iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VII **Month of publication:** July 2024

DOI: https://doi.org/10.22214/ijraset.2024.63735

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 12 Issue VII July 2024- Available at www.ijraset.com

Proactive Identification of Live Cyber Threats in IoT-Enhanced Security Systems

Dr. Sapna B Kulkarni[1], Sayed Abunasr Quadri[2]
[1]*Associate Professor,* [2]*Student, M Tech 4th Sem, Dept of CSE, RYMEC Ballari VTU University, Belgaum*

Abstract: ***A computer network may be impacted by malicious software, computer viruses, and other hostile attacks. A crucial element of network security is intrusion detection, which is an active defensive system. Traditional intrusion detection systems suffer from problems including poor accuracy, poor detection, a high rate of false positives, and an inability to handle novel forms of intrusions. To address these issues, we propose a deep learning-based novel method to detect cybersecurity vulnerabilities and breaches in cyber-physical systems. The proposed framework contrasts the unsupervised and deep learning-based discriminative approaches. We presents a generative adversarial network to detect cyber threats in IoT-driven IICs networks. The results demonstrate a performance increase in terms of accuracy, reliability, and efficiency in detecting all types of attacks. The output of well-known state-of-the-art DL classifiers achieved the highest true rate (TNR) and highest detection rate (HDR) when detecting the following attacks such as BruteForceXXS, BruteForceWEB, DoS_Hulk_Attack, and DOS_LOIC_HTTP_Attack on the three data sets namely NSL-KDD, KDDCup99, and UNSW-NB15 datasets. It also maintained the confidentiality and integrity of users' and systems' sensitive information during the training and testing phases.***
Keywords: IoT, cybersecurity, intrusion detection system, deep learning, generative adversarial network, cyber-physical

I. INTRODUCTION

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Intrusion detection systems (IDS) are part of a system's subsequent protection line. Employing a variety of benign traffic/ normal flow patterns and precise attack-specific rules, IDS can distinguish between harmful and non-malicious activity. Data mining is used to describe and deploy IDSs with robust behaviour with higher accuracy than traditional IDS that may impact modern, sophisticated cyber-attacks. Businesses are growing increasingly worried about securing critical infrastructure (CI), especially Internet Industrial Control Systems (IICs), as the number of devices used in IIoT based setups is continuously rising. In the literature, several intrusion detection systems (IDS) have been developed to identify online attacks on IICSs networks. However, there are some significant flaws in the methodologies and evaluation metrics of the majority of the current IDSs. To address the issues of poor detection rate and high false positive rates (FPR), we provides an effective IDS for IIoT-powered IICs utilizing deep-autoencoder-based LSTM model/method.

II. LITERATURE SURVEY

1) Convolutional Neural Network—A Practical Case Study:

ABSTRACT: The convolutional neural networks had enormous success in the classification of images, and networks such as "AlexNet", "VGG", "Inception" and "ResNet" were references for this purpose. This way, it is intended to verify which networks were more successful in the "Imagenet" dataset challenge. Then, it was verified their success when classifying videos through the "Kinetics400" and "UCF101" datasets and, finally, to conclude if the success in the classification of images can also evidence a possible success in the classification of videos. To this end, the margin of error of the networks mentioned above is compared.

2) Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets

ABSTRACT: The explosive growth of the Internet of Things (IoT) applications has imposed a dramatic increase of network data and placed a high computation complexity across various connected devices. The IoT devices capture valuable information, which allows the industries or individual users to make critical live dependent decisions. Most of these IoT devices have resource constraints such as low CPU, limited memory, and low energy storage. Hence, these devices are vulnerable to cyber-attacks due to the lack of capacity to run existing general-purpose security software. It creates an inherent risk in IoT networks.

The multi-access edge computing (MEC) platform has emerged to mitigate these constraints by relocating complex computing tasks from the IoT devices to the edge. Most of the existing related works are focusing on finding the optimized security solutions to protect the IoT devices. We believe distributed solutions leveraging MEC should draw more attention. This paper presents a comprehensive review of state-of-the-art network intrusion detection systems (NIDS) and security practices for IoT networks. We have analyzed the approaches based on MEC platforms and utilizing machine learning (ML) techniques. The paper also performs a comparative analysis on the public available datasets, evaluation metrics, and deployment strategies employed in the NIDS design. Finally, we propose an NIDS framework for IoT networks leveraging MEC.

3) A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method:

ABSTRACT: Due to the rapid growth in IT technology, digital data have increased availability, creating novel security threats that need immediate attention. An intrusion detection system (IDS) is the most promising solution for preventing malicious intrusions and tracing suspicious network behavioral patterns.

Machine learning (ML) methods are widely used in IDS. Due to a limited training dataset, an ML-based IDS generates a higher false detection ratio and encounters data imbalance issues. To deal with the data-imbalance issue, this research develops an efficient hybrid network-based IDS model (HNIDS), which is utilized using the enhanced genetic algorithm and particle swarm optimization(EGA-PSO) and improved random forest (IRF) methods. In the initial phase, the proposed HNIDS utilizes hybrid EGA-PSO methods to enhance the minor data samples and thus produce a balanced data set to learn the sample attributes of small samples more accurately.

A. Functional Requirements

1) Data Collection
2) Data Preprocessing
3) Training and Testing
4) Modeling
5) Predicting

B. Non Functional Requirements

NON-FUNCTIONAL REQUIREMENT (NFR) specifies the quality attribute of a software system. They judge the software system based on Responsiveness, Usability, Security, Portability and other non-functional standards that are critical to the success of the software system. Example of non-functional requirement, “how fast does the website load?” Failing to meet non-functional requirements can result in systems that fail to satisfy user needs. Non- functional Requirements allow you to impose constraints or restrictions on the design of the system across the various agile backlogs.

Example, the site should load in 3 seconds when the numbers of simultaneous users are > 10000. Description of non-functional requirements is just as critical as a functional requirement.

1) Usability requirement
2) Serviceability requirement
3) Manageability requirement
4) Recoverability requirement
5) Security requirement
6) Data Integrity requirement
7) Capacity requirement
8) Availability requirement
9) Scalability requirement
10) Interoperability requirement
11) Reliability requirement
12) Maintainability requirement
13) Regulatory requirement
14) Environmental requirement

III. SYSTEM DESIGN

A. *System Architecture*

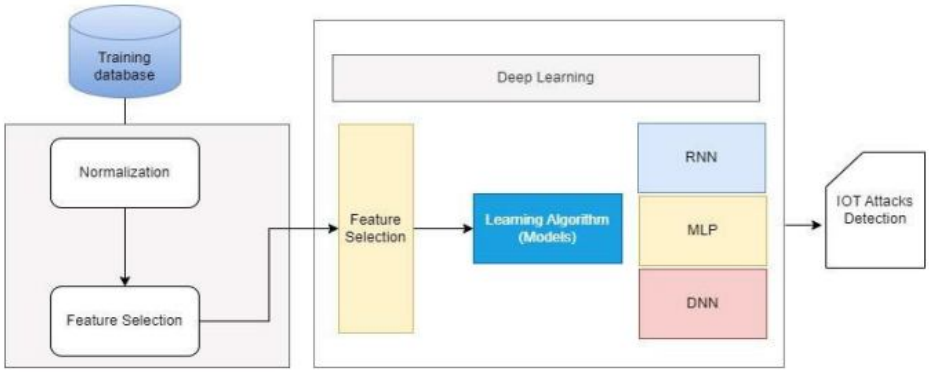


Fig.4.1.1 System architecture

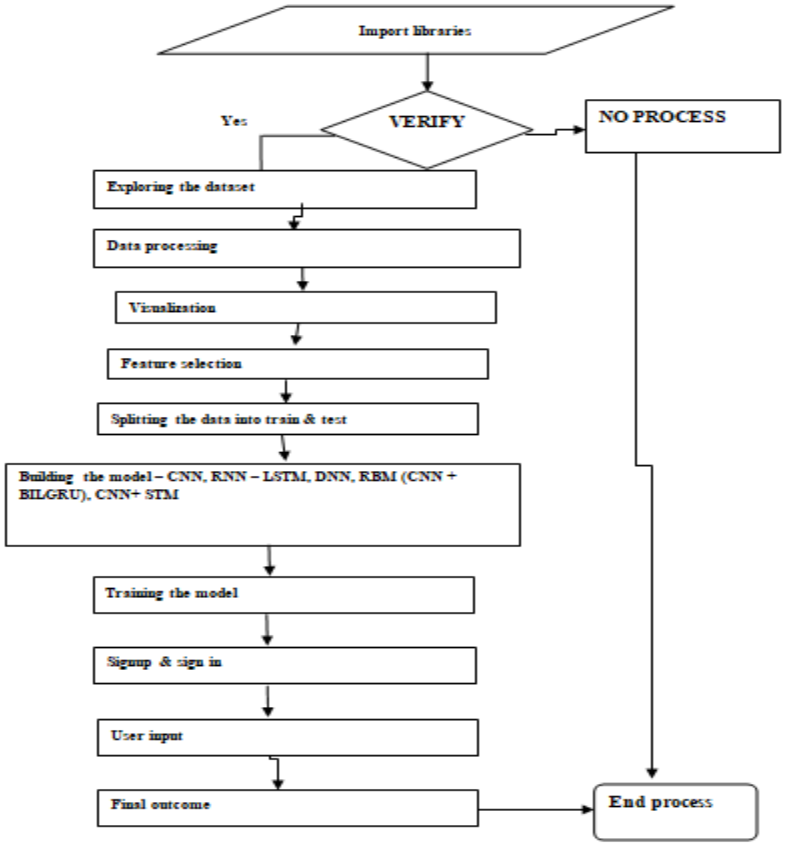
IV. DATA FLOW DIAGRAM

1) The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

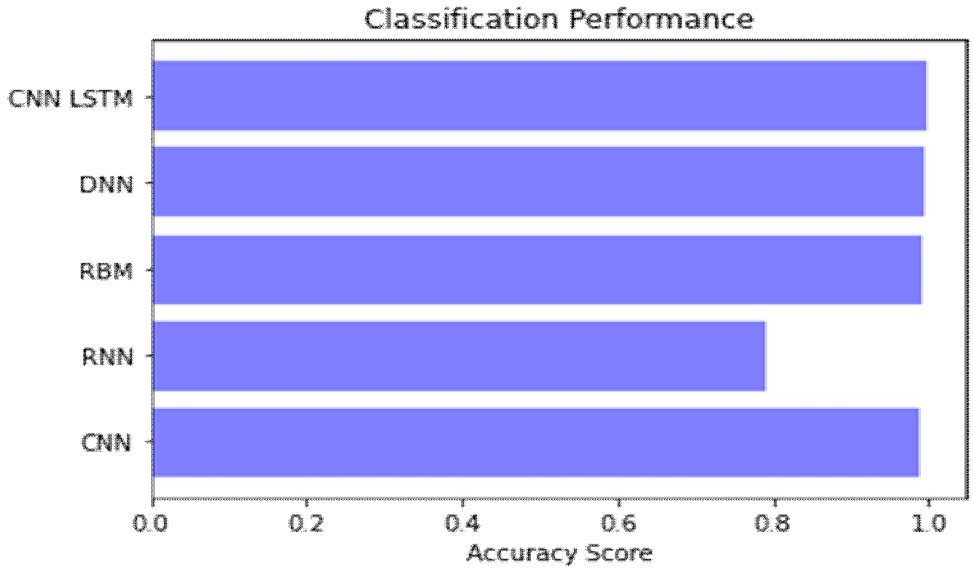
2) The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

3) DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

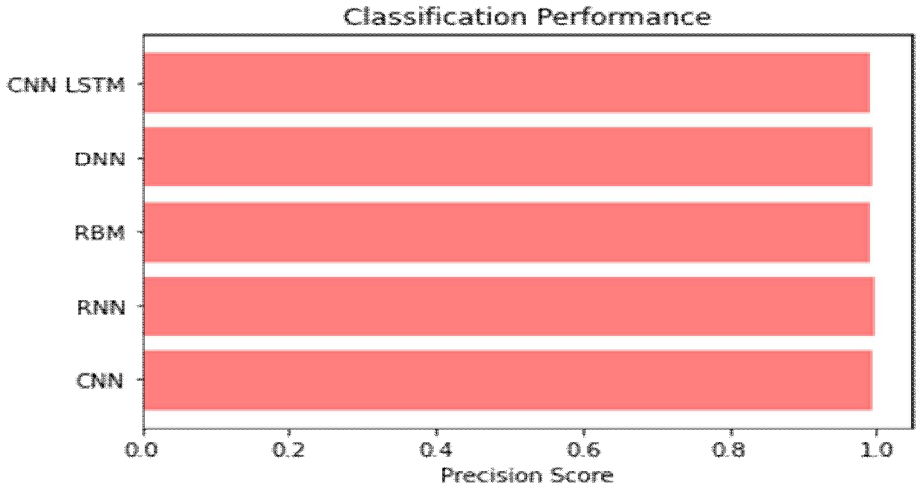
4) DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



V. RESULT



ACCURACY COMPARISON GRAPHS -KDDCUP99 DATASET

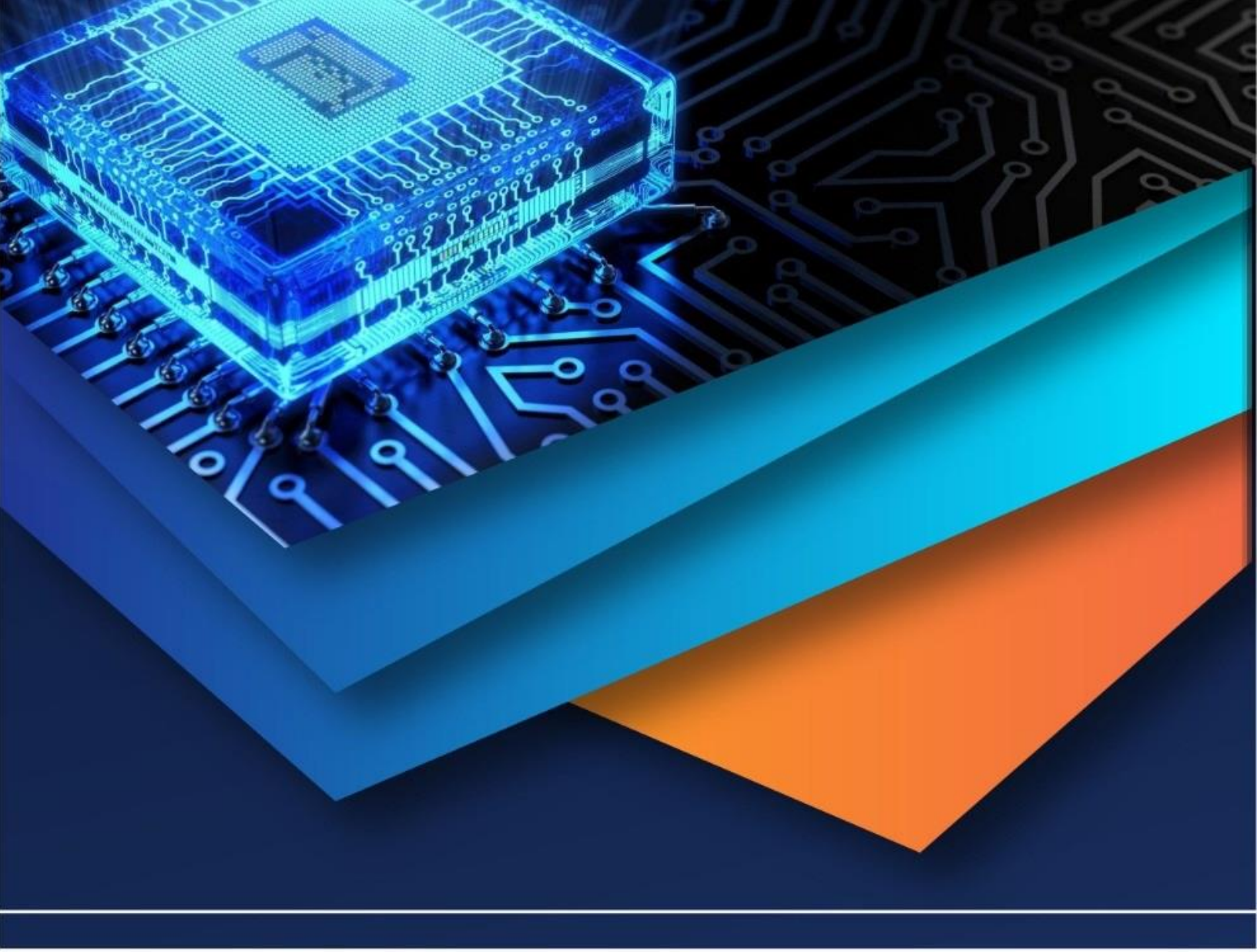


VI. CONCLUSION

This paper addresses challenges in using deep learning for early detection and eradication of cyber threats. It employs deep learning techniques for malware detection and summarizes approaches like RNN, CNN, DNN, and generative models. The experimental results demonstrate the effectiveness of the proposed IDS framework in detecting cybersecurity attacks. Future work includes extending the study to advanced deep learning methods and validating the system's robustness using IDS training.

REFERENCES

[1] Y. LeCun, Y. Bengio, and G. Hinton, 'Deep learning,' Nature, vol. 521, no. 7553, pp. 436–444, 2015.
[2] A. Krizhevsky, I. Sutskever, and G. H. Hinton, 'ImageNet classification with deep convolutional neural networks,' Commun. ACM, vol. 60, no. 2, pp. 84–90, Jun. 2017.
[3] M. K. Islam et al., 'Melanoma skin lesions classification using deep convolutional neural network with transfer learning,' in Proc. 1st Int. Conf. Artif. Intell. Data Analytics (CAIDA), Apr. 2021.
[4] A. Ahmim, M. Derdour, and M. A. Ferrag, 'An intrusion detection system based on combining probability predictions of a tree of classifiers,' Int. J. Commun. Syst., vol. 31, no. 9, p. e3547, Jun. 2018.
[5] A. Ahmim et al., 'A novel hierarchical intrusion detection system based on decision tree and rules-based models,' in Proc. 15th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS), May 2019, pp. 228–233.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY