A

Major Project On

**TRUSTWORTHY AND RELIABLE DEEP LEARNING BASED CYBERATTACK DETECTION IN INDUSTRIAL IOT**

(Submitted in partial fulfillment of the requirements for the award of Degree)

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

K. Anil Kumar (217R1A05A1)

S. Rahul (217R1A05C0)

K. Tejeshwar Rao (217R1A0596)

Under the Guidance of

###### CH. REKHA

(Assistant Professor)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

###### CMR TECHNICAL CAMPUS

**UGC AUTONOMOUS**

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH,Approved by AICTE, New Delhi) Recognized Under Section 2(f) & 12(B) of the UGC Act.1956,

Kandlakoya (V), Medchal Road, Hyderabad-501401.

**2021-25**

### DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

****

**CERTIFICATE**

This is to certify that the Mini Project Report entitled “TRUSTWORTHY AND RELIABLE DEEP LEANING BASED CYBERATTACK DTECTION IN INDUSTRIAL IOT” being submitted by **K. ANIL KUMAR (217R1A05A1), S. RAHUL (217R1A05C0) & K. TEJESHWAR RAO (217R1A0596)** in partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in **COMPUTER SCIENCE AND ENGINEERING** to the **Jawaharlal Nehru Technological University , Hyderabad** is a record of bonafide work carried out by them under my guidance and supervision during the academic year 2024-25.

The results embodied in this project have not been submitted to any other University or Institute for the award of any degree or diploma.

CH. REKHA Dr. A. Raji Reddy

**Assistant Professor DIRECTOR**

**INTERNAL GUIDE**

Dr. Nuthanakanti Bhaskar EXTERNAL EXAMINER HOD

**Submitted for viva voice Examination held on**

Apart from the efforts of us, the success of any project depends largely on the encouragement and guidelines of many others. We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project. We take this opportunity to express my profound gratitude and deep regard to my guide

**CH. Rekha** Assistant Professor for her exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by her shall carry us a long way in the journey of life on which we are about to embark. We also take this opportunity to express a deep sense of gratitude to Project Review Committee (PRC) Coordinators: **Dr. K. Maheshwari, Dr. J. Narasimha Rao, Ms. K. Shilpa, Mr. K. Ranjith Reddy** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. Nuthanakanti Bhaskar,** Head of the Department of Computer Science and Engineering for providing encouragement and support for completing this project successfully.

We are obliged to **Dr. A. Raji Reddy,** Director for being cooperative through out the course of this project. We would like to express our sincere gratitude to Sri. **Ch. Gopal Reddy,** Chairman for providing excellent infrastructure and a nice atmosphere throughout the course of this project.

The guidance and support received from all the members of **CMR Technical Campus** who contributed to the completion of the project. We are grateful for their constant support and help.

Finally, we would like to take this opportunity to thank our family for their constant encouragement, without which this assignment would not be completed. We sincerely acknowledge and thank all those who gave support directly and indirectly in the completion of this project

**K. ANIL KUMAR (217R1A05A1)**

**S. RAHUL (217R1A05C0)**

**K. TEJESHWAR RAO (217R1A0596)**

A fundamental expectation of the stakeholders from the Industrial Internet of Things (IIoT) is its trustworthiness and sustainability to avoid the loss of human lives in performing a critical task. A trustworthy IIoT-enabled network encompasses fundamental security characteristics, such as trust, privacy, security, reliability, resilience, and safety. The traditional security mechanisms and procedures are insufficient to protect these networks owing to protocol differences, limited update options, and older adaptations of the security mechanisms. As a result, these networks require novel approaches to increase trust level and enhance security and privacy mechanisms. Therefore, in this article, we propose a novel approach to improve the trustworthiness of IIoT-enabled networks. The proposed scheme combines the deep learning- based pyramidal recurrent units (PRU) and decision tree (DT) with SCADA-based IIoT networks. We also use an ensemble-learning method to detect cyberattacks in SCADA-based IIoT networks.

**FIGURE NO FIGURE NAME PAGE NO**

Figure 3.1 Project Flow Chart 7

Architecture

Figure 3.3 Use case diagram for 9

Cyberattack detection

Figure 3.4 Class diagram for 10

Cyberattack detection

Figure 3.5 Sequence diagram for 11

Cyberattack detection

Figure 3.6 Activity diagram for 12

Cyberattack detection

ABSTRACT i

LIST OF FIGURES ii

INTRODUCTION 1

* 1. PROJECT SCOPE 1
  2. PROJECT PURPOSE 1
  3. PROJECT FEATURES 1

1. SYSTEM ANALYSIS 2
   1. PROBLEM DEFINITION 2
   2. EXISTING SYSTEM 2
      1. LIMITATIONS OF THE EXISTING SYSTEM 3
   3. PROPOSED SYSTEM 3
      1. ADVANTAGES OF PROPOSED SYSTEM 4
   4. FEASIBILITY STUDY 4
      1. ECONOMIC FEASIBILITY 4
      2. TECHNICAL FEASIBILITY 5
      3. SOCIAL FEASIBILITY 5
   5. HARDWARE & SOFTWARE REQUIREMENTS 5
      1. HARDWARE REQUIREMENTS 5
      2. SOFTWARE REQUIREMENTS 6
2. **ARCHITECTURE** 7
   1. [PROJECT ARCHITECTURE 7](#_TOC_250013)
   2. DESCRIPTION 8
   3. [USE CASE DIAGRAM 9](#_TOC_250011)
   4. [CLASS DIAGRAM 10](#_TOC_250010)
   5. [SEQUENCE DIAGRAM 11](#_TOC_250009)
   6. [ACTIVITY DIAGRAM 12](#_TOC_250008)

# INTRODUCTION

## INTRODUCTION

### PROJECT SCOPE

This project focuses on creating a deep learning-based cyberattack detection system designed specifically for Industrial Internet of Things (IIoT) environments. The system aims to monitor and analyze network traffic in real-time to identify and classify various cyberattacks, such as malware, Distributed Denial of Service (DDoS), data tampering, and unauthorized access attempts.

### PROJECT PURPOSE

The purpose of this project is to strengthen cybersecurity in IIoT environments by leveraging the advanced capabilities of deep learning. Unlike traditional rule-based or signature-based approaches, the proposed system will utilize neural networks to identify both known and novel threats with higher accuracy. This approach aims to enhance the overall security posture of IIoT systems, ensuring uninterrupted industrial operations and safeguarding sensitive data.

### PROJECT FEATURES

The system will feature an intelligent threat detection engine powered by deep learning models, capable of analyzing large volumes of IIoT network traffic in real-time. It will include an adaptive mechanism to learn from new attack patterns, ensuring continuous improvement in detection capabilities. The solution will also provide a user-friendly interface for monitoring and managing threats, along with real-time alerts and detailed analytics..

# SYSTEM ANALYSIS

2. SYSTEM ANALYSIS

### SYSTEM ANALYSIS

The proposed system for cyberattack detection in Industrial Internet of Things (IIoT) involves analyzing the current challenges, functional requirements, and technological solutions to address cybersecurity threats effectively. This section provides an in-depth analysis of the system’s components, feasibility, and operational goals.

### PROBLEM DEFINITION

The rapid integration of Industrial Internet of Things (IIoT) technologies has revolutionized industrial processes by enabling interconnected systems, real-time monitoring, and automation. However, this digital transformation has also made IIoT environments increasingly susceptible to sophisticated cyberattacks. These attacks, including malware, ransomware, Distributed Denial of Service (DDoS), and data tampering, can disrupt operations, compromise sensitive data, and cause significant financial and reputational damage.

### EXISTING SYSTEM

The Internet of Things (IoT) has revolutionized modern tech with interconnected smart devices. While these innovations offer unprecedented opportunities, they also introduce complex security challenges. Cybersecurity is a pivotal concern for intrusion detection systems (IDS). Deep Learning has shown promise in effectively detecting and preventing cyberattacks on IoT devices. Although IDS is vital for safeguarding sensitive information by identifying and mitigating suspicious activities, conventional IDS solutions grapple with challenges in the IoT context. This paper delves into the cutting-edge intrusion detection methods for IoT security, anchored in Deep Learning.

### LIMITATIONS OF EXISTING SYSTEM

* The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cyber Attacks.
* Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient quantities, then model accuracy may suffer.
* Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

### PROPOSED SYSTEM

By considering the limitations of previous techniques, we employ network attributes of industrial protocols and propose a pyramidal recurrent unit (PRUs)- and decision tree (DT)-based ensemble detection mechanism. The proposed mechanism has the potential to detect cyberattacks in any extensive industrial network. The interoperability with other detection engines and expandability for a wider industrial network with multiple areas distinguishes the proposed mechanism from previous studies. The proposed detection method is disseminable across many IIoT domains. Furthermore, our model is straightforward to implement and deploy and can improve efficiency and accuracy while overcoming the shortcomings of previous efforts.

### ADVANTAGES OF THE PROPOSED SYSTEM

##### We propose a scalable and efficient DL- and DT-based ensemble cyber-attack detection framework to resolve trustworthiness issues in the SCADA-based IIoT networks.

##### We present an efficient probing approach by the SCADAbased network data to solve the protocol mismatch limitations of traditional security solutions for the IIoT platform.

* A statistical analytic approach for ensuring the trustworthiness and reliability of the proposed model for SCADA based IIoT networks.

### FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

* ECONOMICAL FEASIBILITY
* TECHNICAL FEASIBILITY
* SOCIAL FEASIBILITY

### ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

### 

### TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

### 2.4.3 SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

### 2.5 HARDWARE & SOFTWARE REQUIREMENTS

### 2.5.1 HARDWARE REQUIREMENTS:

➢ **H/W System Configuration:-**

➢  **Processor** - Pentium –IV

➢ **RAM** - 4 GB (min)

➢ **Hard Disk** - 20 GB

➢ **Key Board** - Standard Windows Keyboard

➢ **Mouse** - Two or Three Button Mouse

➢  **Monitor** - SVGA

### 2.5.2 SOFTWARE REQUIREMENTS:

* **S/W System Configuration:-**
* **Operating system :** Windows 7 Ultimate.
* **Coding Language** : Python
* **Front End**  : Python
* **Back End**  : Django - ORM
* **Designing** : HTML, CSS, Javascript
* **Data Base** : MySQL(WAMP Server)

# ARCHITECTURE

3. ARCHITECTURE

**3.1 PROJECT ARCHITECTURE**

This project architecture shows the procedure followed for classification, starting from input to final output.

Service Provider

Login,

Train & Test Datasets,

View Trained and Tested Datasets Accuracy in Bar Chart,

View Trained and Tested Accuracy Results,

View Prediction Of Cyber Attack Type,

View Cyber Attack Type Ratio,

Download Predicted Data Sets,

View Cyber Attack Type Ratio Results,

View All Remote Users.

Accepting all Information

**Web Server**

Datasets Results Storage

Accessing Data

Process all user queries

**WEB Database**

Remote User

Tweet Server

Tweet Server

Tweet Server

REGISTER AND LOGIN,

PREDICT CYBER ATTACK TYPE,

VIEW YOUR PROFILE.

Figure 3.1: Project Flow Chart Architecture

### 3.2 DESCRIPTION

The system architecture is designed to facilitate a deep learning-based cyberattack detection system for Industrial IoT (IIoT) environments. It consists of four main components:

**Service Provider**:

The Service Provider acts as the central control unit. It manages user authentication, dataset training and testing, cyberattack predictions, and result visualization, including accuracy in bar charts and attack type ratios. Users can also download prediction results and view remote user activity.

**Web Server**:

The Web Server serves as an intermediary between users, the Service Provider, and the Web Database. It processes user queries, accepts datasets, and forwards requests for prediction or analysis.

**Web Database**:

The Web Database securely stores all datasets, trained results, cyberattack logs, and prediction outcomes. It processes and retrieves data as needed, ensuring data persistence and easy access for system operations.

**Remote User Tweet Server**:

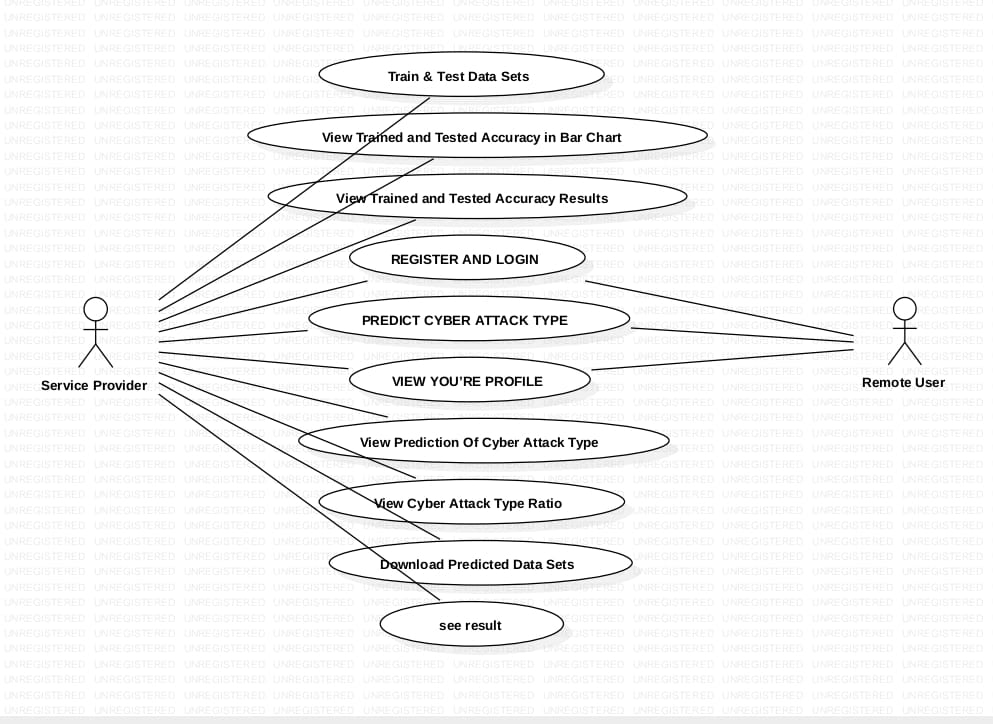
Remote users can register, log in, predict cyberattack types, and view their profiles. This component enables external access to the system for real-time interaction and prediction services.

The architecture ensures smooth communication between components, efficient data storage, and accurate cyberattack detection, making it scalable, reliable, and suitable for IIoT environments.

.

### 3.3 USE CASE DIAGRAM

In the use case diagram we have basically two actors who are the user and the system. The user has the rights to login, access to resources and to view the results. Whereas the system has the login, access to resources of the users and also the right to update and remove the details, and system can also view the user files.



##### Figure 3.3: Use Case Diagram for Cyberattack detection

A UML use case diagram is a behavioral diagram from use-case analysis that provides a graphical overview of system functionality, showing actors, their goals (use cases), and dependencies between these goals.

### 3.4 CLASS DIAGRAM

##### Class Diagram is a collection of classes and objects.

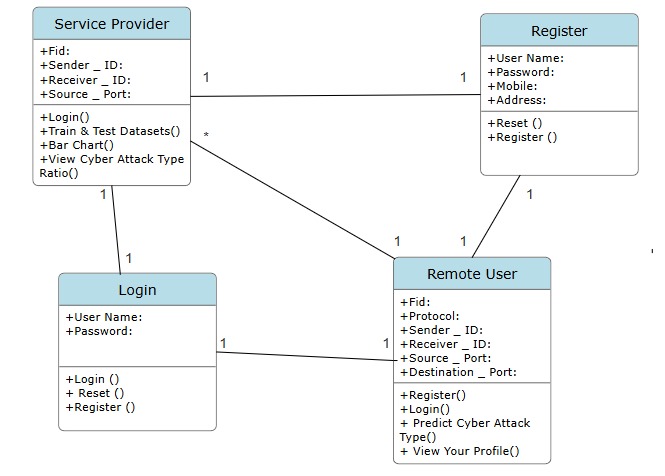


Figure 3.4: Class Diagram for Cyberattack detection

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

### 3.5 SEQUENCE DIAGRAM

##### WhatsApp Image 2024-12-18 at 01.20.19_90ff27cc

##### Figure 3.5: Sequence Diagram for Cyberattack detection

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

### 3.6 ACTIVITY DIAGRAM

It describes about flow of activity states.

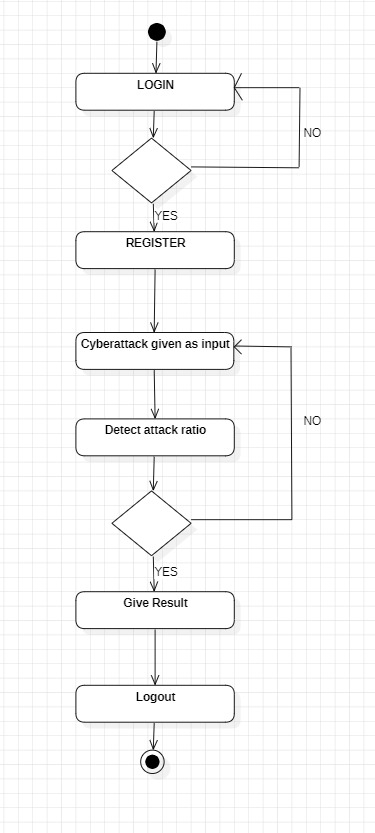


Figure 3.6: Activity Diagram for Cyberattack detection

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.