DETECTING CYBER THREATS – A DEEP LEARNING BASED FRAMEWORK FOR NETWORK ATTACK DETECTION

A PROJECT REPORT – PHASE II

Submitted by

DESHA JAYA SAI MANJUNATH (9920004215)

KOLLIPATI NIKHIL CHOWDARY (9920004296)

SIRUPA KARTHIK REDDY (9920004359)

PALLE PARTHA SARADHI REDDY (9919004209)

In partial fulfillment for the award of the degree

Of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

DEPARTMENT OF COMPUTER SCIENCE

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(Deemed to be University)

ACADEMIC YEAR 2023-24

KRISHNANKOIL – 626126

DECLARATION

We affirm that the project work titled **"DETECTING CYBER THREATS – A DEEP LEARNING BASED FRAMEWORK FOR NETWORK ATTACK DETECTION"** being submitted in partial fulfilment for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** is the original work carried out by us. It has not formed part of any other project work submitted for the award of any degree or diploma, either in this or any other University.

Desha Jaya Sai Manjunath

9920004215

Sirupa Karthik Reddy

9920004359

Kollipati Nikhil Reddy

9920004296

Palle Partha Saradhi Reddy

9919004209

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Date:

Signature of supervisor

Ms.R.Syed Ali Fathima

Assistant Professor

Department of Computer Science and Engineering

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade

BONAFIDE CERTIFICATE

DEPARTMENT OF COMPUTER SCIENCE

Certified that this project report **"Detecting cyber threats – A Deep Learning based Framework for Network Attack Detection"** is the bonafide work of **"DESHA JAYA SAI MANJUNATH (9920004215), KOLLIPATI NIKHIL CHOWDARY (9920004296), SIRUPA KARTHIK REDDY (9920004359), PALLE PARTHA SARADHI REDDY (9919004209)"** who carried out the project work under my supervision.

MS.R.SYED ALI FATHIMA
SUPERVISOR
Assistant Professor
Department of CSE
Kalasalingam Academy of Research and Education
Krishnankovil - 626126
Virudhunagar District

Dr. N. SURESH KUMAR
HEAD OF THE DEPARTMENT
Professor/Head
Department of CSE
Kalasalingam Academy of Research and Education
Krishnankovil - 626126
Virudhunagar District

Submitted for the Project Viva-voce examination held on **_____.**

Internal Examiner **External Examiner**

ACKNOWLEDGEMENT

First and foremost, we thank the 'Supreme Power' for the immense grace showered on us which enabled us to do this project. We take this opportunity to express sincere thanks to the late, **"Kalvivallal" Thiru T. KALASALINGAM, Chairman, Kalasalingam Group of Institutions, "Illayavallal" Dr. K. SRIDHARAN, Ph.D., Chancellor, Dr. S. SHASI ANAND, Ph.D., Vice President**, who is the guiding light for all the activities in our university.

We thank our Vice Chancellor **Dr. S. NARAYANAN, Ph.D**., for guiding every one of us and infusing us with the strength and enthusiasm to work successfully.

We wish to express our sincere thanks to our respected Head of the Department **Dr. N. SURESH KUMAR,** whose moral support encouraged us to process through our project work successfully.

We offer our sincerest gratitude to our Project Supervisor, **Ms.R.SYED ALI FATHIMA,** for her patience, motivation, enthusiasm, and immense knowledge.

We are extremely grateful to our Overall Project Coordinator, **Dr. S. ARIFFA BEGUM,** for her constant encouragement in the completion of the Capstone Project.

Finally, we thank all, our Parents, Faculty, Non-Teaching Faculty, and our friends for their moral support.

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade

SCHOOL OF COMPUTING
COMPUTER SCIENCE AND ENGINEERING

PROJECT SUMMARY

Project Title	Detecting cyber threats – A Deep Learning based Framework for Network Attack Detection
Project Team Members (Name with Register No)	DESHA JAYA SAI MANJUNATH (9920004215) KOLLIPATI NIKHIL CHOWDARY 9920004296) SIRUPA KARTHIK REDDY (9920004359) PALLE PARTHA SARADHI REDDY (9919004209)
Guide Name/Designation	Ms.R.Syed Ali Fathima, Assistant Professor, Department of Computer Science and Engineering
Program Concentration Area	Machine Learning, Cyber Security
Technical Requirements	Machine Learning, Python.

Engineering standards and realistic constraints in these areas

Area	Codes & Standards / Realistic Constraints	Tick ✓
Economic	Compliance with financial regulations and industry standards related to data security. Budgetary considerations for implementing cybersecurity measures, cost-effectiveness of the proposed framework.	✓
Environmental	Adherence to environmental regulations regarding the disposal of electronic equipment used in the framework. Minimization of energy consumption and environmental impact of the computational infrastructure required for deep learning model training and deployment.	✓
Ethical	Ethical guidelines for handling sensitive information and ensuring fairness in algorithmic decision-making. Transparency in the functioning of the deep learning model, mitigation of biases, and accountability in case of false positives/negatives.	✓
Social	Alignment with privacy laws and regulations to protect user data. Consideration of societal impacts of cyber-attacks and the importance of safeguarding personal and organizational information.	✓

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 present 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.

Index Terms: Intrusion Detection, Deep Learning, Cyber security Vulnerabilities, Generative Adversarial Network, Network Security.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Full forms
HDR	Highest Detection Rate
IDS	Intrusion Detection System
IoT	Internet of things
IIC	Internet Industrial Control
CI	Critical Infrastructure
FPR	False positive rates
HCL	Hardware Compatibility List
AI	Artificial intelligence
ML	Machine Learning
SVM	Support Vector Machine
LSTM	Long Short-Term Memory
RNN	Recurrent Neural Network
CNN	Convolutional Neural Network
DNN	Deep Neural Network
GAN	General Adversarial Network
DFD	Data Flow Diagram
UML	Unified Modeling Language
DLP	Data Loss Prevention
NIC	Network Interface Card
DPI	Deep Packet Inspection
DL	Deep Learning

LIST OF ACADEMIC REFERENCE COURSES

S. NO.	COURSE CODE	COURSE NAME
1	CSE18R254	INTRODUCTION TO PYTHON PROGRAMMING
2	CSE18R212	MACHINE LEARNING
3	CSE18R393	IT NETWORK SECURITY

CHAPTER 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 provide an effective IDS for IIoT-powered IICs utilizing deep-autoencoder-based LSTM model/method.

1.1 Objective:

This research aims to enhance computer network security by developing a novel deep learning-based intrusion detection method for cyber-physical systems. By contrasting unsupervised and deep learning discriminative approaches and employing a generative adversarial network, we seek to improve the accuracy, reliability, and efficiency of detecting various cyber threats within IoT-driven Industrial Internet of Cyber-Physical Systems (IICs) networks. Our objective is to achieve superior performance in terms of true rate and detection rate while safeguarding sensitive information integrity throughout the process.

1.2 Problem Statement:

In the realm of computer network security, the persistent menace of malicious software, computer viruses, and hostile attacks poses significant challenges. Traditional intrusion detection systems are plagued by issues such as low accuracy, poor detection capabilities, a high rate of false positives, and a lack of adaptability to emerging intrusion forms. This research addresses these pressing concerns by proposing a deep learning-driven methodology for identifying and mitigating cybersecurity vulnerabilities and breaches in cyber-physical systems. The primary problem at hand is the need for a more effective and efficient intrusion

detection solution capable of safeguarding sensitive data and systems while delivering superior performance across various attack scenarios.

1.3 SOFTWARE REQUIREMENTS

Software requirements deal with defining software resource requirements and prerequisites that need to be installed on a computer to provide optimal functioning of an application. These requirements or prerequisites are generally not included in the software installation package and need to be installed separately before the software is installed.

Platform – In computing, a platform describes some sort of framework, either in hardware or software, which allows software to run. Typical platforms include a computer's architecture, operating system, or programming languages and their runtime libraries.

Operating system is one of the first requirements mentioned when defining system requirements (software). Software may not be compatible with different versions of same line of operating systems, although some measure of backward compatibility is often maintained. For example, most software designed for Microsoft Windows XP does not run on Microsoft Windows 98, although the converse is not always true. Similarly, software designed using newer features of Linux Kernel v2.6 generally does not run or compile properly (or at all) on Linux distributions using Kernel v2.2 or v2.4.

APIs and drivers – Software making extensive use of special hardware devices, like high-end display adapters, needs special API or newer device drivers. A good example is DirectX, which is a collection of APIs for handling tasks related to multimedia, especially game programming, on Microsoft platforms.

Web browser – Most web applications and software depending heavily on Internet technologies make use of the default browser installed on system. Microsoft Internet Explorer is a frequent choice of software running on Microsoft Windows, which makes use of ActiveX controls, despite their vulnerabilities.

1) Anaconda

1.4 HARDWARE REQUIREMENTS

The most common set of requirements defined by any operating system or software application is the physical computer resources, also known as hardware, A hardware requirements list is often accompanied by a hardware compatibility list (HCL), especially in case of operating systems. An HCL lists tested, compatible, and sometimes incompatible hardware devices for a particular operating system or application. The following sub-sections discuss the various aspects of hardware requirements.

Architecture – All computer operating systems are designed for a particular computer architecture. Most software applications are limited to particular operating systems running on particular architectures. Although architecture-independent operating systems and applications exist, most need to be recompiled to run on a new architecture. See also a list of common operating systems and their supporting architectures.

Processing power – The power of the central processing unit (CPU) is a fundamental system requirement for any software. Most software running on x86 architecture define processing power as the model and the clock speed of the CPU. Many other features of a CPU that influence its speed and power, like bus speed, cache, and MIPS are often ignored. This definition of power is often erroneous, as AMD Athlon and Intel Pentium CPUs at similar clock speed often have different throughput speeds. Intel Pentium CPUs have enjoyed a considerable degree of popularity, and are often mentioned in this category.

Memory – All software, when run, resides in the random access memory (RAM) of a computer. Memory requirements are defined after considering demands of the application, operating system, supporting software and files, and other running processes. Optimal performance of other unrelated software running on a multi-tasking computer system is also considered when defining this requirement.

Secondary storage – Hard-disk requirements vary, depending on the size of software installation, temporary files created and maintained while installing or running the software, and possible use of swap space (if RAM is insufficient).

Display adapter – Software requiring a better than average computer graphics display, like graphics editors and high-end games, often define high-end display adapters in the system requirements.

Peripherals – Some software applications need to make extensive and/or special use of some peripherals, demanding the higher performance or functionality of such peripherals. Such peripherals include CD-ROM drives, keyboards, pointing devices, network devices, etc.

1)Operating System : Windows Only

2)Processor : i5 and above

3)Ram : 8gb and above

4)Hard Disk : 25 GB in local drive

CHAPTER II

2. FEASIBILITY STUDY

Feasibility Study

A feasibility study evaluates a project's or system's practicality. As part of a feasibility study, the objective and rational analysis of a potential business or venture is conducted to determine its strengths and weaknesses, potential opportunities and threats, resources required to carry out, and ultimate success prospects. Two criteria should be considered when judging feasibility: the required cost and expected value.

Types Of Feasibility Study

A feasibility analysis evaluates the project's potential for success; therefore, perceived objectivity is an essential factor in the credibility of the study for potential investors and lending institutions. There are five types of feasibility study—separate areas that a feasibility study examines, described below.

1. Technical Feasibility

This assessment focuses on the technical resources available to the organization. It helps organizations determine whether the technical resources meet capacity and whether the technical team is capable of converting the ideas into working systems. Technical feasibility also involves the evaluation of the hardware, software, and other technical requirements of the proposed system. As an exaggerated example, an organization wouldn't want to try to put Star Trek's transporters in their building—currently, this project is not technically feasible.

2. Economic Feasibility

This assessment typically involves a cost/ benefits analysis of the project, helping organizations determine the viability, cost, and benefits associated with a project before financial resources are allocated. It also serves as an independent project assessment and enhances project credibility—helping decision-makers determine the positive economic benefits to the organization that the proposed project will provide.

3. Legal Feasibility

This assessment investigates whether any aspect of the proposed project conflicts with legal requirements like zoning laws, data protection acts or social media laws. Let's say an organization wants to construct a new office building in a specific location. A feasibility study might reveal the organization's ideal location isn't zoned for that type of business. That

organization has just saved considerable time and effort by learning that their project was not feasible right from the beginning.

4. Operational Feasibility

This assessment involves undertaking a study to analyze and determine whether—and how well—the organization's needs can be met by completing the project. Operational feasibility studies also examine how a project plan satisfies the requirements identified in the requirements analysis phase of system development.

5. Scheduling Feasibility

This assessment is the most important for project success; after all, a project will fail if not completed on time. In scheduling feasibility, an organization estimates how much time the project will take to complete.

When these areas have all been examined, the feasibility analysis helps identify any constraints the proposed project may face, including:

- Internal Project Constraints: Technical, Technology, Budget, Resource, etc.
- Internal Corporate Constraints: Financial, Marketing, Export, etc.
- External Constraints: Logistics, Environment, Laws, and Regulations, etc.

CHAPTER III

3. LITERATURE SURVEY

Definition: A literature survey, often referred to as a literature review, is a critical and comprehensive evaluation of existing literature, scholarly articles, books, and other sources relevant to a particular topic or research question. It involves systematically searching, summarizing, and synthesizing existing knowledge and findings on the chosen subject.

The purpose of a literature survey is multi-fold:

Understanding the Existing Knowledge: It helps researchers gain a deep understanding of what has already been studied and discovered in their field of interest.

Identifying Gaps and Trends: By analyzing existing literature, researchers can identify gaps in knowledge, inconsistencies in findings, and emerging trends that warrant further investigation.

Contextualizing Research: A literature survey helps researchers place their own work within the broader context of existing scholarship, thereby demonstrating the significance and originality of their research.

Informing Methodology and Theory: It informs researchers about the methodologies, theories, and approaches that have been employed in previous studies, guiding them in selecting appropriate methods for their own research.

Table 3.1: Comparison Tabular Format for Literature Survey

TITLE & AUTHORS	METHODOLOGY	PROPOSED SYSTEM	CONS	CONCLUSION
TITLE: Convolutional Neural Network—A Practical Case Study **AUTHOR:** João Azevedo et.al., **(2022)**	The research evaluates the performance of convolutional neural networks (CNNs) known as "AlexNet," "VGG," "Inception," and "ResNet" in image classification using the "Imagenet" dataset. It then extends the evaluation to video classification using the "Kinetics400" and "UCF101" datasets to determine if success in image classification translates to video classification.	The study selects the two CNNs with the lowest margin of error in image classification and examines their performance in classifying videos. The goal is to assess whether these networks can accurately identify human activities in input videos from sensors.	1. The research focuses on a specific set of CNN architectures and does not explore a broader range of network models. 2. The study primarily evaluates existing networks, and the approach may not introduce novel techniques or innovations in image and video classification.	The research demonstrates that CNNs, particularly "ResNet" and "Inception," achieve satisfactory success rates in both image and video classification tasks. This suggests that networks successful in image classification can also perform well in video classification, making them suitable for identifying human

				activities in sensor-generated videos.
TITLE: Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets **AUTHOR:** Eric Gyamfi et.al., **(2022)**	This research reviews the state-of-the-art network intrusion detection systems (NIDS) and security practices for IoT networks. It focuses on approaches based on multi-access edge computing (MEC) platforms and employs machine learning (ML) techniques. The study also conducts a comparative analysis of datasets, evaluation metrics, and deployment strategies used in NIDS design for IoT networks.	The paper proposes an NIDS framework for IoT networks that leverages MEC for improved security. This framework aims to address the vulnerabilities of IoT devices by offloading complex computing tasks to the edge, enhancing security practices.	1. The research mainly concentrates on reviewing existing approaches and proposing a framework. It may lack a detailed implementation or experimental validation of the proposed NIDS framework. 2. Integrating MEC into IoT networks may introduce additional complexity, which could be challenging to implement and manage.	The study underscores the importance of security in IoT networks and explores the potential of MEC and ML techniques for network intrusion detection. The proposed NIDS framework offers a promising approach to enhance IoT network security by offloading computational tasks to the edge.
TITLE: A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method **AUTHOR:** Mr. Amit Kr. Balyan et.al., **(2022)**	This research addresses intrusion detection in the context of machine learning, focusing on the data imbalance issue. The proposed Hybrid Network-based IDS (HNIDS) model utilizes an enhanced genetic algorithm and particle swarm optimization (EGA-PSO) for feature selection and data balancing. It also employs an improved random forest (IRF) method to improve classification accuracy.	The HNIDS model consists of two phases. In the first phase, EGA-PSO is used for data balancing and feature selection. PSO enhances genetic algorithms, and a multi-objective function helps select essential features while reducing dimensions. In the second phase, IRF is employed for classification, incorporating decision trees and preventing overfitting.	1. The proposed HNIDS model involves multiple phases and optimization techniques, which may introduce complexity in implementation and configuration. 2. The effectiveness of this approach relies on the specific dataset used. Its performance may vary with different datasets.	The research presents an approach to address data imbalance in intrusion detection using machine learning. The HNIDS model, incorporating EGA-PSO and IRF, demonstrates promising results in terms of accuracy and intrusion detection performance. However, its practical applicability may depend on dataset characteristics and implementation challenges.
TITLE: A tree classifier	This research addresses the cybersecurity	The proposed system aims to	1. While dimensionality	The research focuses on

based network intrusion detection model for Internet of Medical Things **AUTHOR:** Karan Gupta et.al., **(2022)**	challenges in the Internet of Medical Things (IoMT) by designing a network intrusion detection model. The proposed model utilizes a tree classifier-based approach and incorporates dimensionality reduction techniques to enhance anomaly detection efficiency.	enhance the security of IoMT networks. It leverages tree classifier-based algorithms for intrusion detection and employs dimensionality reduction techniques to optimize the processing of input data. The primary goal is to ensure the privacy and safety of patients in IoMT networks.	reduction can improve processing speed, it may lead to information loss if not carefully implemented. 2. The effectiveness of the proposed system may depend on the specific IoMT dataset used for training and testing.	addressing cybersecurity issues in IoMT networks, which are critical for patient privacy and safety. The proposed intrusion detection model, with its emphasis on dimensionality reduction and accuracy, shows promise in enhancing the security of IoMT systems. However, its performance may vary with different datasets and real-world implementations.
TITLE: A drone-based data management and optimization using metaheuristic algorithms and blockchain smart contracts in a secure fog environment **AUTHOR:** Abdullah Ayub Khan et.al., **(2022)**	This research focuses on improving the management and optimization of drone-based data through a collaborative approach using fog computing and blockchain Hyperledger Fabric. The proposed system, named B-Drone, employs a metaheuristic-enabled genetic algorithm for efficient fog node management. It emphasizes secure data collection, scheduling, optimization, processing, management, and preservation within fog nodes.	It ensures the privacy and security of transactions through hash-encryption (SHA-256) algorithms and deploys blockchain smart contracts for managing connectivity and communication protocols between drones and fog nodes within a private permissioned network.	1. Implementing blockchain technology in drone-based data management introduces complexity, which may require specialized knowledge and resources. 2. Blockchain transactions can incur additional computational and storage overhead.	The proposed B-Drone system demonstrates improvements in computing cost reduction and network performance enhancement compared to existing methods. However, it also introduces complexity and resource overhead that need to be carefully managed in practical implementations.
TITLE: BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using	This research focuses on addressing the security and privacy concerns associated with healthcare data transfer and management. It proposes a blockchain Hyperledger Fabric-enabled consortium architecture called	The proposed system, BIoMT, leverages blockchain Hyperledger Fabric to create a secure and transparent environment for healthcare data	1. Implementing blockchain and cryptographic techniques may introduce complexity to healthcare data management. 2. Blockchain transactions and	The research introduces BIoMT, a consortium architecture that enhances the security and privacy of healthcare data transactions in a serverless P2P network. It reduces

Blockchain Smart Contracts **AUTHOR:** Abdullah Ayub Khan et.al., **(2022)**	BIoMT. The architecture aims to provide security, integrity, transparency, and provenance to health-related transactions while facilitating the exchange of sensitive clinical information in a serverless peer-to-peer (P2P) secure network environment. The study introduces consensus mechanisms and privacy-enhancing techniques like NuCypher Re-Encryption.	transactions. It incorporates consensus mechanisms to optimize blockchain resource utilization and employs NuCypher Re-Encryption for transaction privacy. Smart contracts automate device registration, transactions, and ledger preservation.	encryption techniques can consume additional computational resources.	computational costs and improves the robustness of medical nodes. However, implementing such a system may require careful consideration of complexity and resource utilization.

CHAPTER IV

4.SYSTEM ANALYSIS

4.1 EXISTING SYSTEM:

In literature they introduced a deep neural network (DNN), a type of deep learning model, is explored to develop a flexible and effective IDS to detect and classify unforeseen and unpredictable cyberattacks. The continuous change in network behavior and rapid evolution of attacks makes it necessary to evaluate various datasets which are generated over the years through static and dynamic approaches. This type of study facilitates to identify the best algorithm which can effectively work in detecting future cyberattacks. A comprehensive evaluation of experiments of DNNs and other classical machine learning classifiers are shown on various publicly available benchmark malware datasets.

4.1.1 DISADVANTAGES OF EXISTING SYSTEM:

1. The existing work focuses on detecting and classifying unforeseen and unpredictable cyberattacks in general cyber environments.
2. While the existing work explores the use of a deep neural network (DNN) along with classical machine learning classifiers. Which may leads to decrease in performance in cyber-attack detection.
3. The existing work, on the other hand, focuses on publicly available benchmark malware datasets, which may not fully capture the complexities of modern cyber-physical systems.

4.2 Proposed System:

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 (RNN, CNN, and DNN) discriminative approaches. We present a generative adversarial network(RBN, DBN, DBM., and DA) to detect cyber threats in IoT-driven IICs networks. Tests the performance of the proposed efficient IDS framework on IIoT IICs and exterior networks on the NSLKDD, KDDCup99, and UNSW-NB15 datasets.

4.2.1 Advantages of proposed system:

1. We specifically target cybersecurity vulnerabilities and breaches in cyber-physical systems, which may allow for a more specialized and tailored approach to threat detection.
2. We introduce a more diverse range of deep learning techniques and various generative adversarial network (GAN) architectures (RBN, DBN, DBM, and DA). This broader range of approaches might lead to improved detection performance and adaptability.
3. We evaluate our proposed IDS framework on datasets such as NSL-KDD, KDDCup99, and UNSW-NB15. These datasets are widely recognized benchmarks in the field of intrusion detection research.
4. We introduce generative adversarial networks (GANs) for detecting cyber threats. GANs have shown promise in various domains for their ability to generate and discriminate data, potentially enhancing the detection capabilities in cyber-physical systems.

4.3 FUNCTIONAL REQUIREMENTS

1.Data Collection

2.Data Preprocessing

3.Training And Testing

4.Modiling

5.Predicting

4.4 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 nonfunctional 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 allows 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 number of simultaneous users are > 10000. Description of non-functional requirements is just as critical as a functional requirement.

- Usability requirement
- Serviceability requirement

- Manageability requirement
- Recoverability requirement
- Security requirement
- Data Integrity requirement
- Capacity requirement
- Availability requirement
- Scalability requirement
- Interoperability requirement
- Reliability requirement
- Maintainability requirement
- Regulatory requirement
- Environmental requirement

CHAPTER V

5. METHODOLOGY

Methodology refers to the systematic approach or framework used to plan, execute, monitor, and control the project activities from initiation to completion. It encompasses various processes, techniques, tools, and best practices tailored to meet the project's specific objectives, constraints, and requirements. Each methodology has its own set of principles, practices, and guidelines to guide the project team through the project lifecycle.

5.1 SYSTEM ARCHITECTURE:

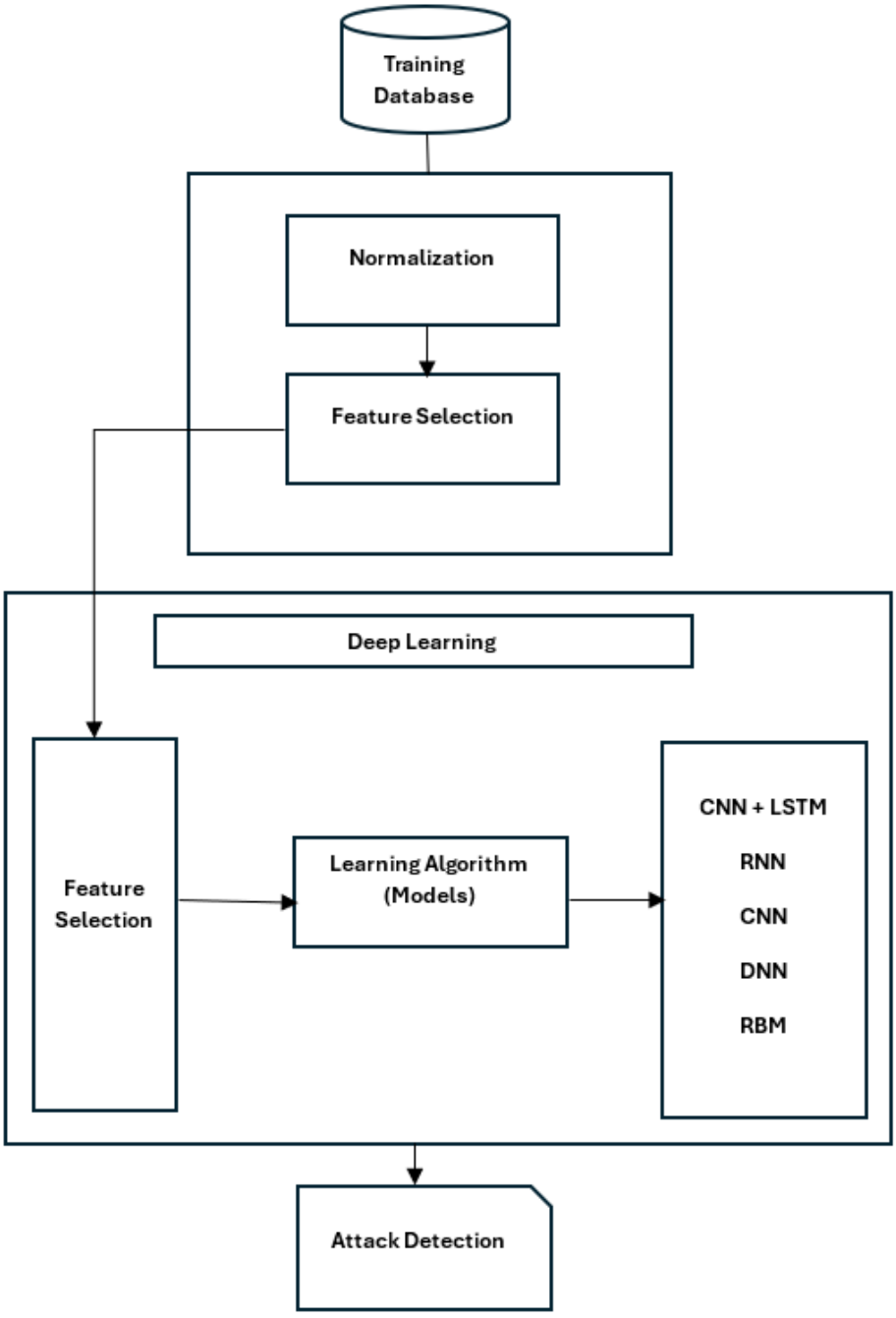

Fig.5.1.1 System architecture

System architecture deals with the high-level design and organization of the project's components or subsystems to ensure they work together efficiently and effectively to achieve the desired functionality and performance. It involves defining the structure, behavior, interfaces, and relationships between various system elements, such as software components, hardware components, databases, networks, and external systems.

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.

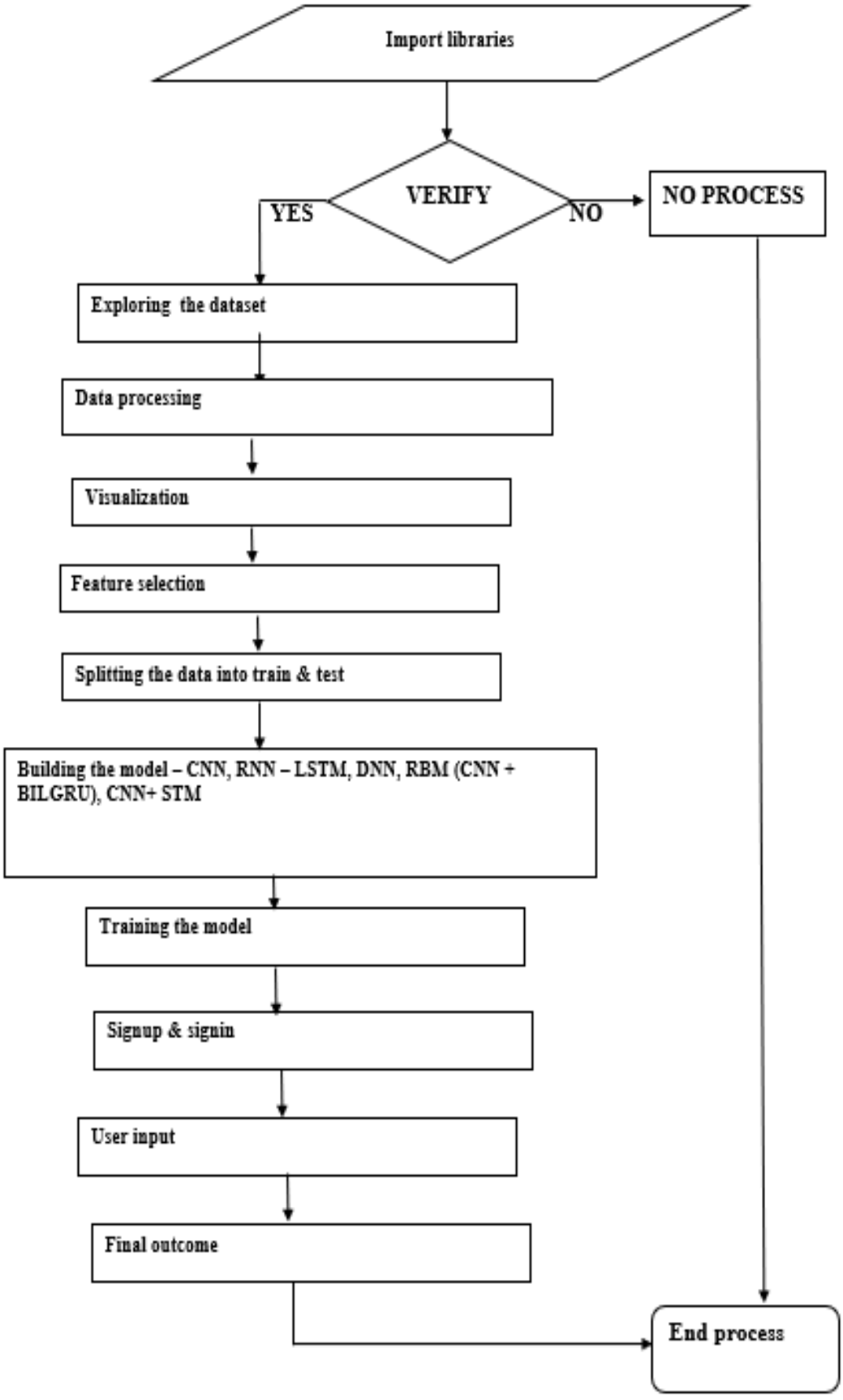

Fig.5.1.2 Data Flow Diagram

5.2 UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object-oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects-oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices.

Use case diagram:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in

the system can be depicted.

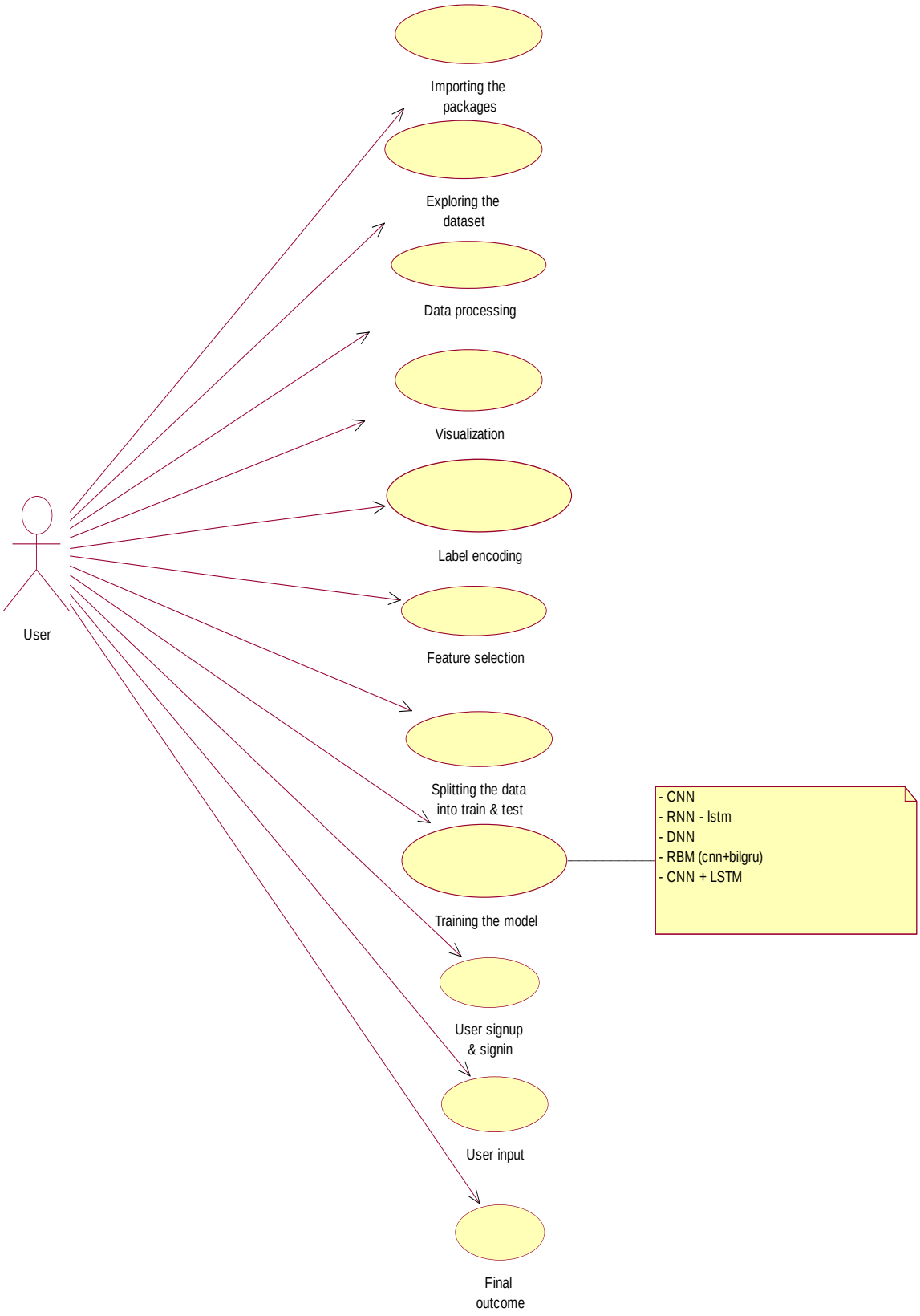

Fig.5.2.1 User Case Diagram

Class diagram:

The class diagram is used to refine the use case diagram and define a detailed design of the system. The class diagram classifies the actors defined in the use case diagram into a set of interrelated classes. The relationship or association between the classes can be either an "is-a" or "has-a" relationship. Each class in the class diagram may be capable of providing certain functionalities. These functionalities provided by the class are termed "methods" of the class. Apart from this, each class may have certain "attributes" that uniquely identify the class.

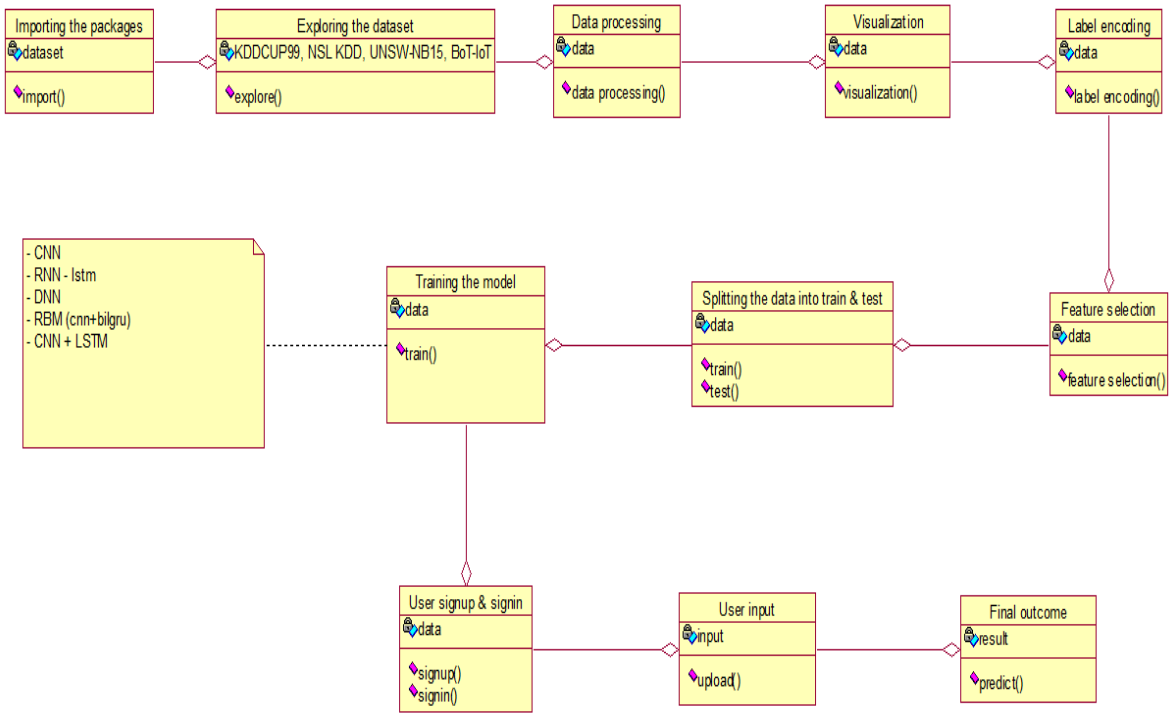

Fig.5.2.2 Class Diagram

Activity diagram:

The process flows in the system are captured in the activity diagram. Similar to a state diagram, an activity diagram also consists of activities, actions, transitions, initial and final states, and guard conditions.

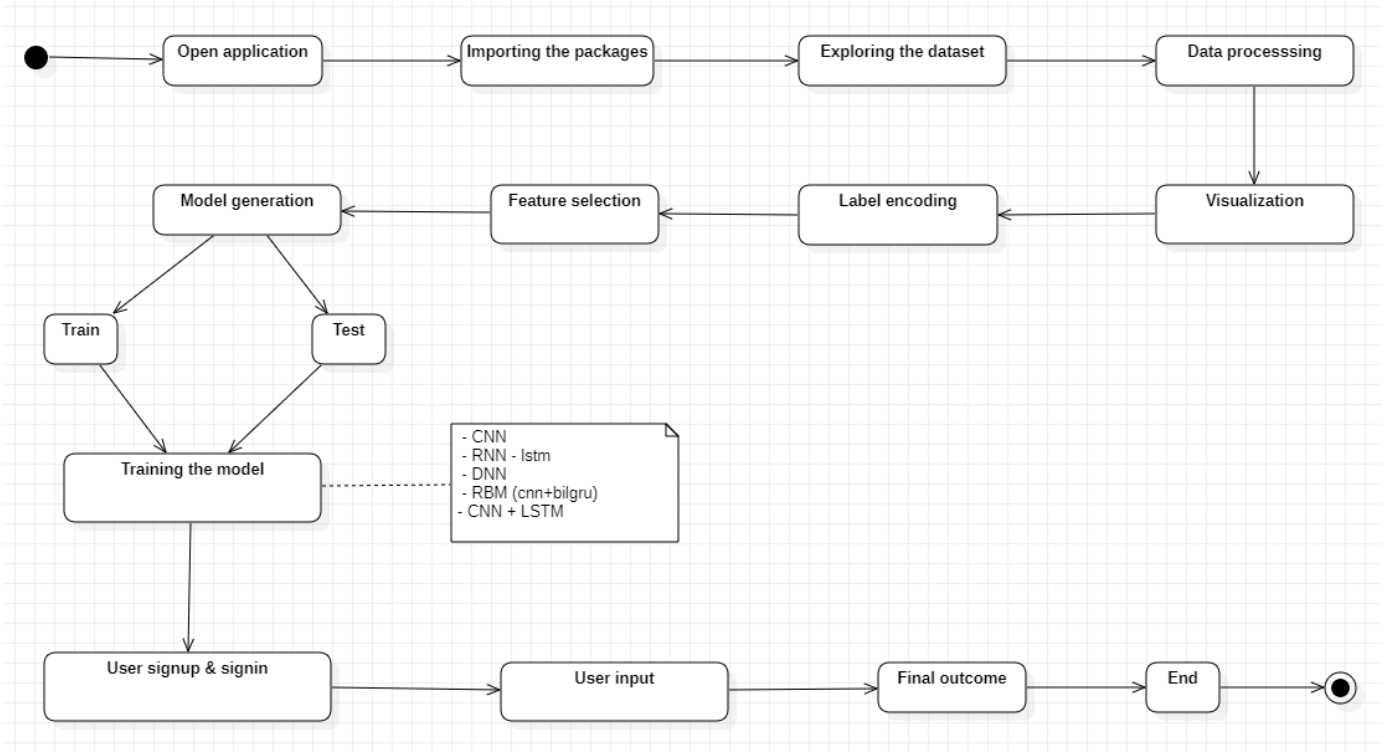

Fig.5.2.3 Activity Diagram

Collaboration diagram:

A collaboration diagram groups together the interactions between different objects. The interactions are listed as numbered interactions that help to trace the sequence of the interactions. The collaboration diagram helps to identify all the possible interactions that each object has with other objects.

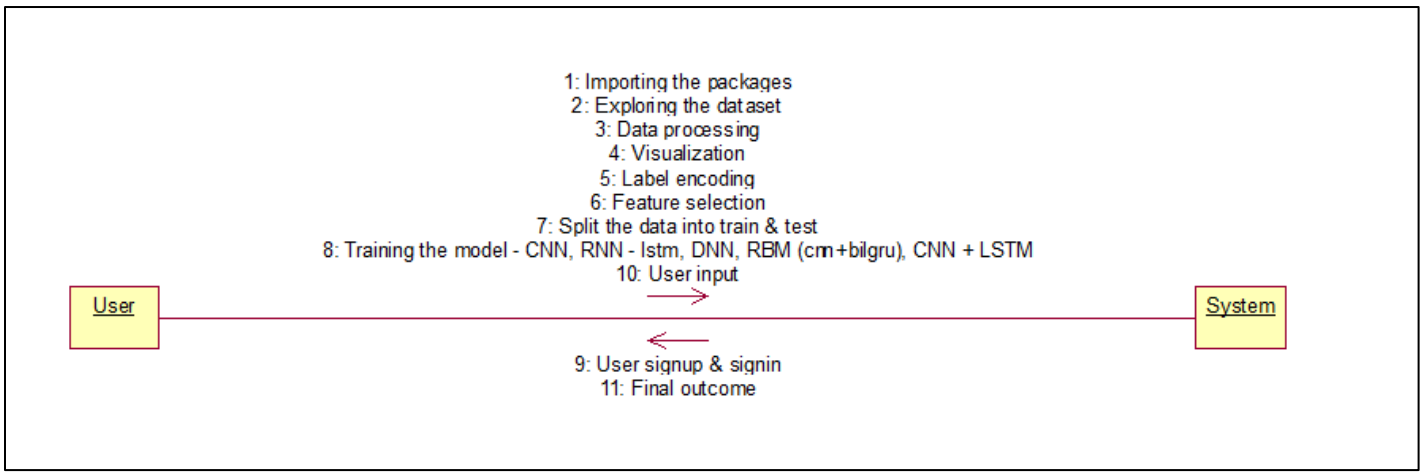

Fig.5.2.5 Collaboration Diagram

Sequence diagram:

A sequence diagram represents the interaction between different objects in the system. The important aspect of a sequence diagram is that it is time-ordered. This means that the exact sequence of the interactions between the objects is represented step by step. Different objects in the sequence diagram interact with each other by passing "messages".

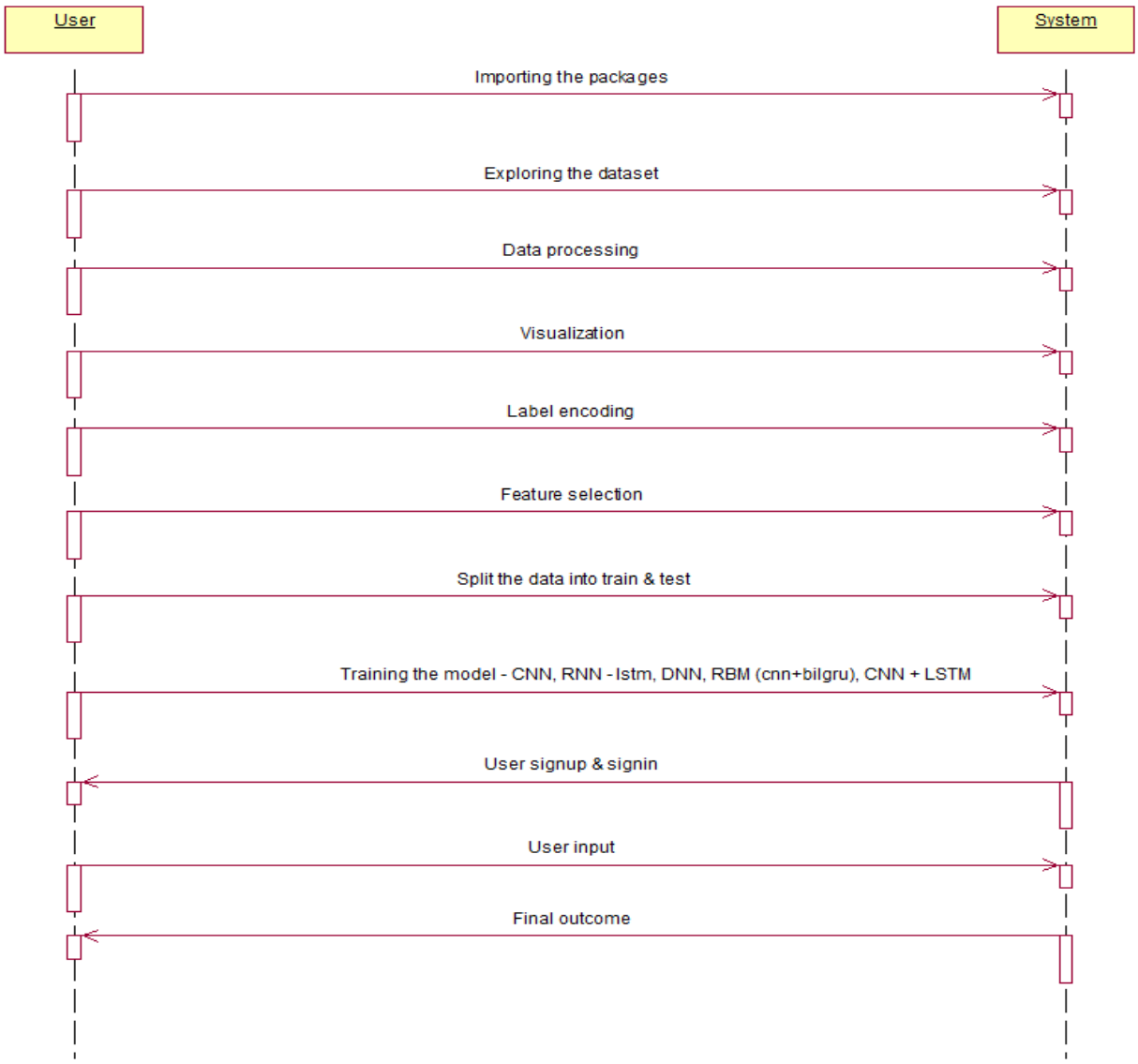

Fig.5.2.4 Sequence Diagram

Component diagram:

The component diagram represents the high-level parts that make up the system. This diagram depicts, at a high level, what components form part of the system and how they are

interrelated. A component diagram depicts the components culled after the system has undergone the development or construction phase.

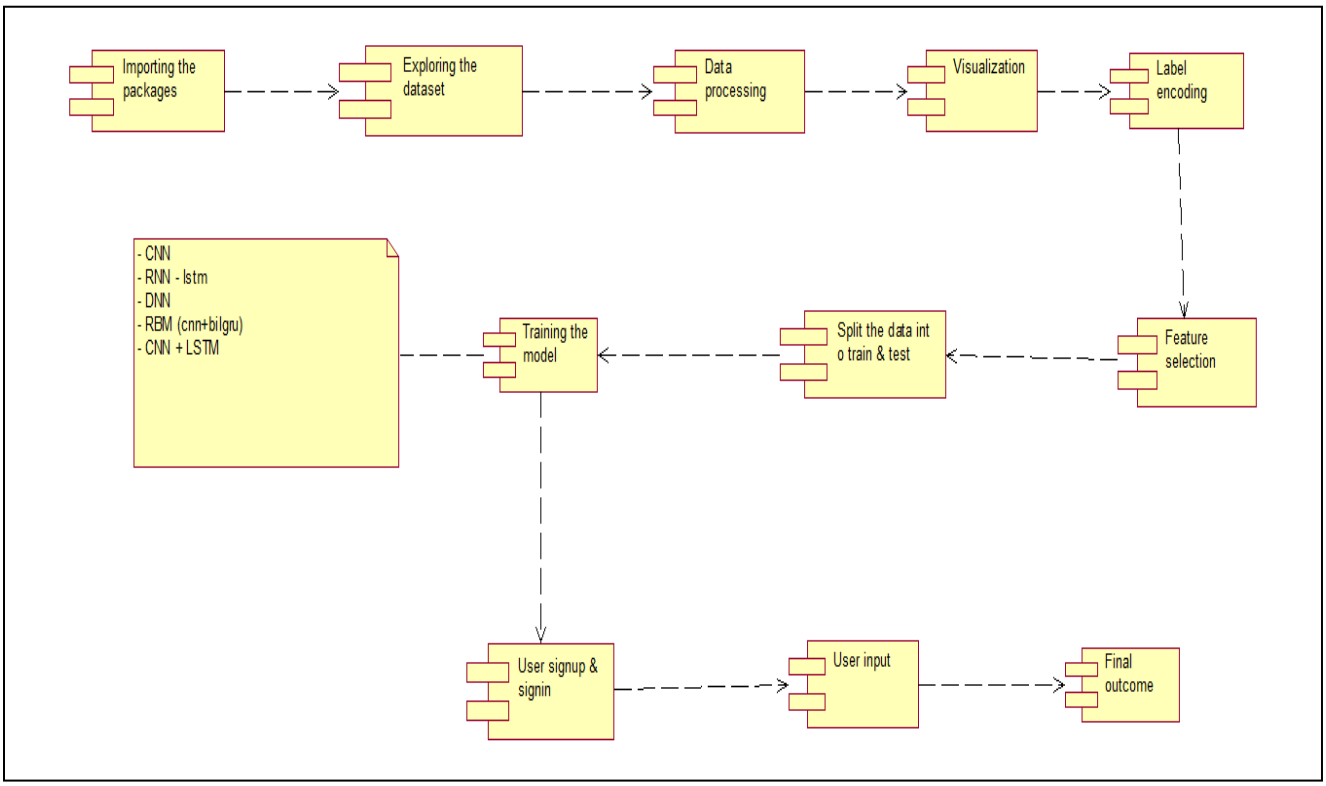

Fig.5.2.6 Component Diagram

Deployment diagram:

The deployment diagram captures the configuration of the runtime elements of the application. This diagram is by far most useful when a system is built and ready to be deployed.

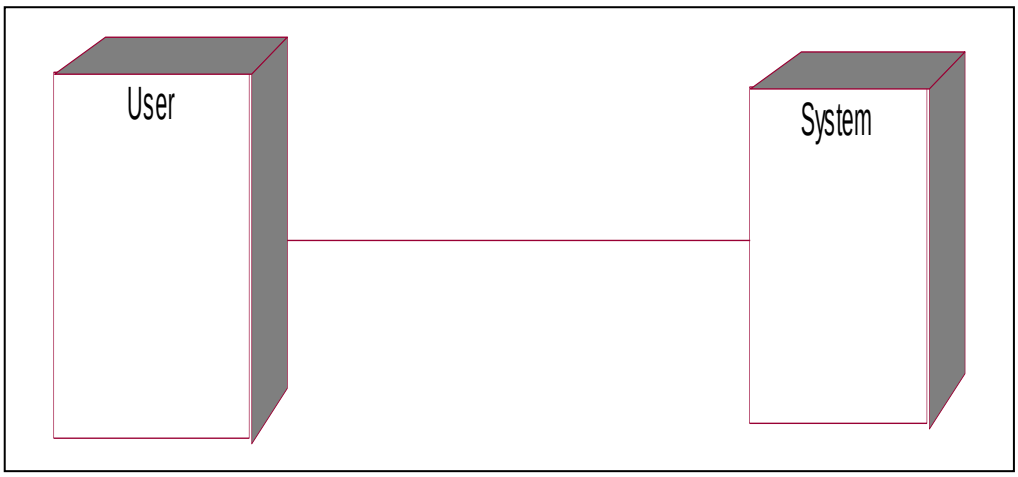

Fig.5.2.7 Deployment Diagram

CHAPTER VI

IMPLEMENTATION AND RESULT

6.1 IMPLEMENTATION:

The detection of real-time malicious intrusions and attacks in IoT-empowered cybersecurity infrastructures is a critical challenge due to the increasing complexity and heterogeneity of IoT networks. Traditional intrusion detection systems (IDS) are often unable to keep up with the ever-evolving threat landscape, resulting in missed detections and false positives.

To address these challenges, we have proposed a number of novel approaches for real-time intrusion detection in IoT networks. These approaches include:

- **Machine learning and artificial intelligence (ML/AI)-based IDS:** ML/AI algorithms can be used to analyze network traffic and identify patterns that are indicative of malicious activity. This approach is particularly well-suited for detecting unknown attacks, as it does not rely on predefined signatures.
- **Anomaly detection:** Anomaly detection systems monitor network traffic for deviations from normal behaviour. This approach is effective at detecting anomalous activity, but it can be difficult to distinguish between malicious and non-malicious anomalies.
- **Behavioural analysis:** Behavioural analysis techniques monitor user and device behaviour for signs of malicious activity. This approach can be effective at detecting attacks that target specific behaviours, such as unusual login attempts or data exfiltration.

In addition to these technical approaches, there are a number of operational considerations that are important for real-time intrusion detection in IoT networks. These include:

- **Real-time data collection and analysis:** IoT networks generate a large volume of data, which must be collected and analysed in real time to detect attacks.
- **Scalability:** IoT networks can be large and complex, and intrusion detection systems must be able to scale to handle the volume of data and the number of devices.
- **Integration with other security systems:** Intrusion detection systems should be integrated with other security systems, such as firewalls and data loss prevention (DLP) systems, to provide a comprehensive security solution.

- **Threat intelligence:** Intrusion detection systems should be able to leverage threat intelligence feeds to keep up with the latest attack techniques.

By combining these technical and operational approaches, organizations can create a more effective real-time intrusion detection system for their IoT networks.

The implementation of a real-time intrusion detection system for IoT networks typically involves the following steps:

Data collection

The first step in implementing a real-time intrusion detection system for IoT networks is to collect network traffic data from IoT devices and sensors. This data can be collected using a variety of methods, including:

- Sniffing: Sniffing involves capturing network traffic using a network interface card (NIC) in promiscuous mode.
- Deep packet inspection (DPI): DPI involves inspecting the contents of network packets to extract more detailed information.
- Network flow analysis: Network flow analysis involves analysing the flow of traffic between different endpoints on the network.

The specific method used to collect data will depend on the network topology and the available resources.

Preprocessing

Once the data has been collected, it must be pre-processed to remove noise and prepare it for analysis. This may involve the following steps:

- Normalization: Normalizing the data to a consistent scale can improve the accuracy of ML/AI models.
- Imputation: Imputing missing values in the data can help to ensure that the ML/AI models have all the information they need to make accurate predictions.
- Feature engineering: Creating new features from the existing data can help to improve the performance of ML/AI models.

The specific preprocessing steps used will depend on the nature of the data and the ML/AI models that will be used to analyze it.

Algorithms

CNN

CNNs, or Convolutional Neural Networks, are DL models designed to interpret visual data like images and videos. The network's convolutional layers allow it to learn from the input and

detect patterns, shapes, and features. These layers use filters to find and pull out important data while keeping the connections between things in space. CNNs are very useful for tasks like image classification, object detection, and face recognition because they can learn and describe complex visual traits in a hierarchical way. This makes them important in computer vision applications and many other areas that involve understanding and analyzing images.

RNN (LSTM)

LSTM artificial neural networks handle sequential input using memory and feedback loops. Recurrent neural networks. They excel in time-sensitive tasks like time series analysis, natural language processing, voice recognition, and more.

Standard RNNs have the vanishing gradient issue, but LSTMs overcome it. They employ custom memory cells, switches, and cell states, making their design more sophisticated. Because they can store data throughout time, LSTMs can grasp and predict sequential data context.

In an LSTM network, information passes between input, forget, and output gates. These gates control how data enters and leaves the memory cell. They do this so that important data stays in the memory cell and useless data is thrown away. This lets LSTMs understand long-distance connections and correctly guess or group things based on sequential trends.

To sum up, LSTMs are a type of RNN that are great at dealing with sequential data because they can keep and change background information over time. They are used for many things, like analyzing text and speech to making predictions based on time series and more, where it's important to understand and use how time works.

DNN

Artificial neural networks with numerous layers of linked nodes are called deep neural networks (DNNs). DNNs solve complicated issues in computer vision, voice recognition, and natural language processing, making them vital to machine learning and DL. A typical DNN has an input layer, numerous hidden layers, and an output layer. The network's nodes alter and transform data at each layer. DL methods, which are often used to train DNNs, change the weights and biases of these neurons over and over again while they are being trained. This lets them learn complex patterns and representations in the data. Deep neural networks can easily pull-out hierarchical features because of their depth. This makes them good at learning features and abstracting them. Many jobs, such as picture classification, object recognition, machine translation, and voice synthesis, have been done very well by DNNs. However, training deep networks can be hard on computers and may need a lot of tagged data. Hardware improvements

and better training methods have made DNNs much more useful and effective, strengthening their place as a mainstay of modern machine learning and artificial intelligence.

RBM (CNN + BiLSTM)

A DL design called a Recurrent Boltzmann Machine (RBM) combines a Convolutional Neural Network (CNN) and Bidirectional Long Short-Term Memory (BiLSTM). It is used for many things, such as handling images and sequences. The CNN takes in data like images and pulls out spatial features, while the BiLSTM finds trends that happen in a certain order. RBM adds the ability to generate and distinguish. These parts work together to make a strong model that can learn hierarchical structures from complex data. This model can handle both spatial and time information, which makes it useful for tasks like picture recognition, natural language processing, and more.

CNN + LSTM

A mixed DL design is made up of a Convolutional Neural Network (CNN) and a Long Short-Term Memory (LSTM). CNN is great at taking out spatial traits from data, which makes it perfect for picture analysis. LSTM, on the other hand, is great at dealing with sequential data, like natural language. When CNN and LSTM work together, CNN can pull out useful features from the input, and LSTM handles these features in order, recording how they change over time. This combination is very helpful for tasks like video analysis, which needs both geographical and time information, and for natural language tasks, which need to understand the context and links between words in a string of text.

Feature extraction

The next step is to extract relevant features from the pre-processed data. Features are the characteristics of the data that will be used by ML/AI models to identify malicious patterns. Some common features used in intrusion detection include:

- Packet size: The size of network packets can be indicative of malicious activity.
- Packet direction: The direction of network packets can be used to identify unusual traffic patterns.
- Port numbers: The port numbers used in network traffic can be used to identify malicious applications.
- Protocol types: The protocol types used in network traffic can be used to identify malicious protocols.

The specific features used will depend on the specific ML/AI models that will be used to analyze the data.

Model training

The next step is to train a ML/AI model to identify malicious patterns in the features. There are many different types of ML/AI models that can be used for intrusion detection, including:

- Decision trees: Decision trees are a type of supervised learning model that can be used to classify data.
- Support vector machines (SVMs): SVMs are a type of supervised learning model that can be used to classify data and to detect outliers.
- Neural networks: Neural networks are a type of unsupervised learning model that can be used to learn patterns from data.

The specific ML/AI model used will depend on the specific characteristics of the data and the desired performance of the intrusion detection system.

Real-time analysis

The next step is to analyze network traffic in real time using the trained model. This involves continuously monitoring the network traffic and classifying it as either malicious or non-malicious. The classified traffic is then used to generate alerts when malicious activity is detected.

Alert generation

The final step is to generate alerts when malicious activity is detected. Alerts should include information about the type of attack, the source of the attack, and the target of the attack. Alerts can be sent to a variety of destinations, such as a security console, an email address, or a pager.

6.2 RESULT:

The results of real-time intrusion detection systems for IoT networks can be measured in terms of:

- **Detection rate:** The percentage of malicious attacks that are detected.
- **False positive rate:** The percentage of non-malicious activity that is incorrectly classified as malicious.
- **Response time:** The time it takes to detect and respond to an attack.

In general, real-time intrusion detection systems for IoT networks can achieve high detection rates and low false positive rates. The response time can vary depending on the complexity of the network and the resources available to the IDS.

CHAPTER VII

OUTPUT

Screenshot of the output:

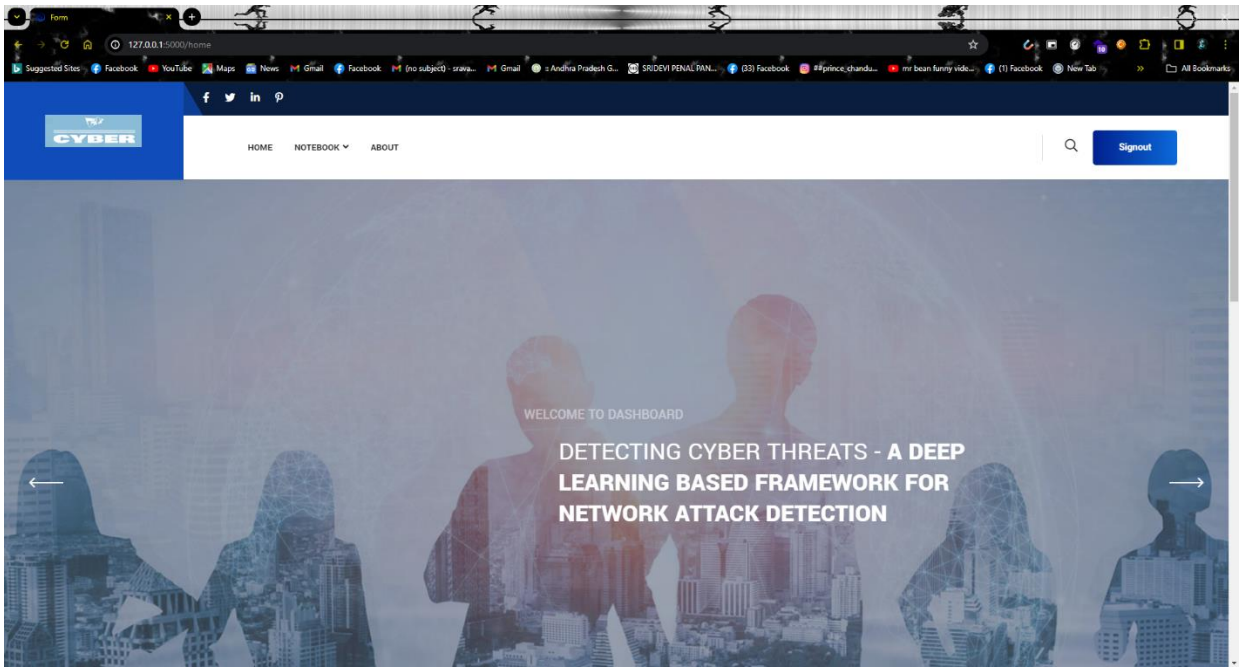

Fig.7.1: Dashboard

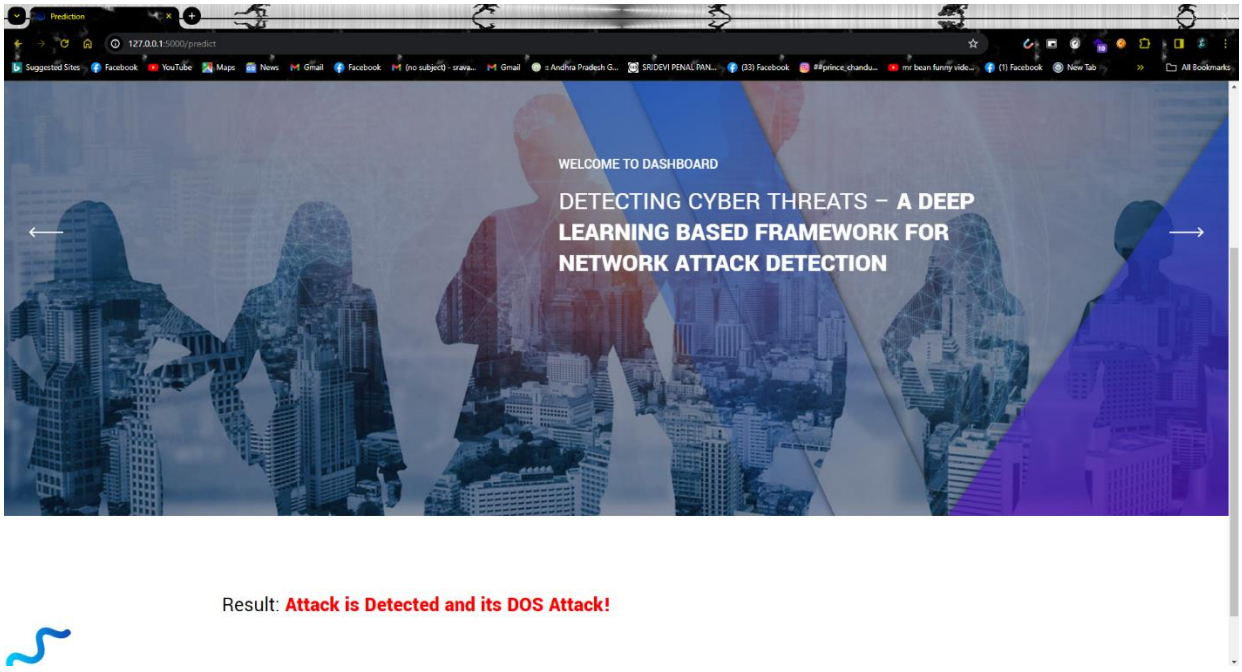

Fig.7.2: Attack Prediction

CHAPTER VIII

CONCLUSION AND FUTURE WORK

This project discusses the involving challenges and limitations in previous studies, which have been investigating how to use deep learning in the early detection and eradication of cyber threats. We employ deep learning techniques for cyber-attack malware detection, such as identification and discriminative. However, we summarized the seven approaches, i.e., deep learning (RNN, CNN, and DNN) and generative models/methods (RBN, DBN, DBM., and DA). In addition, our investigation focuses on accuracy and provided dictionaries in the research field. The experimentation of our work demonstrates IDS and Cybersecurity attacks, which are detected successfully using a collaborative technological environment. Also, we have investigated to find which deep learning techniques performed better among the others. According to this analysis, the use of deep learning methods increases the investigational rate of classification intrusion while providing a robust performance of state-of-the-art supervised systems.

In this scenario, a part of future work, this study extended to include advanced deep learning methods and transfer learning approaches. Moreover, the robustness of the supervised system is validated using IDS training. Thus, when designing a newfangled Intrusion Detection System (IDS), the properties can be used in the real-time system to detect internal and external intruders and their malicious behaviors.

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. E. Hinton, ‘‘ImageNet classification with deep convolutional neural networks,’’ Commun. ACM, vol. 60, no. 2, pp. 84–90, Jun. 2017.

[3] M. K. Islam, M. S. Ali, M. M. Ali, M. F. Haque, A. A. Das, M. M. Hossain, D. S. Duranta, and M. A. Rahman, ‘‘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, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, ‘‘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.

[6] Z. Dewa and L. A. Maglaras, ‘‘Data mining and intrusion detection systems,’’ Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 1, pp. 1–10, 2016.

[7] B. Stewart, L. Rosa, L. A. Maglaras, T. J. Cruz, M. A. Ferrag, P. Simoes, and H. Janicke, ‘‘A novel intrusion detection mechanism for SCADA systems which automatically adapts to network topology changes,’’ EAI Endorsed Trans. Ind. Netw. Intell. Syst., vol. 4, no. 10, p. e4, 2017.

[8] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, ‘‘Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,’’ J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102419.

[9] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, ‘‘A bidirectional LSTM deep learning approach for intrusion detection,’’ Expert Syst. Appl., vol. 185, Dec. 2021, Art. no. 115524.

[10] A. A. Salih, S. Y. Ameen, S. R. Zeebaree, M. A. Sadeeq, S. F. Kak, N. Omar, I. M. Ibrahim, H. M. Yasin, Z. N. Rashid, and Z. S. Ageed, ‘‘Deep learning approaches for intrusion detection,’’ Asian J. Res. Comput. Sci., vol. 9, no. 4, pp. 50–64, 2021.

[11] J. Azevedo and F. Portela, ‘‘Convolutional neural network—A practical case study,’’ in Proc. Int. Conf. Inf. Technol. Appl. Singapore: Springer, 2022, pp. 307–318.

[12] K. He, X. Zhang, S. Ren, and J. Sun, ‘‘Deep residual learning for image recognition,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 770–778.

[13] J. Yosinski, J. Clune, Y. Bengio, and H. Lipson, ‘‘How transferable are features in deep neural networks?’’ in Proc. Adv. Neural Inf. Process. Syst., vol. 27, 2014, pp. 1–9.

[14] G. Awad, C. G. Snoek, A. F. Smeaton, and G. Quénot, ‘‘Trecvid semantic indexing of video: A 6-year retrospective,’’ ITE Trans. Media Technol. Appl., vol. 4, no. 3, pp. 187–208, 2016.

[15] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, ‘‘Rethinking the inception architecture for computer vision,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2016, pp. 2818–2826.

[16] M. Uddin, R. Alsaqour, and M. Abdelhaq, ‘‘Intrusion detection system to detect DDoS attack in Gnutella hybrid P2P network,’’ Indian J. Sci. Technol., vol. 6, no. 2, pp. 71–83, 2013.

[17] R. L. Haupt and S. E. Haupt, Practical Genetic Algorithms. Wiley, 2004, doi: 10.1002/0471671746.

[18] D. Hossain, G. Capi, and J. M., ‘‘Optimizing deep learning parameters using genetic algorithm for object recognition and robot grasping,’’ J. Electron. Sci. Technol., vol. 16, no. 1, pp. 11–15, 2018.

[19] O. E. David and I. Greental, ‘‘Genetic algorithms for evolving deep neural networks,’’ in Proc. Companion Publication Annu. Conf. Genetic Evol. Comput., Jul. 2014, pp. 1451–1452.

[20] J. Gu and S. Lu, ‘‘An effective intrusion detection approach using SVM with Naïve Bayes feature embedding,’’ Comput. Secur., vol. 103, Apr. 2021, Art. no. 102158.

[21] E. Gyamfi and A. Jurcut, ‘‘Intrusion detection in Internet of Things systems: A review on design approaches leveraging multi-access edge computing, machine learning, and datasets,’’ Sensors, vol. 22, no. 10, p. 3744, May 2022.

[22] A. K. Balyan, S. Ahuja, U. K. Lilhore, S. K. Sharma, P. Manoharan, A. D. Algarni, H. Elmannai, and K. Raahemifar, ‘‘A hybrid intrusion detection model using EGA-PSO and improved random forest method,’’ Sensors, vol. 22, no. 16, p. 5986, Aug. 2022.

[23] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu, and K. I.-K. Wang, ‘‘Hierarchical adversarial attacks against graph-neural-network-based IoT network intrusion detection system,’’ IEEE Internet Things J., vol. 9, no. 12, pp. 9310–9319, Jun. 2021.

[24] A. A. Khan, A. A. Laghari, T. R. Gadekallu, Z. A. Shaikh, A. R. Javed, M. Rashid, V. V. Estrela, and A. Mikhaylov, ‘‘A drone-based data management and optimization using Metaheuristic algorithms and blockchain smart contracts in a secure fog environment,’’ Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108234.

[25] K. Gupta, D. K. Sharma, K. Datta Gupta, and A. Kumar, ‘‘A tree classifier based network intrusion detection model for Internet of Medical Things,’’ Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108158.

Conference Acceptance Letter:

NATIONAL CONFERENCE

NCACSI - 24

NATIONAL CONFERENCE ON ADVANCED COMPUTER SCIENCE AND INFORMATION TECHNOLOGY (NCACSI - 24)

6th April 2024 Bangalore, India

Acceptance Letter

Authors Name: R. Syed Ali Fathima, S. Karthik Reddy, K. Nikhil Chowdary, D. Jaya Sai Manjunath, P. Partha Saradhi Reddy

Dear Authors,

We are pleased to inform you that your paper has been accepted by the review committee for Oral / Poster Presentation at the **NATIONAL CONFERENCE ON ADVANCED COMPUTER SCIENCE AND INFORMATION TECHNOLOGY (NCACSI - 24)**

Article Title: **DETECTING CYBER THREATS - A DEEP LEARNING BASED FRAMEWORK FOR NETWORK ATTACK DETECTION**

Paper ID: **National Conference_0395261**

This conference will be held on **6th April 2024 in Bangalore, India**

Your paper will be published in the conference proceeding and Well reputed journal after registration.

Please register as soon as possible in order to secure your participation:

https://www.nationalconference.in/event/registration.php?id=2480882

You are requested to release the payment and mail us the screen of successful payment release with your name and title of paper to confirm your registration.

Sincerely,

NATIONAL CONFERENCE NC

Dr. Tara Srivastava
National Conference

+91 96770 07228 info@nationalconference.in www.nationalconference.in

Certificate of Presentation:

Google Meet

CERTIFICATE
OF PRESENTATION

NATIONAL CONFERENCE

National Conference on Advanced Computer Science and Information Technology (NCACSI - 24)

6th April 2024 | Bangalore, India

This is to certify that **R. Syed Ali Fathima** affiliated with Kalasalingam Academy Of Research And Education Virudhunagar, Tamil Nadu, India has presented a paper titled "Detecting Cyber Threats - A Deep Learning Based Framework For Network Attack Detection"

at the esteemed International Conference organized by the National Conference (NC) held on 6th April 2024 at Bangalore, India.

CiteFactor Academic Scientific Journals

Dr. Tara Srivastava
Director

NC

Raj Kumar
Co-ordinator

Crossref

Google Meet

CERTIFICATE
OF PRESENTATION

NATIONAL CONFERENCE

National Conference on Advanced Computer Science and Information Technology (NCACSI - 24)

6th April 2024 | Bangalore, India

This is to certify that **P. Partha Saradhi Reddy** affiliated with Kalasalingam Academy Of Research And Education Virudhunagar, Tamil Nadu, India has presented a paper titled "Detecting Cyber Threats - A Deep Learning Based Framework For Network Attack Detection"

at the esteemed International Conference organized by the National Conference (NC) held on 6th April 2024 at Bangalore, India.

CiteFactor Academic Scientific Journals

Dr. Tara Srivastava
Director

NC

Raj Kumar
Co-ordinator

Crossref

Google Meet

CERTIFICATE
OF PRESENTATION

NATIONAL CONFERENCE

National Conference on Advanced Computer Science and Information Technology (NCACSI - 24)

6th April 2024 | Bangalore, India

This is to certify that **K. Nikhil Chowdary** affiliated with Kalasalingam Academy Of Research And Education Virudhunagar, Tamil Nadu, India has presented a paper titled "Detecting Cyber Threats - A Deep Learning Based Framework For Network Attack Detection"

at the esteemed International Conference organized by the National Conference (NC) held on 6th April 2024 at Bangalore, India.

CiteFactor Academic Scientific Journals

Dr. Tara Srivastava
Director

NC

Raj Kumar
Co-ordinator

Crossref

Google Meet

CERTIFICATE
OF PRESENTATION

NATIONAL CONFERENCE

National Conference on Advanced Computer Science and Information Technology (NCACSI - 24)

6th April 2024 | Bangalore, India

This is to certify that **S. Karthik Reddy** affiliated with Kalasalingam Academy Of Research And Education Virudhunagar, Tamil Nadu, India has presented a paper titled "Detecting Cyber Threats - A Deep Learning Based Framework For Network Attack Detection"

at the esteemed International Conference organized by the National Conference (NC) held on 6th April 2024 at Bangalore, India.

CiteFactor Academic Scientific Journals

Dr. Tara Srivastava
Director

NC

Raj Kumar
Co-ordinator

Crossref


Google Meet
CERTIFICATE
OF PRESENTATION
NATIONAL CONFERENCE
National Conference on Advanced Computer Science and Information Technology (NCACSI - 24)
6th April 2024 | Bangalore, India
This is to certify that D. Jaya Sai Manjunath affiliated with
Kalasalingam Academy Of Research And Education Virudhunagar, Tamil Nadu, India has presented a paper titled
"Detecting Cyber Threats - A Deep Learning Based Framework For Network Attack Detection"
at the esteemed International Conference organized by the National Conference (NC) held on 6th April 2024
at Bangalore, India.
CiteFactor
Dr. Tara Srivastava
Director
NC
Raj Kumar
Co-ordinator
Crossref

DETECTING CYBER THREATS – A DEEP LEARNING BASED FRAMEWORK FOR NETWORK ATTACK DETECTION

ORIGINALITY REPORT

10%	6%	8%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	1%
2	K. Muthamil Sudar, P. Nagaraj, V. Muneeswaran, S. Kavya Jeevana Swetha, K. Madhuri Nikhila, R. Venkatesh. "An Empirical Data Analytics and Visualization for UBER Services: A Data Analysis Based Web Search Engine", 2022 International Conference on Computer Communication and Informatics (ICCCI), 2022 Publication	1%
3	Irfan Ali Kandhro, Sultan M. Alanazi, Fayyaz Ali, Asadullah Kehar, Kanwal Fatima, Mueen Uddin, Shankar Karuppayah. "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures", IEEE Access, 2023 Publication	1%
4	Submitted to Rangsit University Student Paper	1%

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade

INTERNAL QUALITY ASSURANCE CELL
PROJECT AUDIT REPORT

This is to certify that the project work entitled "Detecting cyber threats – A Deep Learning based Framework for Network Attack Detection" categorized as an internal project done by DESHA JAYA SAI MANJUNATH, KOLLIPATI NIKHIL CHOWDARY, SIRUPA KARTHIK REDDY , PALLE PARTHA SARADHI REDDY of the Department of Computer Science and Engineering, under the guidance of MS.R.SYED ALI FATHIMA during the Even semester of the academic year 2023 - 2024 are as per the quality guidelines specified by IQAC.

Quality Grade

Deputy Dean (IQAC)

Administrative Quality Assurance **Dean(IQAC)**