A

Mini Project

On

TOWARD DETECTION AND ATTRIBUTION OF CYBER ATTACKS IN IOT-ENABLED CYBER-PHYSICAL SYSTEMS

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

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

G.RAHUL (207R1A05L1)

Under the guidance of

Mr.M.MADHUSUDAN

(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 UGCAct.1956, Kandlakoya (V), Medchal Road, Hyderabad-501401.

2020-2024

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"TOWARD DETECTION AND ATTRIBUTION OF CYBER-ATTACKS IN IOT-ENABLED CYBER-PHYSICAL SYSTEMS"** being submitted by **G.RAHUL (207R1A05L1)** in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Engineering to the Jawaharlal Nehru Technological University Hyderabad , is a record of bonafide work carried out by them under our guidance and supervision during the year 2023-2024.

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

Mr.M.Madhusudan
(Assistant professor)
INTERNAL GUIDE

Dr. A. Raji Reddy
DIRECTOR

DR. K. Srujan Raju
HOD

EXTERNAL EXAMINER

Submitted for viva voice Examination held on_____

ACKNOWLEDGEMENT

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 **Mr.M.Madhusudan,** Assistant Professor**,**for his exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by him 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 the Project Review Committee (PRC) **G.Vinesh Shanker, Dr. J. Narasimharao, Ms. Shilpa, & Dr. K. Maheswari** for their cordial support, valuable information and guidance, which helped us in completing this task through various stages.

We are also thankful to **Dr. K. Srujan Raju,** Head, 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 throughout the course of this project. We also 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.

G.RAHUL (207R1A05L1)

ABSTRACT

Securing Internet of Things (IoT)-enabled cyber- physical systems (CPS) can be challenging, as security solutions developed for general information / operational technology (IT / OT) systems may not be as effective in a CPS setting. Thus, this paper presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS).

At the first level, a decision tree combined with a novel ensemble deep representation- learning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution. The proposed model is evaluated using real-world datasets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.

The expanding realm of IoT-enabled cyber-physical systems, the escalating interconnectedness gives rise to unprecedented vulnerabilities in the face of cyber threats. This research endeavours to address the imperative need for establishing robust mechanisms for detecting and attributing these cyber-attacks. The study initiates with a comprehensive examination of the dynamic threat landscape, accompanied by an elucidation of the formidable challenges posed by identifying and attributing such attacks in this context.

Fundamental principles of intrusion detection systems (IDS) are explored, emphasizing their adaptability to the unique characteristics of IoT-enabled cyber-physical systems. The application of machine learning and anomaly detection techniques is scrutinized as a means to analyze real-time data from sensors and devices. These techniques can pinpoint irregularities, deviations, and suspicious patterns, which are indicative of cyber-attacks. The study further delves into the complexities of attack attribution, including the challenges of ascertaining the source of these attacks within the intricate web of interconnected systems. Innovative methodologies for correlating and attributing attacks are proposed, incorporating insights from network forensics and threat intelligence.

In this rapidly evolving landscape, where the fusion of physical and digital realms defines modern industry, the paramount importance of safeguarding IoT-enabled cyber-physical systems cannot be overstated.

LIST OF FIGURES/TABLES

LIST OF SCREENSHOTS

TABLE OF CONTENTS

TABLE OF CONTENTS

1. INTRODUCTION

1.INTRODUCTION

1.1 PROJECT SCOPE

Securing Internet of Things (IoT) can be challenging, as security may not be as effective in a CPS settings So, there is a need for effective cyber-attack detection and attribution in Internet of Things (IoT) enabled cyber-physical systems (CPS). The cyber-attacks can disturb critical services ,loss of confidential information. There is a two-level ensemble attack detection and attribution framework designed for CPS. At the first level, a decision tree combined with deep representation- learning model is developed for detecting attack At the second level, a deep neural network is designed for attack attribution.

.

1.2 PROJECT PURPOSE

The purpose of a project focused on the “Towards detection and attribution of cyber-physical systems in IoT ,typically involves addressing the security and reliability challenges associated with IoT devices and systems that are interconnected in the physical world. Enhancing the security of IoT devices and cyber-physical systems is a primary objective. This including identifying vulnerabilities, developing security protocols, and implementing encryption techniques to protect data and communication channels within the IoT ecosystem.

1.3 PROJECT FEATURES

Detecting and attributing cyber-physical system (CPS) attacks in an Internet of Things(IoT) project involves implementing various features and techniques to enhance security. Encrypt data both in transit and at rest to protect sensitive information from eavesdropping and tampering. Integrate threat intelligence feeds to stay updated on the latest threats and improve the accuracy of attack attribution. Enforce strong authentication mechanisms for IoT devices, including device certificates or biometric authentication where feasible. Implement a device identify and access management systems.

2. SYSTEM ANALYSIS

2.SYSTEM ANALYSIS

2.1 INTRODUCTION

System Analysis is the important phase in the system development process. The System is studied to the minute details and analyzed. The system analyst plays an important role of an interrogator and dwells deep into the working of the present system. In analysis, a detailed study of these operations performed by the system and their relationships within and outside the system is done. A key question considered here is, "what must be done to solve the problem?" The system is viewed as a whole and the inputs to the system are identified. Once analysis is completed the analyst has a firm understanding of what is to be done.

2.2 PROBLEM DEFINITION

Cyber-physical systems (CPS) are integral components of the Internet of Things (IoT) that integrate physical processes with digital control systems, enabling automation and remote monitoring of critical infrastructures such as smart cities, industrial plants, and healthcare systems. However, the interconnected nature of CPS within IoT networks exposes them to various cyber threats, including malware, ransomware, denial-of-service attacks, and data breaches. These threats can lead to significant disruptions, safety hazards, and financial losses. Therefore, the problem is to develop effective methods for the detection and attribution of cyber-physical system attacks in IoT environments.

2.3 EXISTING SYSTEM

The comparative summary suggested that the RF algorithm has the best attack detection, with a recall of 0.9744; the ANN is the fifth-best algorithm, with a recall of 0.8718; and the LR is the worst- performing algorithm, with a recall of 0.4744. The authors also reported that the ANN could not detect 12.82% of the attacks and considered 0.03% of the normal samples to be attacks.

In addition, LR, SVM, and KNN considered many attack samples as normal samples, and these ML algorithms are sensitive to imbalanced data. In other words, they are not suitable for attack detection in ICS. The authors presented a KNN algorithm to detect cyber-attacks on gas pipelines. To minimize the effect of using an imbalanced dataset in the algorithm, they performed oversampling on the dataset to achieve balance. Using the KNN on the balanced dataset, they reported an accuracy of 97%, a precision of 0.98, a recall of 0.92, and an f-measure of 0.95.

The authors presented a Logical Analysis of Data (LAD) method to extract patterns/rules from the sensor data and use these patterns/rules to design a two-step anomaly detection system. In the first step, a system is classified as stable or unstable, and in the second one, the presence of an attack is determined. They compared the performance of the proposed LAD method with the DNN, SVM, and CNN methods. Based on these experiments, the DNN outperformed the LAD method in the precision metric; however, the LAD performed better in recall and f-measure.

2.3.1 DISADVANTAGES OF EXISTING SYSTEM

Following are the disadvantages of existing system:

- Limited Scalability: Large scale attacks cannot be handled. It is difficult to detect and attribute cyber-attacks in real-time.
- False Positives: Sometimes, it will fail to detect the attack.
- Privacy Concerns: Existing systems may not be able to protect private data from cyber-attacks or unauthorized access.
- Less Accuracy
- Low Efficiency

2.4 PROPOSED SYSTEM

Attack attribution seeks to answer the question of “What kind of attack was it?” and this is generally more challenging to answer in ICS than in typical IT/OT systems due to the different network structures, industry-specific protocols, and so forth. While there have been a small number of ML-based malware attack attributions , designing robust and effective ML-based attack attribution for ICS and IIoT systems appears to be understudied.

Thus, this paper proposes a two-stage ensemble deep learning-based attack detection and attack attribution framework for ICS. Our approach incorporates both process and physical data to solve the im- balanced data problem without subsampling or oversampling. The proposed framework utilizes an unsupervised ensemble of learned representations from normal and attack instances for attack detection. Next, using an ensemble of several one-vs-all classifiers trained on each attack attribute, it forms a two-part DNN to attribute the samples into their corresponding attack attributes.

2.4.1 ADVANTAGES OF THE PROPOSED SYSTEM

- Early Detection of Cyber-Attacks: It provides warning to prevent or mitigate the impact of the attack.
- Real-time Monitoring: The system continuously monitors, if any unusual activity or behavior happens it will indicate.
- Cost-Effective: It does not require the deployment of additional hardware or infrastructure.
- High Efficiency.
- High Accuracy.

2.5 FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and a 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. Three key considerations involved in the feasibility analysis:

- EconomicFeasibility
- TechnicalFeasibility
- SocialFeasibility

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.6 HARDWARE & SOFTWARE REQUIREMENTS

2.6.1 HARDWARE REQUIREMENTS:

Hardware interfaces specify the logical characteristics of each interface between the software product and the hardware components of the system. The following are some hardware requirements.

- Processor : Intel I3 and above
- Hard disk : 40GB and above
- RAM : 4GB and above
- Input devices : Keyboard, mouse.

2.6.2 SOFTWARE REQUIREMENTS:

Software Requirements specifies the logical characteristics of each interface and software components of the system. The following are some software requirements:

- Operating system : Windows 8 and above
- Languages : Python, Django, MySql
- Tools: Python IDEL3.7 version, Anaconda - Jupyter, Spyder, MySqlclient, WampServer 2.4

3. ARCHITECTURE

3.ARCHITECTURE

3.1 PROJECT ARCHITECTURE

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

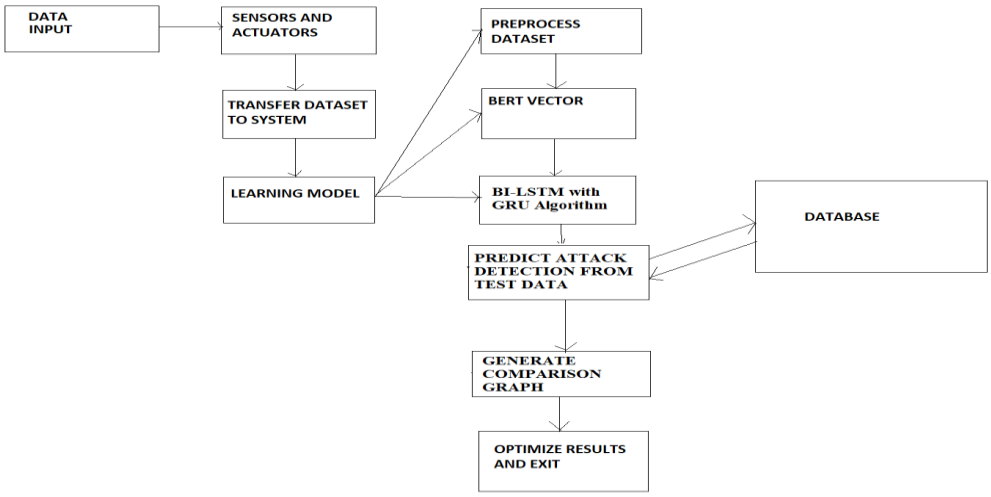


Figure 3.1: Project Architecture for Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems

3.2 DESCRIPTION

- The Unique characteristics such as heterogeneity, complexity and inter-connectedness pose significant security for IoT-enabled cyber-physical systems (CPS).
- Detection involves identifying ongoing attacks, whereas attribution involves identifying the attacker, responsible for the attack.
- Machine learning can learn from data and adapt to changing conditions, making it well-suited for cyber-security applications.

3.3 USE CASE DIAGRAM

In the use case diagram, we have basically one actor who is the user in the trained model.

A use case diagram is a graphical depiction of a user's possible interactions with a system. A use case diagram shows various use cases and different types of users the system has. The use cases are represented by either circles or ellipses. The actors are often shown as stick figures.

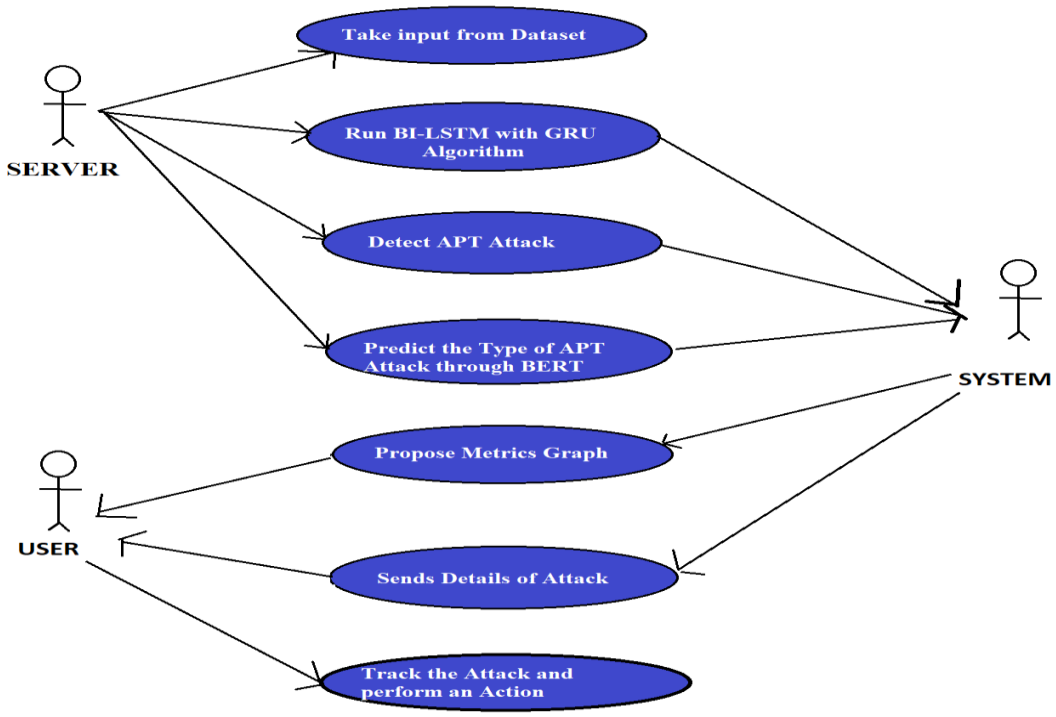


Figure 3.2: Use Case Diagram for Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems

3.4 CLASS DIAGRAM

Class diagram 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 objects.

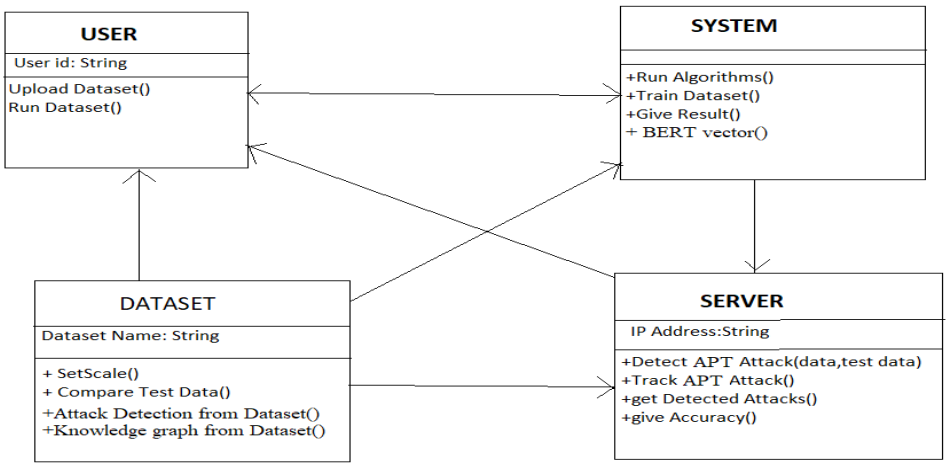


Figure 3.3: Class Diagram for Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems

3.5 SEQUENCE DIAGRAM

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the logical view of the system under development.

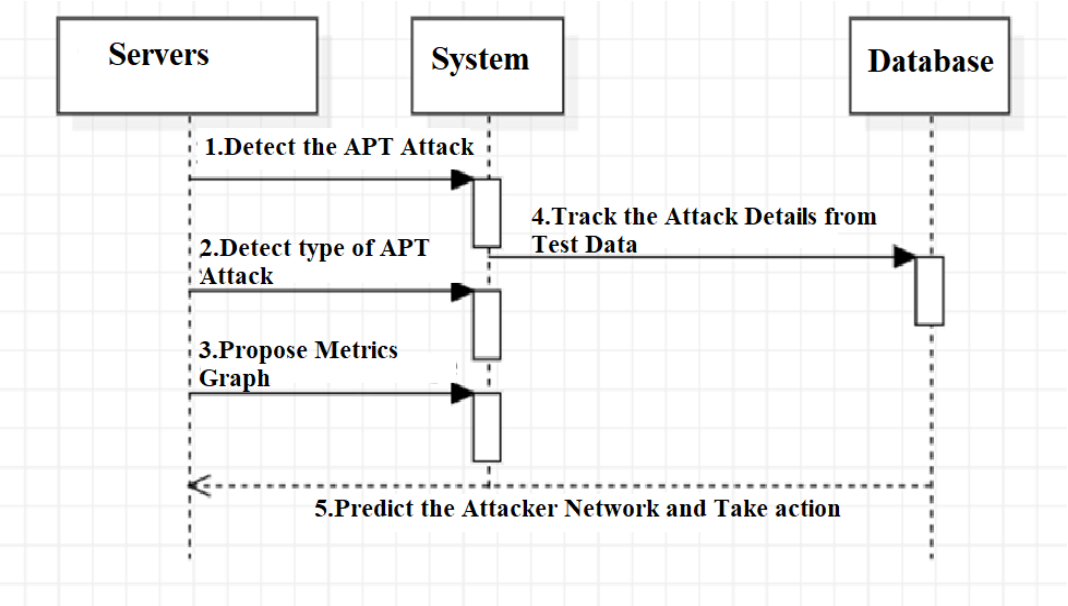


Figure 3.4: Sequence Diagram for Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems

3.6 ACTIVITY DIAGRAM

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. They can also include elements showing the flow of data between activities through one or more data stores.

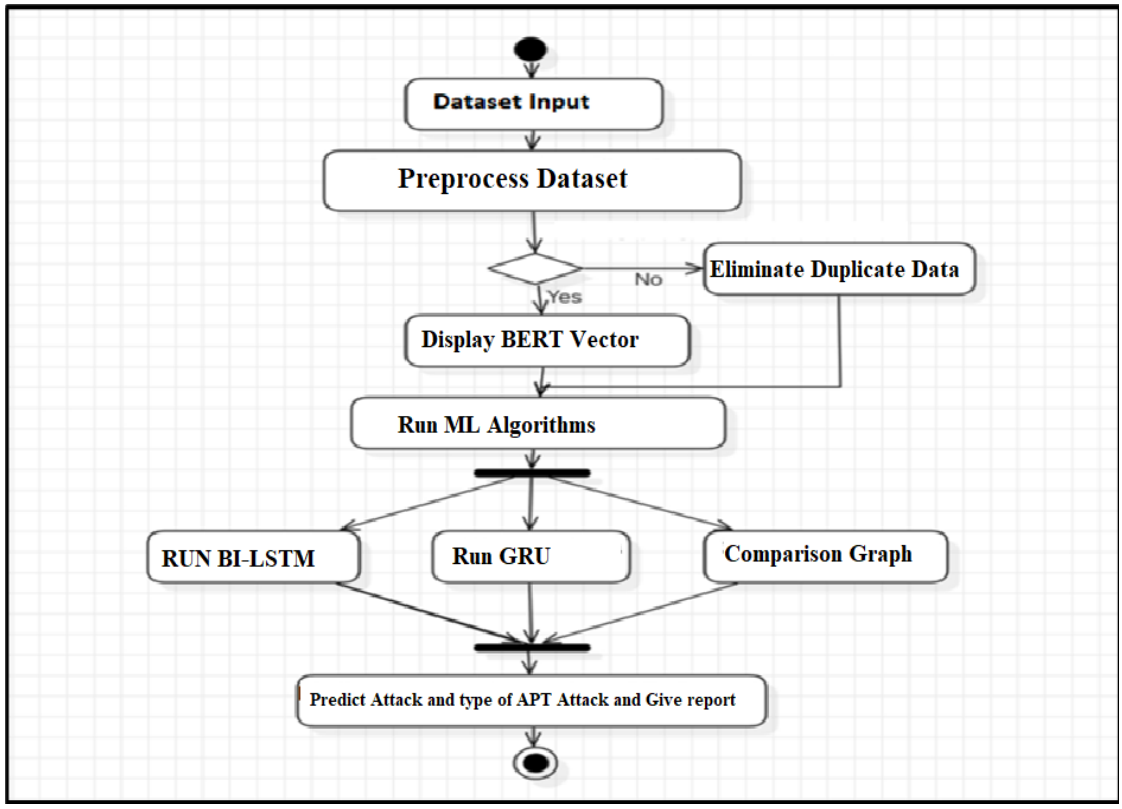


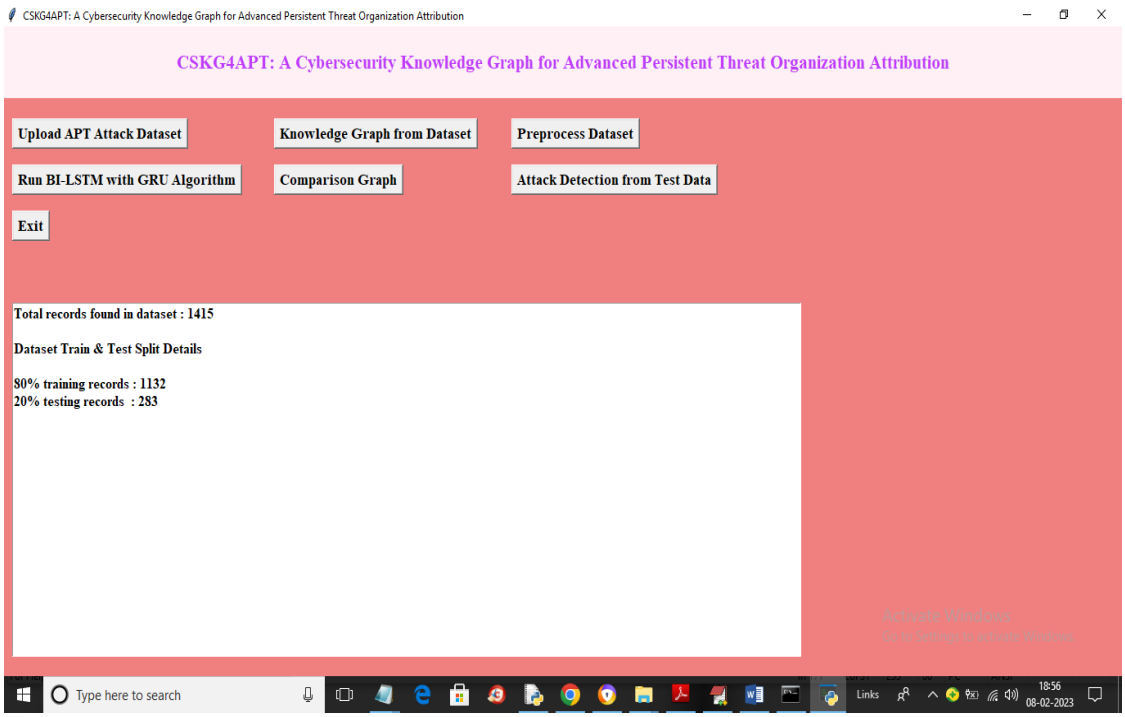
Figure 3.5: Activity Diagram for Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems

4. IMPLEMENTATION

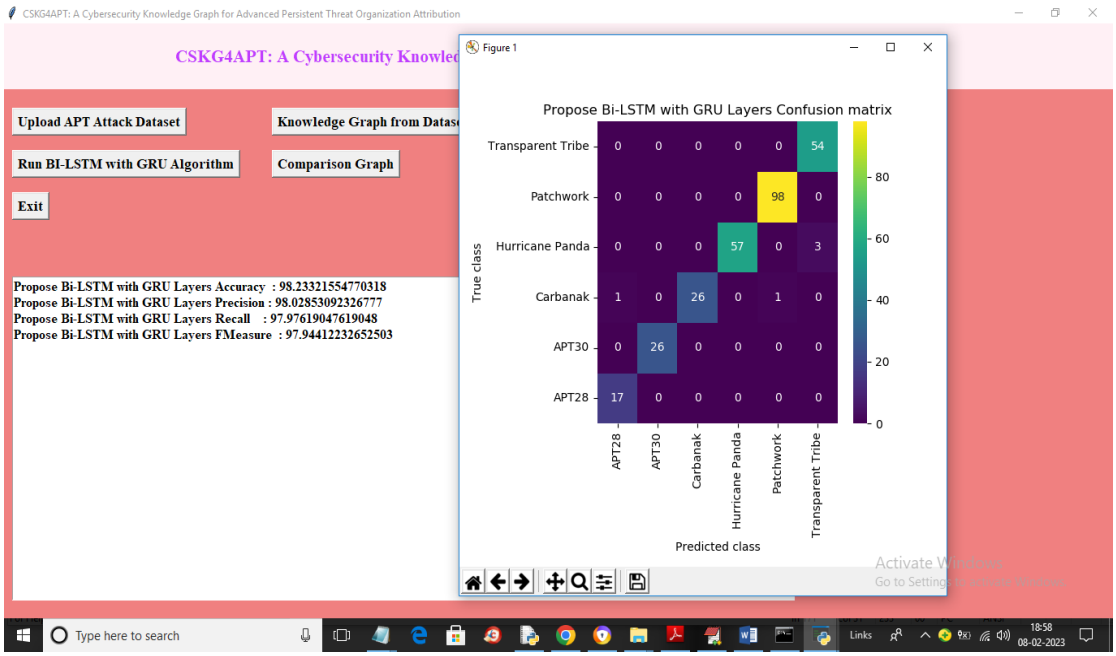
4.1 SAMPLE CODE

```
import matplotlib.pyplot as plt
import pandas as pd
import numpy as np
main = tkinter.Tk()
main.title("CSKG4APT: A Cybersecurity
Knowledge Graph for Advanced Persistent
Threat Organization Attribution") #designing
main screen
main.geometry("1000x650")
global dataset, X, Y, bilstm
global X_train, X_test, y_train, y_test
global accuracy, precision, recall, fscore,
labels, scaler, le1, le2


def loadDataset():
    global dataset, labels
    filename =
filedialog.askopenfilename(initialdir="Dataset")
    text.delete('1.0', END)
    text.insert(END,filename+" loaded\n\n");
    dataset = pd.read_csv(filename)
    text.insert(END,str(dataset.head()))
    labels = np.unique(dataset['apt'])
    label = dataset.groupby('apt').size()
    label.plot(kind="bar")
    plt.title("APT attacks found in Dataset")
    plt.show() os

def graph():
    global accuracy, precision, recall, fscore
    height = [accuracy, precision, recall, fscore]
    bars = ('Accuracy','Precision','Recall','FScore')
    y_pos = np.arange(len(bars))
    plt.bar(y_pos, height)
    plt.xticks(y_pos, bars)
    plt.xlabel("Comparison Matrics")
    plt.ylabel("Metric Values")
    plt.title("Propose Bi-LSTM with GRU Layer
Comparison Graph")
    plt.show()
```

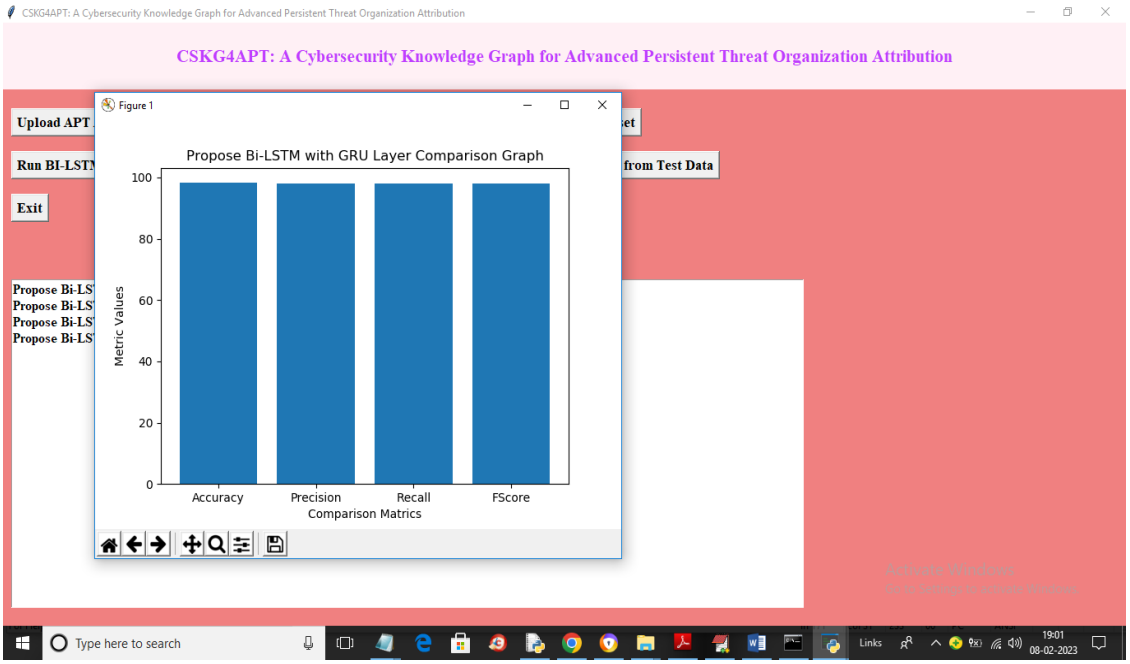
5. SCREENSHOTS



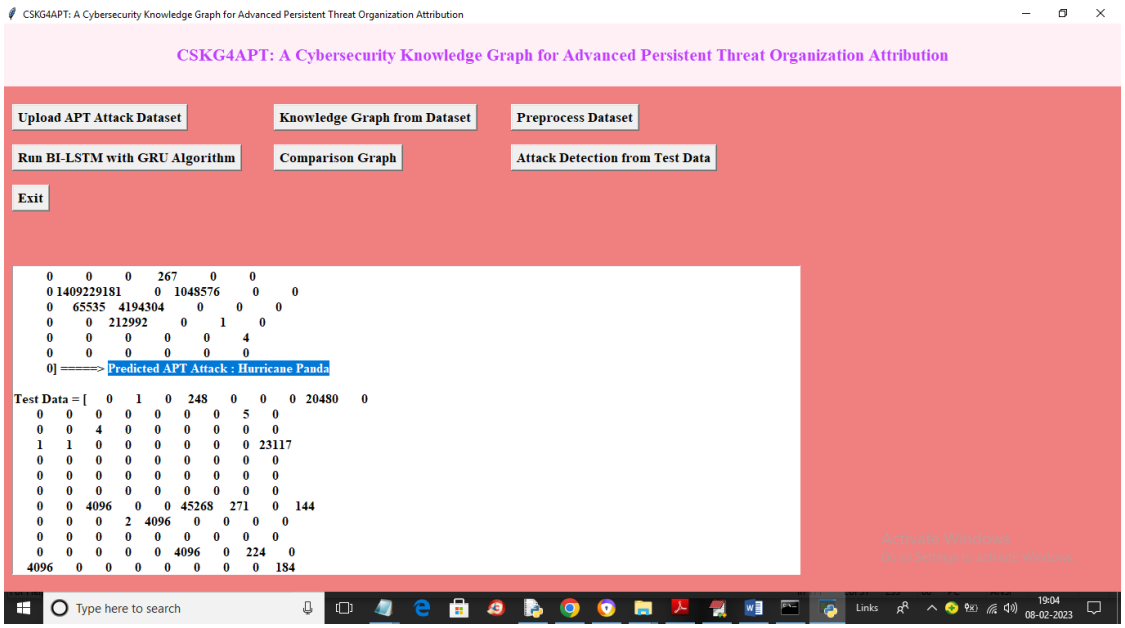
Screenshot 5.1: preprocess dataset in the given dataset



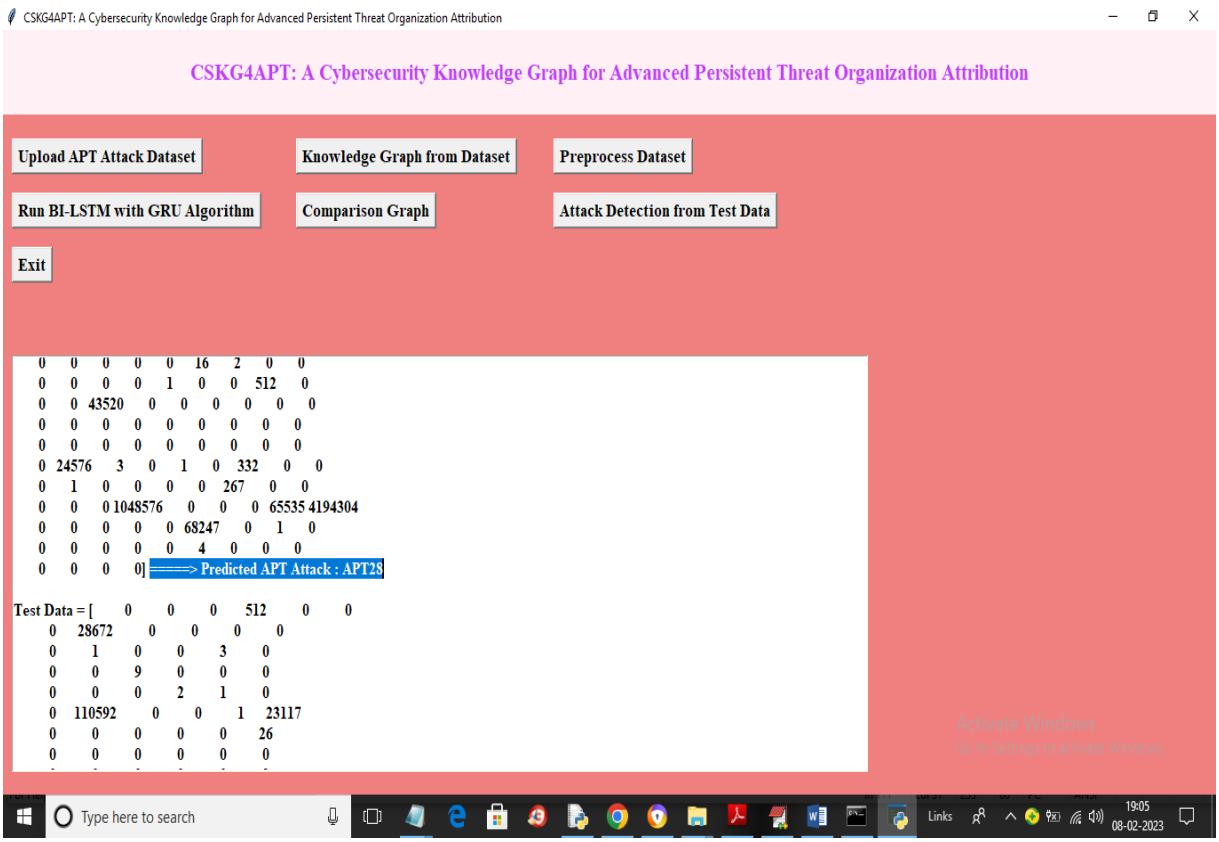
Screenshot 5.2: propose Bi-LSTM with GRU confusion matrix



Screenshot 5.3: Bi-LSTM with GRU layer Comparison matrices



Screenshot 5.4: Attack Detection from Test Data of Hurricane Panda



Screenshot 5.5: Attack Detection from Test Data of APT28

6. TESTING

6.TESTING

6.1 INTRODUCTION TO TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, subassemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

6.2 TYPES OF TESTING

6.2.1 UNIT TESTING

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

6.2.2 INTEGRATION TESTING

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit

testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

6.2.3 FUNCTIONAL TESTING

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input	: identified classes of valid input must be accepted.
Invalid Input	: identified classes of invalid input must be rejected.
Functions	: identified functions must be exercised.
Output	: identified classes of application outputs must be exercised.
Systems/Procedures	: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions, or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

6.3 TEST CASES

6.3.1 CLASSIFICATION

S.NO	Test Case	Excepted Result	Result	Remarks(IF Fails)
1.	User Register	If User registration successfully.	Pass	If already user email exist then it fails.
2.	User Login	If Username and password is correct then it will getting valid page.	Pass	Un Register Users will not logged in.
3.	User View User	Show our dataset	Pass	If Data set Not Available fail.
4.	View Fast History Results	The Four Alarm Score Should be Displayed.	Pass	The Four Alarm Score Not Displaying fail
5.	User Prediction	Display Review with true results	Pass	Results not True Fail
6.	Show Detection process	Display Detection process	Pass	Results Not True Fail
7.	Show Eye Blink Process	Display Eye Blink Process	Pass	If Results not Displayed Fail.
8.	Admin login	Admin can login with his login credential. If success he get his home page	Pass	Invalid login details will not allowed here
9.	Admin can activate the register users	Admin can activate the register user id	Pass	If user id not found then it won't login
10.	Results	For our Four models the accuracy and F1 Score	Pass	If Accuracy And F1 Score Not Displayed fail

7. CONCLUSION

7. CONCLUSION & FUTURE SCOPE

7.1 PROJECT CONCLUSION

- The project focus on developing innovative techniques for detecting and attributing cyber-attacks in these systems using machine learning algorithms.
- The project involves cybersecurity, machine learning, and IoT - enabled CPS, consists a more comprehensive view of the problem, leading to effective solutions.
- It is essential to implement proper security protocols, such as authentication and encryption, to prevent unauthorized access and data breaches.

7.2 FUTURE SCOPE

- **Behavioral Analysis**: Develop behavioral analysis models that can detect anomalies in the behavior of IoT devices and cyber-physical systems.
- **Real-time Monitoring**: Implement real-time monitoring and alerting systems that can quickly identify and respond to suspicious activities or anomalies in IoT networks and CPS, enabling the early detection of potential attacks.
- **Privacy Preservation**: Ensure that the project considers privacy preservation techniques, especially when dealing with data collection and analysis in IoT environments, to comply with privacy regulations.
- **Threat Intelligence Sharing**: Encourage the sharing of threat intelligence and attack attribution information within the cybersecurity community to enhance collective defense.
- **Adaptive Security**: Develop adaptive security measures that can dynamically adjust and respond to changing attack patterns and tactics in real-time.
- **Blockchain and Trust Mechanisms**: Explore the integration of blockchain technology and trust mechanisms to enhance the security and traceability of IoT-enabled CPS, making it easier to attribute attacks and secure data.

8. BIBLIOGRAPHY

8.BIBLIOGRAPHY

8.1 REFERENCES

[1] Y. Liu, P. Ning, and M. K. Reiter "Cyber-Physical Attacks and Defenses in the Smart Grid: A Review", IEEE Transactions on Industrial Control Systems, 2011.

[2] K. Scarfone, M. Badger, and T. Nichols "Cyber Threat Attribution: A Systematic Review", Computers & Security, 2016.

[3] R. K. Gupta, J. P. Alves-Foss, and K. R. Pattipati "Cyber-Physical Systems Security—A Review", IEEE Access, 2017.

[4] M. H. Bhuyan, D. K. Bhattacharyya, and J. Kalita "A Survey on Intrusion Detection in Cyber-Physical Systems", IEEE Transactions on Industrial Informatics, 2015.

8.2 GITHUB LINK

https://github.com/Sakethpaindla/miniproject