrusion will be replaced based on estimated values by a long short-term memory-based deep regressor (LSTM DR) to avoid any performance disruption of the system. The main contribution of this study is that the proposed fusion approach uses the inherent redundancy among heterogeneous sensors to create a resilient system against compromised sensors.

## III. EXISTING SYSTEM

### 3.1 Existing System

An existing novel approach for intrusion detection that uses Support Vector Machine (SVM) and decision tree. Existing to exploit quantitative data flow properties to extract highly characteristic behavior patterns from collections of known intrusion. By combining a SVM and NB based machine learning techniques provide low classification accuracy prediction results.

#### 3.1.1 Disadvantages:

- ➢ The computational complexity of this current method would be limiting in a real-time setting.
- ➢ Increasing the complexity of detection makes for a much more robust analysis system.
- ➢ In the graph mining data representation gets away from the need to specify the appropriate.

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305166

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

**3.2 Proposed System**:

It focuses on dynamic analysis to discover hidden behavior in packed samples where it is essential to do so. The proposed RNN algorithm gives high accuracy for intrusion detection. In addition, it also classifies malware based on their family and checked the accuracy of each of the malware behavior. Static analysis targets source and object codes and examines codes without actually starting a project. It decompiles malware source code to detect commands, reports, and vulnerabilities in many programs. RNN method of searching for certain types of memory leakage, traffic flow, and flows data into code that actually runs. However, a large amount of storage is required for applying this method to the mobile environment, and the performance overhead is high for system matching.

**3.2.1 Advantages**

- ➢ Very effective at detecting intrusion in network.
- ➢ The detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.
- ➢ Unique identifier is established about a known threat so that the threat can be identified in the data.

## IV. SYSTEM REQUIREMENTS

**4.1. INTRODUCTION**

It focuses on dynamic analysis to discover hidden behavior in packed samples where it is essential to do so. The proposed RNN algorithm gives high accuracy for intrusion detection. In addition, it also classifies malware based on their family and checked the accuracy of each of the malware behavior. Static analysis targets source and object codes and examines codes without actually starting a project. It decompiles malware source code to detect commands, reports, and vulnerabilities in many programs. RNN method of searching for certain types of memory leakage, traffic flow, and flows data into code that actually runs. However, a large amount of storage is required for applying this method to the mobile environment, and the performance overhead is high for system matching.

**4.2 BLOCK DIAGRAM**

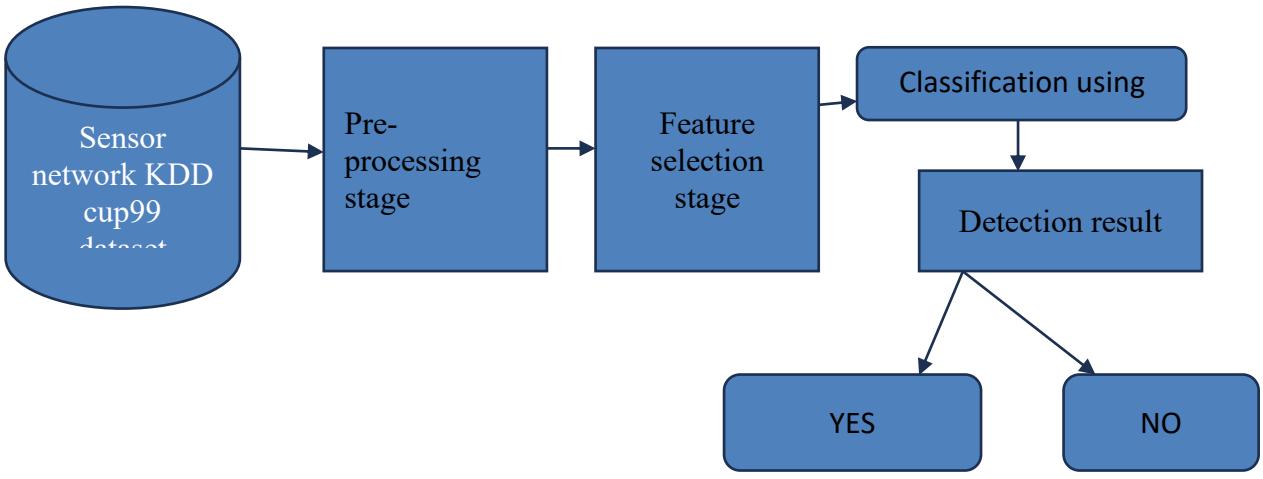



**FIG1: PROPOSED DIAGRAM**

**Hardware Requirements**

- ➢ CPU type : Intel core i3
- ➢ Ram size : 8 GB
- ➢ Hard disk capacity : 500 GB

© 2025 IJIRCCE | Volume 13, Issue 5, May 2025| DOI:10.15680/IJIRCCE.2025.1305166

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

**Software Requirement**

- Operating System : Windows 10
- Language : Python
- Tool : Anaconda

**Software Description**

Python is a high-level, interpreted, interactive and object-oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages.

Python is a MUST for students and working professionals to become a great Software Engineer especially when they are working in Web Development Domain. I will list down some of the key advantages of learning Python:

**Python is Interpreted** − Python is processed at runtime by the interpreter. You do not need to compile your program before executing it. This is similar to PERL and PHP.

**Python is Interactive** − You can actually sit at a Python prompt and interact with the interpreter directly to write your programs.

**Python is Object-Oriented** − Python supports Object-Oriented style or technique of programming that encapsulates code within objects.

**Python is a Beginner's Language** − Python is a great language for the beginner-level programmers and supports the development of a wide range of applications from simple text processing to WWW browsers to games.

**Characteristics of Python**

Following are important characteristics of Python Programming

- It supports functional and structured programming methods as well as OOP.
- It can be used as a scripting language or can be compiled to byte-code for building large applications.
- It provides very high-level dynamic data types and supports dynamic type checking.
- It supports automatic garbage collection.
- It can be easily integrated with C, C++, COM, ActiveX, CORBA, and Java.

**Python Features**

Python provides lots of features that are listed below.

**1) Easy to Learn and Use**

Python is easy to learn and use. It is developer-friendly and high level programming language.

**2) Expressive Language**

Python language is more expressive means that it is more understandable and readable.

**3) Interpreted Language**

Python is an interpreted language i.e. interpreter executes the code line by line at a time. This makes debugging easy and thus suitable for beginners.

## V. MODULE DESCRIPTION

**5.1 KDDcup99 dataset**

KDD
training dataset consists of approximately 4,900,000 single
connection vectors each of which contains 41 features and
is labeled as either normal or an attack, with exactly one
specific attack type.

KDD dataset consists of approximately 4,900,000 single connection vectors each of which contains 41 features and is labeled as either normal or an attack, with exactly one specific attack type. The Dataset contains various attacks such as Denial of Service Attack (DOS), User to Root Attack (U2R), Remote to Local Attack (R2L) and Probing Attack.

- Denial of Service (dos): Attacker tries to prevent legitimate users from using a service.
- Remote to Local (r2l): Attacker does not have an account on the victim machine, hence tries to gain access.
- User to Root (u2r): Attacker has local access to the victim machine and tries to gain super user privileges.
- Probe: Attacker tries to gain information about the target host.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

### 5.2 Pre-processing

Pre-processing of data becomes crucial in avoid the noisy, missing and inconsistent data available in the dataset. Since the records of the dataset are collected from multiple and heterogeneous sources, the quality of the data deteriorates and therefore needs to be pre-processed. Several factors affect the quality of the data. These factors comprise accuracy, completeness, consistency, timeliness, believability and interpretability. The proposed pre-processing check null values, and fill missing values in efficient manner.

### 5.3 Feature selection

Feature selection aims to select the best feature in the data set. Deep learning technique can classify the data into a set of class features and targets. Feature selection (variable elimination) helps understand the data, reduces computing needs, reduces dimensional curse effects and improves the performance.

## VI. CONCLUSION

### 6.1 Conclusion

Intrusion detection systems are one of the essential security components of the current information technology-based organizations. However, providing an efficient and high-performance IDS approach to deal with a wide variety of security attacks is a challenging approach. Recently, deep learning techniques have proved to deal with intrusion detection problems, and several deep learning-based IDS schemes are introduced in the literature. Deep learning is a subset of machine learning techniques, which incorporate several layers to conduct nonlinear processing and learn several data representation levels. The advent of network-based technologies has increased the associated vulnerabilities. As a result, it has become paramount to design and implement effective IDS. In this paper, we apply feature selection methods to improve our understanding of relevant features inside network traffic data and construct potent detection systems using KDDcup99 dataset. The proposed Recurrent Neural Network (RNN) algorithm to detect the IDS. The data processed by the preprocessing module are compressed by the auto-encoder module to obtain a lower-dimensional reconstruction feature, and the classification result is obtained through the classification module.

### 6.2 Future work

Future work in intrusion detection for sensor networks is crucial to address the growing challenges of security and scalability. IDS models will need to balance high detection accuracy with low energy consumption to ensure the longevity of sensor networks. Furthermore, decentralized and collaborative intrusion detection methods could enhance network resilience by allowing nodes to share and analyze data in a distributed manner. As cyber threats become increasingly sophisticated, it is essential to develop IDS frameworks that can evolve autonomously, adapt to new attack vectors, and maintain privacy and scalability.

## REFERENCES

1. O. Y. Al-Jarrah, K. E. Haloui, M. Dianati and C. Maple, "A Novel Detection Approach of Unknown Cyber-Attacks for Intra-Vehicle Networks Using Recurrence Plots and Neural Networks," in IEEE Open Journal of Vehicular Technology, vol. 4, pp. 271-280, 2023, doi: 10.1109/OJVT.2023.3237802.
2. M. Moradi et al., "Sensor and Decision Fusion-Based Intrusion Detection and Mitigation Approach for Connected Autonomous Vehicles," in IEEE Sensors Journal, vol. 24, no. 13, pp. 20908-20919, 1 July 1, 2024, doi: 10.1109/JSEN.2024.3397966.
3. E. -U. -H. Qazi, T. Zia, M. Hamza Faheem, K. Shahzad, M. Imran and Z. Ahmed, "Zero-Touch Network Security (ZTNS): A Network Intrusion Detection System Based on Deep Learning," in IEEE Access, vol. 12, pp. 141625-141638, 2024, doi: 10.1109/ACCESS.2024.3466470.
4. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," in IEEE Access, vol. 10, pp. 99837-99849, 2022, doi: 10.1109/ACCESS.2022.3206425.
5. M. Almehdhar et al., "Deep Learning in the Fast Lane: A Survey on Advanced Intrusion Detection Systems for Intelligent Vehicle Networks," in IEEE Open Journal of Vehicular Technology, vol. 5, pp. 869-906, 2024, doi: 10.1109/OJVT.2024.3422253.
6. Jamalipour and S. Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9444-9466, 15 June 15, 2022, doi: 10.1109/JIOT.2021.3126811.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details