The Deep Intru-Net for anomaly detection in massive IoT networks

The Deep Intru-Net for anomaly detection in massive IoT networks

A Review Report submitted to

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY

ANANTAPUR, ANANTAPURAMU

In partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

Submitted by

J JAYA PRAKASH (19HR1A0547) D CHIRANJEEVI (19HR1A0534)

B THEJASWINI (19HR1A0515) G TEJASREE (19HR1A0543)

Under the esteemed guidance of

Mrs.G.Lavanya, M.Tech

ASSISTANT PROFESSOR, CSE Department

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MOTHER THERESA INSTITUTE OF ENGINEERING AND TECHNOLOGY

Melumoi (Post), Palamaner-517408.

Approved by AICTE, New Delhi and Affiliated to JNTUA, Anantapuramu-515002

NAAC Accredited and An ISO 9001:2015 Certified Institution

2022-2023

The Deep Intru-Net for anomaly detection in massive IoT networks

GUIDE

Mrs. G. Lavanya M.Tech

Assistant professor

PRESENTED BY

J.Jaya Prakash (19HR1A0547)

D.Chiranjeevi (19HR1A0534)

B.Thejaswini (19HR1A0515)

G.Tejasree (19HR1A0543)

CONTENTS

ABSTRACT

The massive development of the internet of things enabled various applications in smart devices, mobiles, laptops, and equipment that are configured with the common internet to provide flexible access. numerous users benefited by the reliability of the internet as a common medium. on the similar scope of work, the intrusion attacks threaten the system security. The data stored in the cloud needs to be protected from network anomalies. The presented system is focused on development of novel deep learning architecture with tuned layers for better performance. The presented system considers the CICIDS2017 dataset. The system considers the CICIDS dataset as the reference information and creates an architecture using Deep Intru-Net to test. The dataset is divided into training data of 80% and testing data of 20%. The dataset holds the recorded patterns of network anomalies. The Deep Intru-Net learns the frequent pattern of anomaly in the network and detects the occurrence of similar patterns. The improved iterations increase the learning strength of the system. The performance evaluation is made using accuracy value estimation and the proposed network achieved 98% accuracy.

Keywords: Internet of things, smart devices, intrusion attacks, CICIDS , Deep Intru-Net, Accuracy.

INTRODUCTION

Smart devices, including smartphones, smartwatches, and other Internet of Things (IoT) devices, have become an essential part of our daily lives. These devices generate and store vast amounts of personal and sensitive data, making them an attractive target for cyber-attacks. Traditional security measures, such as firewalls and intrusion detection systems (IDS), are not always effective in detecting and preventing these attacks. Therefore, there is a growing need for more advanced security measures that can detect and prevent cyber-attacks on smart devices. Deep Intrusion Detection System (IDS) is a promising security measure that can detect and prevent cyber-attacks on smart devices. Deep IDS is a type of IDS that uses machine learning algorithms, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, to analyze network traffic and system activity data to identify patterns that indicate potential security threats. The system is designed to extract various features, such as statistical and behavioral features, from the raw data to identify patterns that indicate potential security threats.

RESEARCH GAP

Limited research on deep learning-based anomaly detection techniques Lack of comprehensive evaluation of the performance and scalability of The Deep Intru-Net: Limited research on the impact of varying IoT network characteristics on The Deep Intru-Net's performance: Lack of investigation into the interpretability and explainability of The Deep Intru-Net: Limited research on practical deployment and implementation

OBJECTIVE

The Deep Intru-Net for anomaly detection in massive IoT networks is to develop an efficient and scalable system that can accurately detect and mitigate anomalies or security breaches in massive IoT networks. The system aims to achieve the following objectives:

1. **Enhanced Anomaly Detection:** The system seeks to develop advanced deep learning-based models and algorithms that can effectively detect various types of anomalies in IoT networks, including known and unknown attacks, abnormal behavior patterns, and anomalous data traffic.

2. **Scalability and Efficiency:** The system aims to design a scalable and efficient architecture that can handle the massive volume of data generated by IoT devices in real-time or near real-time, while minimizing computational overhead and resource utilization.

3. **User-Friendly Interfaces:** The system aims to provide user-friendly interfaces and dashboards that offer meaningful insights and visualizations of the system's anomaly detection results, enabling security operators and administrators to easily monitor and manage the security of massive IoT networks.

EXISTING SYSTEM

In the context of MANER-Security, an assessment is made of the research work done on mobile ad-hoc network-based smart IDSS. They classified the data packets using an artificial neural network (ANN). ANN stands for artificial neural network. They said that categorization is a significant factor in the intrusion detection process. The development of a boat classifier may be seen here. It has been determined that the system is effective against uncommon assaults, DOS, and probing difficulties. They conducted research on a WiFi-enabled IoT home intrusion detection system. They integrated a detection algorithm into an identifying router based on received signal strength indicator (RSSI) and made it possible to see the status of the whole home's security system through the Internet of Things.

❑**DISADVANTGES:**

- ❑ Unstructured dataset
- ❑ Detection time is more

PROPOSED SYSTEM

The Deep Intru-Net is an AI-based system that uses deep learning algorithms to detect anomalies in massive IoT networks. The system is designed to work with large-scale networks that may have millions of connected devices generating massive amounts of data.

•The system has three main components:

•Data Preprocessing: The raw data generated by IoT devices is preprocessed to remove any noise or errors. The preprocessing step may include data cleaning, filtering, and normalization.

• Feature Extraction: The preprocessed data is then transformed into features that can be used by the deep learning algorithms. The feature extraction step may include statistical analysis, signal processing, and other techniques to extract relevant features from the data.

•Deep Neural Network: The system uses a deep neural network to learn the normal behavior patterns of the IoT network. The deep neural network is trained using the features extracted from the preprocessed data. Once trained, the neural network can identify any deviations from the learned patterns and flag them as anomalous behavior.

ADVANTAGES

- Deep learning architecture is created
- Accuracy is improved
- Scalability is improved

SYSTEM REQUIREMENTS

- **HARDWARE REQUIREMENTS**:
  - Operating System: Windows 10, 8.1, 7 Service Pack 1
  - Processor: Minimum Intel or AMD x86-64 processor with four logical cores and AVX2 instruction set support
  - RAM: 8 GB

❑SOFTWARE REQUIREMENTS:

- MATLAB 2017
- Toolbox utilized:
  - ❑ IMAGE PROCESSING
  - ❑ STATISTICS AND NEURAL NETWORKS
  - ❑ SIGNAL PROCESSING
  - ❑ DEEP LEARNING

METHODOLOGY

Object oriented methodology is a system development approach encouraging and facilitating re-use of software components. With this methodology, a computer can be developed on a component basis which enables the effective reuse of existing components and facilitates the sharing of its components by other systems. It employs international standard unified modelling language (UML) from the object management group (OMG) .Using this methodology , a system can be developed on a component basis , which enables the effective reuse of existing components, it facilitates the sharing of its other system components. Objects oriented methodology asks the analyst to determine what the objects of the system are?, what responsibilities and relationships an object has to with the other objects? And how they behave over time?

RESULTS & DISCUSSIONS

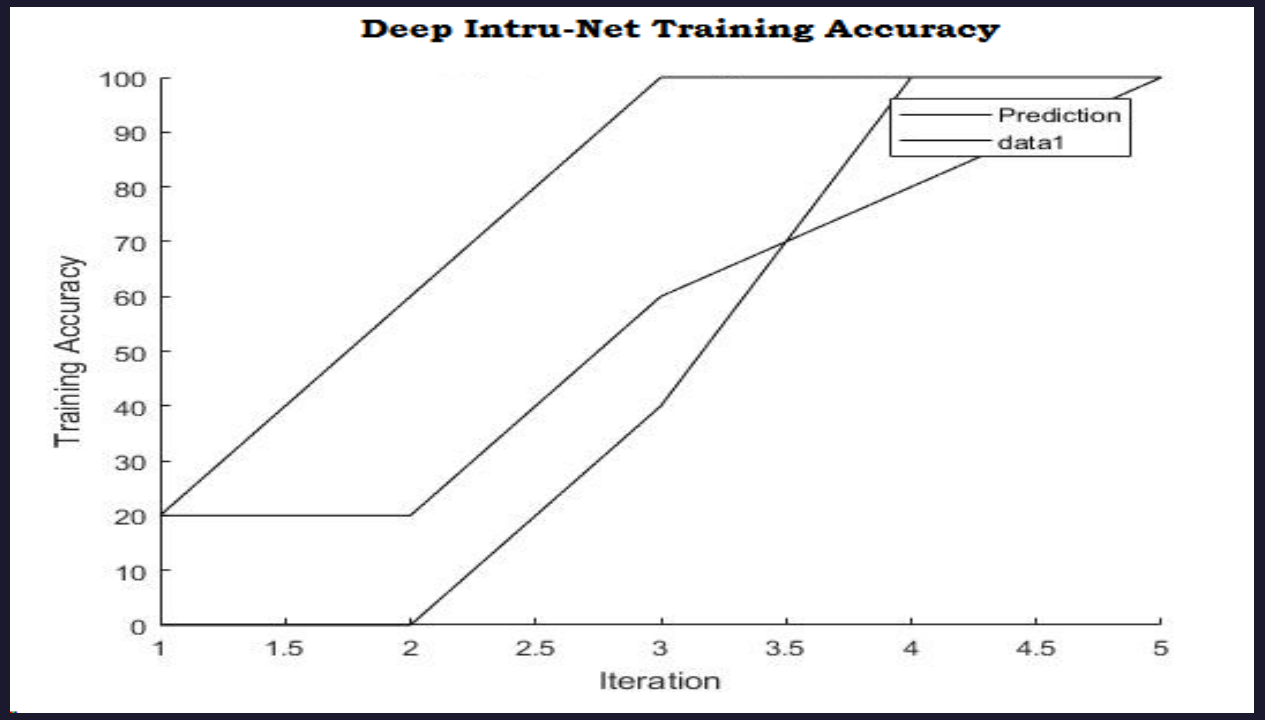

Fig 1.Shows the Deep Intru-Net training accuracy at different iterations are depicted here.

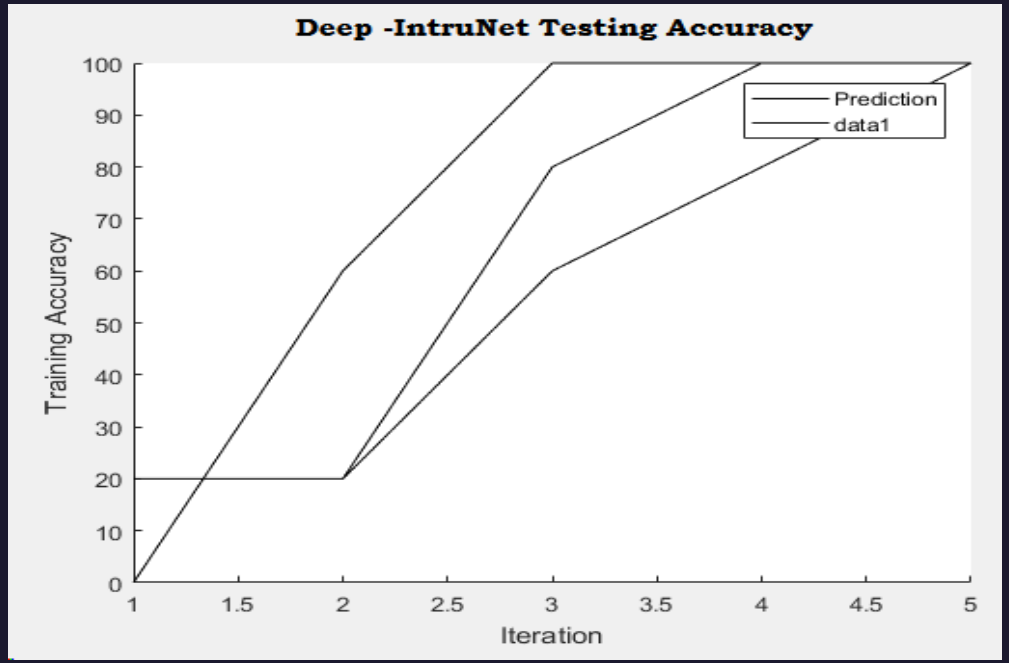

Fig 2. Shows the Deep Intru-Net testing accuracy at different ranges of iterations are depicted here.

CONCLUSION

The widespread growth of the internet of things made it possible for a variety of apps to be installed in smart devices, mobile devices, laptops, and other pieces of equipment that are set to allow flexible access to the internet. There have been a lot of people who have benefitted from the dependability of the internet as a common medium. On the same scale of operations, the intrusion assaults pose a danger to the system's level of security. The data that is kept in the cloud has to have some kind of defense against network irregularities. The primary emphasis of the system that is now being presented is the construction of a revolutionary deep learning architecture that features layers that have been optimized to improve performance. The CICIDS2017 dataset is taken into account by the system that is provided. The CICIDS dataset is taken into account by the system as the reference information, and Deep Intru-Net is used to do testing on the architecture that is developed. The dataset is split into training data comprising 80% of the total and testing data making up the remaining 20%. The documented patterns of network irregularities are included in the dataset. The Deep Intru-Net is able to understand the common pattern of anomaly that occurs in the network and recognize when other patterns with the same characteristics arise. The capacity of the system to learn is increased as a result of the better iterations.

REFERENCES

- Sheikh Tahir Bakhsh , Saleh Alghamdi, Rayan A Alsemmeari and Syed Raheel Hassan, 2019., in open access journal, SAGE, Soft Comp. in IDS.,
- [2] A-Krishna, ALMAA J-Matheiwkutty, DS.-Jacob and HM, "Research on Intrusion Detection & Prevention model Using Deep Learning," 2020 Int. Conf..,((ICESC),(2020,)
- [3] A.-Ali and MM.Yousaf-, "., Research entitled Novel triple Intrusion Detec. & safe Gaurd System in SDN..," in IEEE Open-Access Year 2020.,
- [4] Zhigang Huang.,, Leii Zhangg., “. Key authentication protocols against smart connected devices.,”, IEEE 2019 published.
- [5] Rafał-Kozik & Michałl-Chorass., “.,Machine learning tech., Springer –Int. Published 2014.,

ACKNOWLEDGEMENT

I am grateful to all of those with whom I have had the pleasure to work during this journal and other related projects. Each of the members of my Dissertation Committee has provided me extensive personal and professional guidance and taught me a great deal about both scientific research and life in general to the completion of my project journal titled “**The Deep Intru-Net for anomaly detection in massive IoT networks**”.

Thank You !