International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

DEEP LEARNING MODELS FOR THE RECOGNITION OF HARMFUL ATTACK ACTIVITIES IN IOT

[1]S.Ramya

[1]Assistant Professor in Department of CSE Sri Indu College Of Engineering And Technology

[1]ramya95sakilam@gmail.com

Abstract

IICSs, which integrate technical systems with physical systems to provide services to businesses, have become a new area of study due to their susceptibility to cyber-attacks that could compromise their ability to continue providing services to businesses. For businesses, potential hazards result in revenue loss and reputational risk. Despite the factor protection against them, it is difficult to collect data for the purpose of building a wise NIDS that can effectively recognize both current and novel attacks.In this work, weproposes an anomalies recognition system for IICSs using DL algorithms that may train and evaluate data obtained from TCP/IP package in order to address this problem. A well network datasets NSL-KDD & UNSW-NB15 are used to assess the training courses for deep auto-encoder(DAE) and deep feed-forward NN (DFFNN) designs. The research findings result that this methodology could be used in actual IICS situations because it has a lower false positive rate & a greater detection accuracy compared to previous methods.

KEYWORDS: IIOT, Deep Feed Forward Neural Network, IICS, Deep-auto encoder

I INTRODUCTION

The web has altered how individuals and organizations connect and perform online business, making cyberspace essential to modern communities and economy. The new word "IIoT" now refers to a wide range of programs, systems, and services that connect the digital and physical worlds. Businesses are becoming more concerned about safeguard critical system, or IICSs, as IIoT applications & devices proliferate. Among the most common hazards in IIoT networks is spyware, which attackers use to infect important equipment in order to take control of and change their functionality to use a variety of approaches, such as Distributed Denial of Service (DDoS), DoS, and Advanced Persistent Threat (APT).A internet connected devices can be monitored to spot suspicious

behavior using this software or hardware solution. The latter can recognise both well-known and fresh attacks, but it can also spot recent incursions by comparing upcoming regulations and signatures to a blacklist of its known rules. The former can spot both well-known and novel threats, but it also generates a lot of errors.In order to as much as possible mitigate the drawback of FPRs, we present an effective Anomaly Detection System (ADS) for IICSs in this work.

II LITERATURE SURVEY

Soft computing and IoT based solar tracker:

The significance of the solar energy is to intensify the effectiveness of the Solar Panel with the use of a primordial solar tracking system. Here we propounded a solar positioning system with the use of the global positioning system (GPS) , artificial neural network (ANN) and image processing (IP) . The azimuth angle of the sun is evaluated using GPS which provide latitude, date, longitude and time. The image processing used to find sun image through which centroid of sun is calculated and finally by comparing the centroid of sun with GPS quadrate to achieve optimum tracking point. Weather conditions and situation observed through AI decision making with the help of IP algorithms. The presented advance adaptation is analyzed and established via experimental effects which might be made available on the memory of the cloud carrier for systematization. The proposed system improve power gain by 59.21% and 10.32% compare to stable system (SS) and two-axis solar following system (TASF) respectively. The reduced tracking error of IoT based Two-axis solar following system (IoT-TASF) reduces their azimuth angle error by 0.20 degree.

Modeling and Simulation of Hybrid System

The article presented is a simulation, modeling and designing of a hybrid power generation system which is based on non-conventional (renewable) wind turbine energy and solar photovoltaic reliable sources. The primary system is the solar electric generator, which consist of six models and connected to each other in series, based on predicted P&O and is connected to a MPPT controller and AC/DC converter, system is associated with Permanent Magnet Synchronous Generator. The main purpose this article is serving is to interconnect system so that it generates maximum power for single auxiliary phase loading, and the solar PV generator and systems of wind turbines for simulation with using Simulink/ MATLAB. The result of this simulation indicates that the hybrid power system is planned for efficiency, stability, reliability and model. Wind Turbine and Solar

PV from the use of a renewable energy source for maximum voltage generation. The solar photovoltaic saturation flow and an ideal factor.

Secure IoT Platform for Industrial Control Systems:

Supervisory control and data acquisition (SCADA) systems, are part of industrial control system (ICS), have been playing crucial roles in real-time industrial automation and controls. Internet of things (IoT) is a ubiquitous platform, a new advance enhancement, for efficient SCADA system, where billions of network devices, with smart sensing capabilities, are networked over the Internet access. Deployment of smart IoT platform, SCADA system will significantly increase system efficiency, scalability, and reduce cost. Security is still a major issue for both-, as they were initially designed without any priority and requirements of security. This study modeled IoT-SCADA system and deployed a security mechanism, employing of cryptography based algorithm, which provided a secure transmission channel while each time communication occurred, between the field devices in the SCADA system. Proposed security implementation, and computed measurements analyzed as potential security building block against authentication and confidentiality attacks

A Survey: Intrusion Detection System for Internet Of Things:

The Internet of Things (IoT) is an ever-growing network of smart objects. It refers to the physical objects are capable of exchanging information with other physical objects. It introduces various services and human‟s routine life depends on its available and reliable activities. Therefore, the challenge of implementing secure communication in the IoT network must be addressed. The IoT network is secured with encryption and authentication, but it cannot be protected against cyber-attacks. Hence, the Intrusion Detection System (IDS) is needed. In this paper, we discuss some security attacks and various intrusion detection approaches to mitigate those attacks.

III EXISTING SYSTEM

In literature they design and develop a novel anomaly-based intrusion detection model for IoT networks.First, a convolutional neural network model is used to create a multiclass classification model. Their model is then implemented using convolutional neural networks in 1D, 2D, and 3D. Their convolutional neural network model is validated using the BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23 intrusion detection datasets. Transfer learning is used to implement binary and multiclass classification

using a convolutional neural network multiclass pre-trained model. In another research they present a novel Deep Learning (DL)-based intrusion detection system for IoT devices. Their intelligent system uses a four-layer deep Fully Connected (FC) network architecture to detect malicious traffic that may initiate attacks on connected IoT devices. Their system has been developed as a communication protocol-independent system to reduce deployment complexities.

Disadvantages

The existing work utilizes convolutional neural networks (CNNs) in 1D, 2D, and 3D for intrusion detection. While CNNs can be powerful, they may introduce unnecessary complexity and overhead, especially for IoT networks.

- The existing work validates its model on specific intrusion detection datasets like BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, and IoT-23. This may limit the generalizability of the model to diverse IICS scenarios.
- The existing work employs transfer learning for binary and multiclass classification, utilizing a pre-trained CNN model. However, this approach may not fully capture the unique characteristics and complexities of IICSs.

IV PROBLEM STATEMENT

The proposed Project for detect Anomaly and DDos Attacks including the dataset, pre-processing, feature extraction and feature selection, algorithms, framework, and evaluation metrics, is presented and discusses the evaluation results of the experiments performed, and finally concludes the project with framework detect of different network attacks.

V PROPOSED SYSTEM

We propose an anomaly recognition system for IICSs utilizing DL algorithms that may train and assess data acquired from TCP/IP package. DL methods are used, together with self-dimension reduces and a respectable depiction of typical non SL network topologies. We evaluate the training programs for deep auto-encoder and deep feed-forward (FF) NN designs using the well network datasets NSL-KDD & UNSW-NB15.The DFFNN is employed to identify hazardous vectors throughout test. The effectiveness of the applied DAEDFFNN model is enhanced by the successful construction and extraction of key features.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

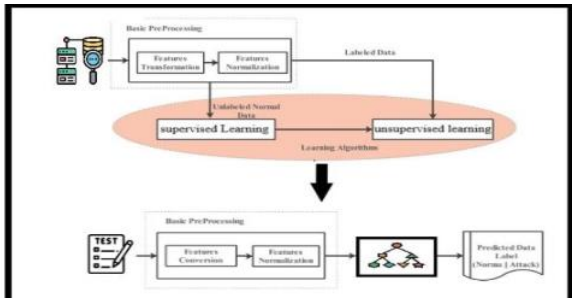
Advantages

1. We employs deep auto-encoder and deep feed-forward neural networks (DFFNN), which are more tailored for data reduction and pattern recognition, making them potentially more suitable for IICSs.

2. Our work, on the other hand, evaluates its methods using well-established network datasets NSL-KDD and UNSW-NB15, which are more commonly used in the field and could provide a better benchmark for performance evaluation.

3. We directly utilize deep auto-encoder and DFFNN models, potentially providing a more specialized and effective approach for anomaly recognition within IICSs.

VI ARCHITECTURE



System architecture

VII IMPLEMENTATION

Data exploration: using this module we will load data into system

Processing: Using the module we will read data for processing

Splitting data into train & test: using this module data will be divided into train & test

Model generation: Model building - Deep Feed Forwarding Neural Network, Auto Encoder DNN, CNN, CNN + LSTMUser signup & login: Using this module will get registration and login

User input: Using this module will give input for prediction

Prediction: final predicted displayed Note: As an extension we applied an ensemble method combining the predictions of multiple individual models to produce a more robust and accurate final prediction.However, we can further enhance the performance by exploring other ensemble techniques such as CNN and CNN + LSTM will give 97% of accuracy.

Algorithms:

Deep Feed Forwarding Neural Network: A feed-forward neural network, in which some routes are cycled, is the polar opposite of a Recurrent Neural Network. The feed-forward model is the basic type of neural network because the input is only processed in one direction. DNNs can model complex non-linear associations. In this site, we will mention two different types of DNN architectures, the multi-layer perceptron

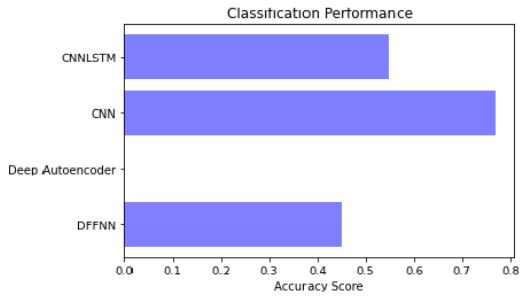
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

neural network (MLPNN) and the stacked autoencoder (SAE).

CNN: Convolutional Neural Network (CNN) is a type of deep learning algorithm that is particularly well-suited for image recognition and processing tasks. It is made up of multiple layers, including convolutional layers, pooling layers, and fully connected layers.

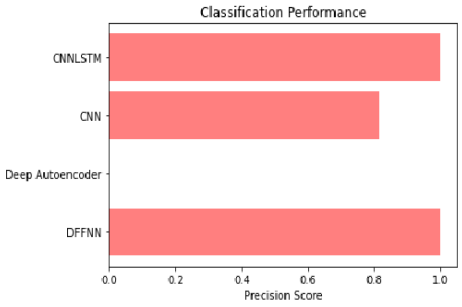
Long Short-Term Memory Networks (LSTM) - LSTM models are a subtype of Recurrent Neural Networks. They are used to recognize patterns in data sequences, such as those that appear in sensor data, stock prices, or natural language.

VIII RESULTS

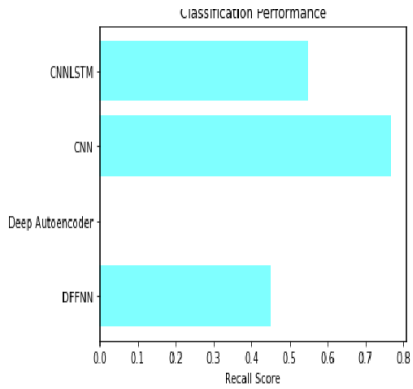


Accuracy Comparison Graphs Of Bot-Iot Dataset

PRECISION COMPARISON GRAPHS OF BOT-IOT DATASET

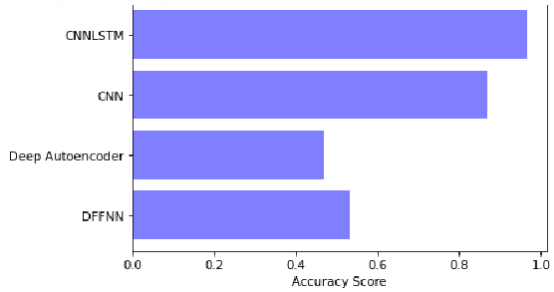


Precision Comparison Graphs Of Bot-Iot Dataset

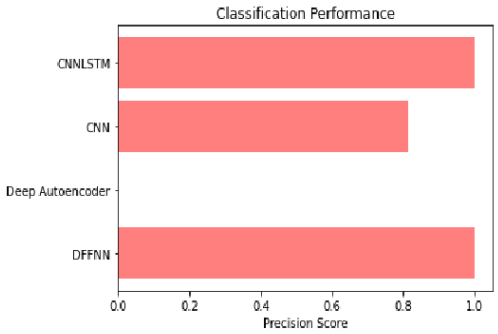


Recall Comparison Graphs Of Bot-Iot Dataset

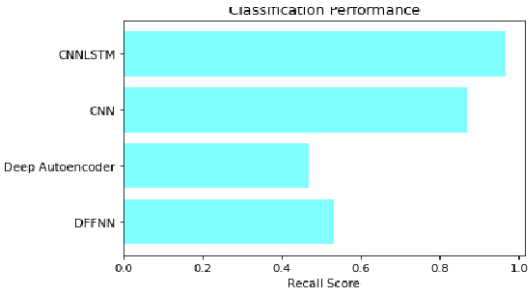
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362



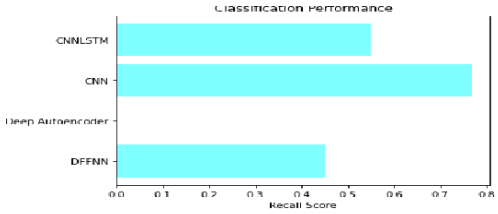
Accuracy Comparison Graphs Of Nsl Kdd Dataset



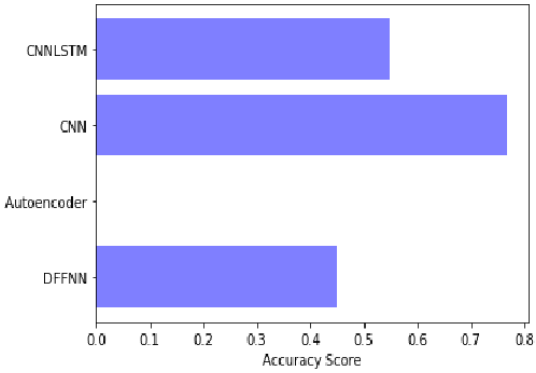
Precision Comparison Graphs Of Unsw-Nb15 Dataset



Recall Comparison Graphs Of Nsl Kdd Dataset



Recall Comparison Graphs Of Unsw-Nb15 Dataset



Accuracy Comparison Graphs Of Unsw-Nb15 Dataset

Result: Attack is Detected and its DOS Attack!

IX CONCLUSION

An ADS approach for recognizing invasive activities in IIoT environments is presented in this work using data from TCP/IP communication. DL methods are used, together with self-dimension reduces and a respectable depiction of typical non SL network topologies. Effective parameters are obtained for a supervised training for DFFNN as opposed to random ones. Then, the supervised DFFNN is used to adjust these variables even more. The effectiveness of the applied DAEDFFNN model is enhanced by successful construction and extraction of key features. The final model built exceeds prior established techniques, delivering the greatest detection accuracy and the fewest false alarms when evaluated on numerous sets of data from the NSL-KDD and NSW-NB15 databases

REFERENCES

[1] Sherasiya T, Upadhyay H, Patel H. A survey: intrusion detection system for in- ternet of things. J. Comput Sci Eng 2016;5:91–8.

[2] Drath R, Horch A. Industry 4.0: hit or hype? [Industry forum]. IEEE Ind Electron Mag 2014:56–8.

[3] Shahzad A, Kim G, Elgamoudi A. Secure IoT platform for industrial control sys- tems. In: Platform technology and service (PlatCon), international conference on. IEEE; 2017. p. 1–6.

[4] Katsikeas S, Fysarakis K, Miaoudakis A, Van Bemten A, Askoxylakis I, Papaef- stathio I, Plemenos A. Lightweight and secure industrial IoT communications via the MQ telemetry transport protocol. Symposium on computers and com- munications conference. IEEE; 2017.

[5] Stouffer K, Falco J, Scarfone K. Guide to industrial control systems (ICS) secu- rity. NIST special publication; 2011. p. 6–16.

[6]Atlantic Council. http://publications.atlanticcouncil.org/cyberri sks//.

[7] Sitnikova E, Foo E, Vaughn B. The power of hands-on exercises in SCADA cyber security education. In: IFIP world conference on information security educa- tion. Springer; 2009. p. 83–94.

[8] Abraham A, Grosan C, Martin-vide C. Evolutionary design of intrusion detec- tion. Int J Netw Secur 2007:328–39.

[9] Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M. A survey of intru- sion detection techniques in cloud. J Netw Comput Appl 2013:42–57.