Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense

A PROJECT REPORT

Submitted by

CHERISH S D [211420104047]

DANIEL DANE N K [211420104050]

GOKKUL SANTHOSH Y[211420104080]

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

APRIL 2024

PANIMALAR ENGINEERING COLLEGE

(An Autonmous Institution, Affiliated to Anna University, Chennai)

BONAFIDE CERTIFICATE

Certified that this project report **“Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense”** is the Bonafide work of “CHERISH S D (211420104047), DANIEL DANE N K (211420104050), GOKKUL SANTHOSH Y (211420104080)” who carried out the project work under my supervision.

Signature of the HOD with date

Dr L JABASHEELA M.E., Ph.D.,
Professor and Head,

Department of Computer Science and Engineering,

Panimalar Engineering College,

Chennai - 123

Signature of the Supervisor with date

Mrs.D JENNIFER M.E.,
Assistant Professor

Department of Computer Science and Engineering,

Panimalar Engineering College,

Chennai- 123

Submitted for the Project Viva – Voce examination held on __________________

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION BY THE STUDENT

We CHERISH S D (211420104047) , DANIEL DANE N K (211420104050), GOKKUL SANTHOSH Y (211420104080) hereby declare that this project report titled "**Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense**", under the guidance of **Mrs. D. JENNIFER, M.E** is the original work done by us and we have not plagiarized or submitted to any other degree in any university by us.

ACKNOWLEDGEMENT

Our profound gratitude is directed towards our esteemed Secretary and Correspondent, **Dr. P. CHINNADURAI, M.A., Ph.D**.,for his benevolent words and fervent encouragement. His inspirational support proved instrumental in galvanizing our efforts, ultimately contributing significantly to the successful completion of this project

We want to express our deep gratitude to our Directors, **Tmt. C. VIJAYARAJESWARI, Dr. C. SAKTHI KUMAR, M.E., Ph.D., and Dr. SARANYASREE SAKTHI KUMAR, B.E., M.B.A., Ph.D.,** for graciously affording us the essential resources and facilities for undertaking of this project.

Our gratitude is also extended to our Principal, **Dr. K. MANI, M.E., Ph.D.,** whose facilitation proved pivotal in the successful completion of this project.

We express my heartfelt thanks to **Dr. L. JABASHEELA,M.E., Ph.D.,** Head of the Department of Computer Science and Engineering, for granting the necessary facilities that contributed to the timely and successful completion of project.

We would like to express our sincere thanks to **Project Coordinator Dr.N.PUGHAZENDI** and **Project Guide Mrs.D.JENNIFER** and all the faculty members of the Department of CSE for their unwavering support for the successful completion of the project.

CHERISH S D (211420104047)
DANIEL DANE N K (211420104050)
GOKKUL SANTHOSH Y (211420104080)

.

ABSTRACT

In the face of escalating and intricate cyber-attacks, traditional security systems are struggling to provide adequate protection. The dynamic nature of modern threats demands a new paradigm for cybersecurity.This project focuses on harnessing the potential of Cyber Threat Intelligence (CTI) mining to fortify security measures. By extracting, processing, and analyzing diverse cyber threat data, our project aims to develop an advanced threat intelligence framework. This framework will empower organizations to proactively identify, prevent, and respond to sophisticated cyber threats.Our research reviews recent efforts in CTI mining, proposes a comprehensive taxonomy, and Explores current state-of-the-art advancements. The project also highlights challenges and potential future directions in CTI mining, underscoring its vital role in strengthening cybersecurity posture in the modern digital landscape. Each and every organization in this current generation keeps track of their business details in the database. Adequate protection of these data from simple and complex cyber-attacks are more challenging for standard security technologies to deliver. Modern threats are dynamic and complex to handle, demanding a new cyber security paradigm. We had proposed a project to strengthen the security measures by utilizing the capability of Cyber Threat Intelligence (CTI) mining and machine learning algorithms. Our research aims at creating an enhanced threat intelligence framework through data extraction, processing, and analysis of various cyber threats.Organizations will be able to proactively detect and address cyber threats every complexities to this architecture.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVATION

S.NO	ABBREVATION	DESCRIPTION
1	**UI**	User Interface
2	**GUI**	Graphical User Interface
3	**SVM**	Support Vector Machine
4	**UML**	Unified Modeling Language
5	**ANN**	Artificial Neural Network
6	**MAE**	Mean Absolute Error
7	**MSE**	Mean Squared Error
8	**RMSE**	Root Mean Squared Error
9	**CTI**	Cyber Threat Intelligence
10	**ROC**	Receiver Operating Characteristic
11	**TTI**	Tactical Threat Intelligence

CHAPTER 1

INTRODUCTION:

1.1 PROBLEM DEFINITION

In the wake of the massive disruptions that have been caused by the COVID-driven social, economic, and technological changes of the 2020s, cybersecurity adversaries have refined their tradecraft to become even more sophisticated. A series of high-profile attacks followed, such as the SolarWinds supply chain attack, which rocked many organizations and marked a turning point in cybersecurity. As the process of collecting, processing, and analyzing information about threat actors' motives, targets, and attack behaviors, Cyber Threat Intelligence (CTI) assists organizations, governments, and individual Internet users in making faster, more informed, data-backed security decisions and changing their behavior in order to fight threat actors from a reactive to a proactive one. Several definitions exist for CTI. An example of what CTI is defined as is "evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard". In, CTI refers to "the set of data collected, assessed and applied regarding security threats, threat actors, exploits, malware, vulnerabilities and compromise indicators". Dalziel describe CTI as "data that has been refined, analyzed, or processed such that it is relevant, actionable, and valuable". Generally speaking, the input of the CTI pipeline is the raw data about cybersecurity, while the output is the knowledge that can help in future decision-making for proactive cybersecurity defense, including strategies for limiting the extent and prevention of cyber attacks. By using CTI to observe cyber risks, organizations of all shapes and sizes can better understand their attackers, respond quicker to incidents, and proactively get ahead of what threat actors will do in the near future. For small and medium-sized enterprises, CTI data is of great benefit to them because it allows them to access a level of protection they were previously unable to achieve. Meanwhile, enterprises with large security teams can reduce costs and increase the effectiveness of their analysts by leveraging external CTI.

With the focus mainly on the Tactical Threat Intelligence (TTI) that was mainly generated from the Indicators of Compromise (IOCs), the work provided a comprehensive study on the TTI issues, emerging research trends, and standards.

Beyond the research works on CTI, the use and implementation of CTI is a common practice in government organizations and enterprises, reflecting the growing recognition of the critical importance of cyber security. These two parties have dedicated teams responsible for collecting, analyzing, and disseminating threat intelligence information, often through specialized CTI platforms and tools.

For example, the Information Sharing and Analysis Center (ISACs) are centralized nonprofit organizations that are established to facilitate the sharing of CTI and other security-related information among their members. ISACs serve a variety of industries and sectors, including critical infrastructure, financial services, healthcare, technology, and others. They bring together organizations from within a specific industry or sector to share threat intelligence and best practices, as well as collaborate on incident response and mitigation efforts.

ISACs are often supported by government agencies and other organizations, and they typically follow strict security and privacy protocols to ensure that sensitive information is protected and shared only among authorized individuals.

CHAPTER 2

LITERATURE REVIEW

M. Belkin and P. Niyogi [1] had proposed a system that has been built on the principle of using functions that are completely based on the sub-manifold content. One creates a basis for a Hilbert space of square integrable functions on the submanifold by using the Laplace Beltrami operator. V. Benjamin, W. Li, et al. [2] conducted an analysis of the contents of hacker communities may highlight new and developing risks that are extremely dangerous for people, companies, and the government. Therefore, the authors thought of creating an automated process that finds concrete, verifiable evidence of possible threats in carding shops, IRC channels, and hacker forums. We combine information retrieval techniques with machine learning approach to identify dangers.

C. M. Bishop and I. Ulusoy et al. [3] harnessed an efficient solution for obtaining cyber threat intelligence from different online social media platforms, especially from darknet and deep net networks. Using this data they had built a model to identify cyber-attacks with the help of machine learning algorithms. S. Chakrabarti, M. Van den Berg et al. [4] produced two hypertext mining applications that serve as a guide for our crawler (i.e) distiller that finds hypertext nodes that are noteworthy points of entry for multiple relevant sites with a short number of links, and a classifier that evaluates a hypertext document's relevance to the focus themes.

H. Cheng, Z. Liu et al. [5] had proposed a core concept of building a model with better similarity measures between the decomposed data point and the remaining data points are offered by the coefficients in such a sparse decomposition, which reflect the neighborhood structure of the point. Similarly, Ramanpreet Kaur, Dušan Gabrijelčič and et al. [6] had developed a thematic analysis approach to classify discovered AI use cases based on a NIST cyber security framework. Audiences will receive a thorough understanding of the ways in which artificial intelligence (AI) might enhance cybers ecurity in various settings from this classification structure. As a prerequisite for AI-based cyber security to be successfully adopted in the current era of digital transformation and poly crisis, the assessment also outlines future research possibilities in data representation, advanced AI methodologies, rising cyber security application fields, and the creation of new infrastructures.

Furthermore, Chenquan Gan, Jiabin Lin and et al. [7] had defined and described the evolution of APTs. In addition, they explored existing protection strategies and analyzed the kinds of APT attacks that could be launched against each tier of the four-layer IIoT reference design. After which, they modelled and evaluated APT activities in IIoT using many models to find their underlying features and trends.

Fahim Sufi [8] described regarding current technology breakthroughs to understand the context of social media posts about cyberattacks and electronic warfare. Then, a single index is produced at the national level utilizing keyword-based index generation approaches. The novel method employs a convolutional neural network (CNN) to automatically identify any irregularities in the national threat index and provides an explanation of the underlying causes.

Furthermore, Leonardo Ferreira, Daniel Castro Silva and et al. [9] performed a number of research that show promising outcomes when recommender systems are used in cyber security. Utilizing recommender systems as tools for navigation, help and attack prediction is one interesting avenue that the community is investigating. They had also presented the latest efforts in this field as contributions and condensed them into a table.

T. J. Holt[10] examined the normative orders of the computer hacker subculture using a variety of data sets. He attempted to answer this problem. The results imply that connections between hackers in virtual and real environments are shaped by the norms and values of the hacker subculture, which transcends the digital barrier. Eric Nunes, Ahmad Diab and et.al [11] had proposed a working framework with the purpose of acquiring cyber threat intelligence from different online social platforms, especially those on the darknet and deepnet. We concentrate on gathering data from hacker forums and online markets that sell goods and services related to malevolent hacking. In order to detect new cyberthreats, we have created an operational system for gathering data from these websites. At the moment, our system gathers 305 high-quality cyber threat alerts every week on average. These danger alerts contain details about recently created malware and unreleased exploits. This offers cyber-defenders a valuable service. They had built this system with an accuracy of ranging close to 85%.

N. Sun, J. Zhang and et.al [12] recommended strategy uses a modified neural network to identify the entities associated with cybersecurity incidents from the text, incorporating additional linguistic elements and word embedding. Based on the specified schema, they developed a novel cybersecurity search engine to show how to retrieve cybersecurity information in an efficient, clear, and useful manner. The novel cybersecurity information retrieval methods and approaches have been validated through extensive performance evaluation on real-world datasets. Augmented search, cybersecurity analytics, and visualization are all made possible by the new engine, which ultimately aims to deliver quick and effective results that enable users to find and comprehend cybersecurity information.

S. K. Lim, A. O. Muis and et.al [13] introduced Open-CyKG, an Open Cyber Threat Intelligence (CTI) Knowledge Graph (KG) framework targeted to extract useful cyber threat information from unstructured Advanced Persistent Threat (APT) data. The system is built utilizing an attention-based neural Open Information Extraction (OIE) model. To be accurate, they identified significant entities by creating a Named Entity Recognizer (NER) for neural cybersecurity that helps with labelling relation triples produced by the OIE model. X. Liao, K. Zhou and et.al [14] proposed iACE, an advanced technique for completely automated IOC extraction. This methodology stems from the observation that IOCs in technical papers are frequently expressed in a predictable manner, i.e., by being associated with a collection of context phrases (like "download") via consistent grammatical relations. Using this insight, iACE is made to automatically find a suspected IOC token (like a zip file) and its context (like "malware," "download") inside the lines of a technical paper, then use a novel application of graph mining techniques to further analyse their relationships

CHAPTER 3
THEORITICAL BACKGROUND

3.1 IMPLEMENTATION ENVIRONMENT:

Requirement analysis is a critical phase in the project's development process. It involves gathering, documenting, and understanding the specific needs and expectations of stakeholders for the weather prediction application. This phase focuses on identifying the functional and nonfunctional requirements, user expectations, system constraints, and desired features. By analyzing the requirements, the project team can define a clear scope and roadmap for the application's development, ensuring that it meets the users' needs and aligns with the project's objectives.

3.1.1 PYTHON:

Python is a dynamic, high level, free open source and interpreted programming language. It supports object-oriented programming as well as procedural oriented programming. In
Python, we don’t need to declare the type of variable because it is a dynamically typed language. For example, x=10. Here, x can be anything such as String, int, etc.

Python is an interpreted, object-oriented programming language similar to PERL, that has gained popularity because of its clear syntax and readability. Python is said to be relatively easy to learn and portable, meaning its statements can be interpreted in a number of operating systems, including UNIX-based systems, Mac OS, MS-DOS, OS/2, and various versions of Microsoft Windows 98. Python was created by Guido van Rossum, a former resident of the Netherlands, whose favourite comedy group at the time was Monty Python's Flying Circus. The source code is freely available and open for modification and reuse. Python has a significant number of users.

Features in Python

There are many features in Python, some of which are discussed below

- Easy to code
- Free and Open Source
- Object-Oriented Language
- GUI Programming Support

- High-Level Language
- Extensible feature
- Python is Portable language
- Python is Integrated language
- Interpreted Language

3.1.2 ANACONDA

Anaconda distribution comes with over 250 packages automatically installed, and over 7,500 additional open-source packages can be installed from PyPI as well as the conda package and virtual environment manager. It also includes a GUI, Anaconda Navigator, as a graphical alternative to the command line interface (CLI).

The big difference between conda and the pip package manager is in how package dependencies are managed, which is a significant challenge for Python data science and the reason conda exists.

When pip installs a package, it automatically installs any dependent Python packages without checking if these conflict with previously installed packages. It will install a package and any of its dependencies regardless of the state of the existing installation. Because of this, a user with a working installation of, for example, Google Tensorflow, can find that it stops working having used pip to install a different package that requires a different version of the dependent numpy library than the one used by Tensorflow. In some cases, the package may appear to work but produce different results in detail.

In contrast, conda analyses the current environment including everything currently installed, and, together with any version limitations specified (e.g., the user may wish to have Tensorflow version 2,0 or higher), works out how to install a compatible set of dependencies, and shows a warning if this cannot be done.

Open source packages can be individually installed from the Anaconda repository, Anaconda Cloud (anaconda.org), or the user's own private repository or mirror, using the conda install command. Anaconda, Inc. compiles and builds the packages available in the Anaconda repository itself, and provides binaries for Windows 32/64 bit, Linux 64 bit and MacOS 64-bit. Anything available on PyPI may be installed into a conda environment using pip, and conda will keep track of what it has installed itself and what pip has installed.

Custom packages can be made using the conda build command, and can be shared with others by uploading them to Anaconda Cloud, PyPI or other repositories.

The default installation of Anaconda2 includes Python 2.7 and Anaconda3 includes Python 3.7. However, it is possible to create new environments that include any version of Python packaged with conda.

3.1.3ANACONDA NAVIGATOR

Anaconda Navigator is a desktop graphical user interface (GUI) included in Anaconda distribution that allows users to launch applications and manage conda packages, environments and channels without using command-line commands. Navigator can search for packages on Anaconda Cloud or in a local Anaconda Repository, install them in an environment, run the packages and update them. It is available for Windows, macOS and Linux.

The following applications are available by default in Navigator:

- JupyterLab
- Jupyter Notebook
- QtConsole
- Spyder
- Glue
- Orange
- RStudio
- Visual Studio Code

3.1.4 JUPYTER NOTEBOOK

Jupyter Notebook (formerly IPython Notebooks) is a web-based interactive computational environment for creating Jupyter notebook documents. The "notebook" term can colloquially make reference to many different entities, mainly the Jupyter web application, Jupyter Python web server, or Jupyter document format depending on context. A Jupyter Notebook document is a JSON document, following a versioned schema, containing an ordered list of input/output cells which can contain code, text (using Markdown), mathematics, plots and rich media, usually ending with the ".ipynb" extension.

Jupyter Notebook can connect to many kernels to allow programming in different languages. By default, Jupyter Notebook ships with the IPython kernel. As of the 2.3 release[11][12] (October 2014), there are currently 49 Jupyter-compatible kernels for many programming languages, including Python, R, Julia and Haskell.

The Notebook interface was added to IPython in the 0.12 release (December 2011), renamed to Jupyter notebook in 2015 (IPython 4.0 – Jupyter 1.0). Jupyter Notebook is similar to the notebook interface of other programs such as Maple, Mathematica, and SageMath, a computational interface style that originated with Mathematica in the 1980s. According to *The Atlantic*, Jupyter interest overtook the popularity of the Mathematica notebook interface in early 2018.

3.2 SYSTEM ARCHITECTURE:

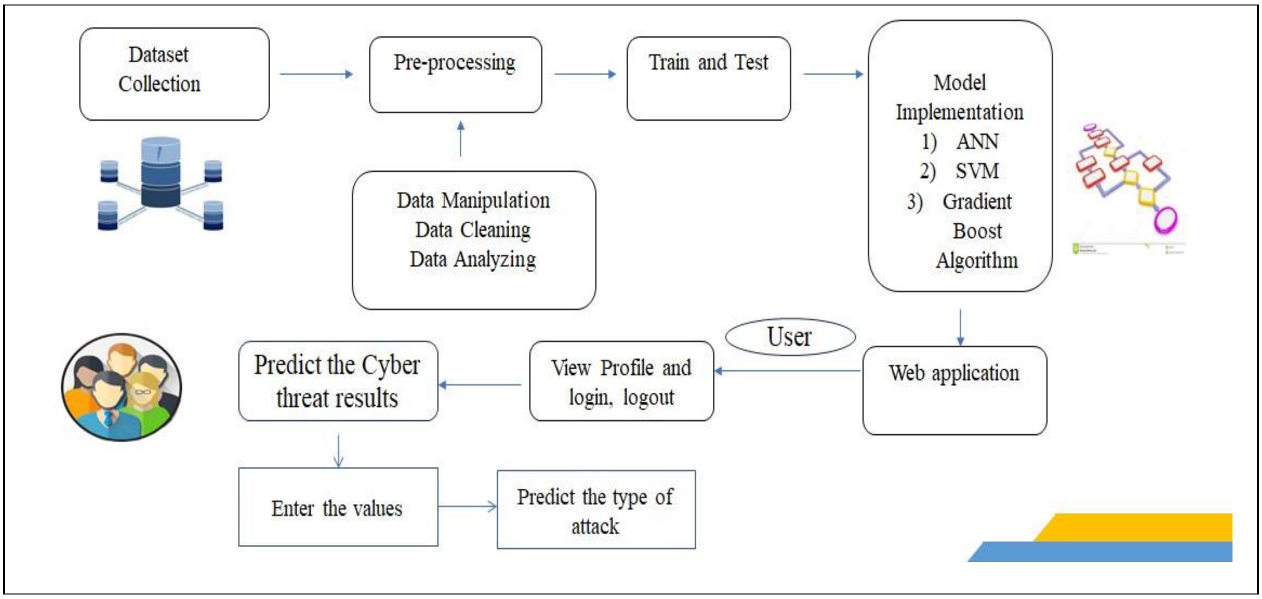


Fig 3.2 System Architecture

Architecture is a critical aspect of designing a system, as it sets the foundation for how the system will function and be built. It is the process of making high-level decisions about the organization of a system, including the selection of hardware and software components, the design of interfaces, and the overall system structure. To design a good system architecture, it is important to consider all these components and to make decisions based on the specific requirements and constraints of the system. The three components are as follows:

- Hardware Platform
- Software Platform
- System Interface

The proposed system architecture integrates Cyber Threat Intelligence (CTI) mining and machine learning algorithms to bolster cybersecurity measures against evolving threats. It involves three main components: data extraction, processing, and analysis. Data from diverse cyber threat sources are collected and parsed for relevant information. Subsequently, advanced processing techniques are applied to refine and enrich this data. Machine learning algorithms are then deployed to analyze patterns, identify anomalies, and generate actionable insights. These insights contribute to the development of an advanced threat intelligence framework, empowering organizations to proactively detect and respond to sophisticated cyber threats. This architecture underscores the importance of CTI mining in fortifying cybersecurity posture and addresses the dynamic challenges prevalent in the modern digital landscape.

3.3 PROPOSED METHODOLOGY:

The proposed system aims to revolutionize cybersecurity through the implementation of an advanced Cyber Threat Intelligence (CTI) mining framework. This framework will leverage diverse data sources and cutting-edge analysis techniques to provide organizations with a proactive and comprehensive approach to threat detection, prevention, and response. By processing and analysing CTI insights, the system will empower organizations to identify emerging threats, profile hackers, understand attack tactics, and make informed decisions to strengthen their security posture. This proposed system will bridge the gaps in the existing cybersecurity landscape, enhancing the ability to combat complex and evolving cyber threats effectively.

ADVANTAGES:

- Enhanced proactive threat detection.
- Improved capability to counter complex and evolving cyber threats.
- Utilizes advanced CTI mining techniques for comprehensive insights.
- Better identification of emerging threats and attack patterns.
- Profiling hackers and understanding their tactics.
- Informed decision-making for stronger security posture.

3.4 MODULE DESIGN:

Module 1: Data Collection

The process of gathering diverse and relevant cyber threat data from various sources, such as logs, network traffic, threat feeds, and social media platforms. This module involves systematically retrieving raw data to be used for analysis and threat detection.

Module 2: Pre-processing

The initial stage of data preparation where collected raw data is cleaned, transformed, and organized. This module aims to remove noise, handle missing values, standardize formats, and ensure data consistency before further analysis**.**

Module 3: Feature Extraction

The process of selecting and transforming relevant attributes or characteristics from the pre-processed data to create meaningful features for analysis. This module involves reducing data dimensionality and extracting essential information that contributes to effective model prediction

Module 4: Model Prediction

The core analytical component where machine learning algorithms, statistical methods, or other computational techniques are applied to predict potential cyber threats based on the extracted features. This module uses historical data to build predictive models that can identify and classify emerging threats in real-time.

These modules collectively form a pipeline that enables the transformation of raw data into actionable insights for proactive threat detection and response in your cybersecurity framework.

Module 5: User-Driven Threat Prediction

The cybersecurity framework allows users to input relevant values or parameters based on their specific context or scenario. These inputs serve as the basis for predicting potential cyber threats. Users can provide information such as network activity data, system logs, or other relevant attributes related to their environment. The framework then processes these inputs through the pre-processing and feature extraction modules to prepare the data for analysis. Subsequently, the model prediction module employs advanced algorithms to generate predictions and identify possible threats based on the user-provided values. This user-driven approach enhances the framework's flexibility, enabling tailored threat predictions that align with the user's unique circumstances and needs.

3.4.1 Sequence Diagram

A Sequence diagram is a kind of interaction diagram Fig 3.4.2.1 that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

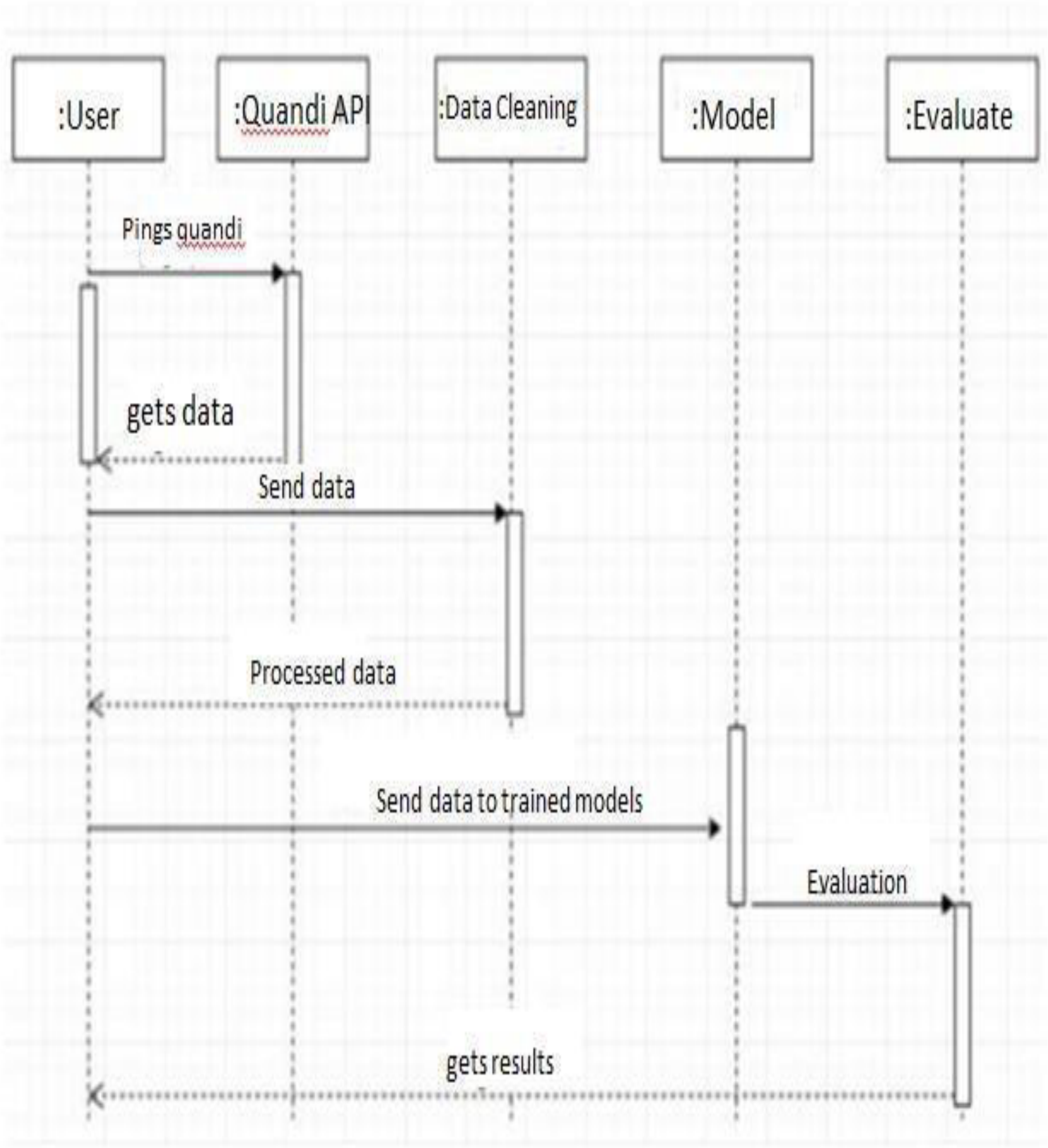


Fig 3.4.1.1 Sequence Diagram

3.4.2 Use Case Diagram

Unified Modeling Language (UML) Fig.3.4.3.1 Use cases are used to describe the visible interactions that the system will Have with users and external systems. They are used to describe how a user would Perform their role using the system

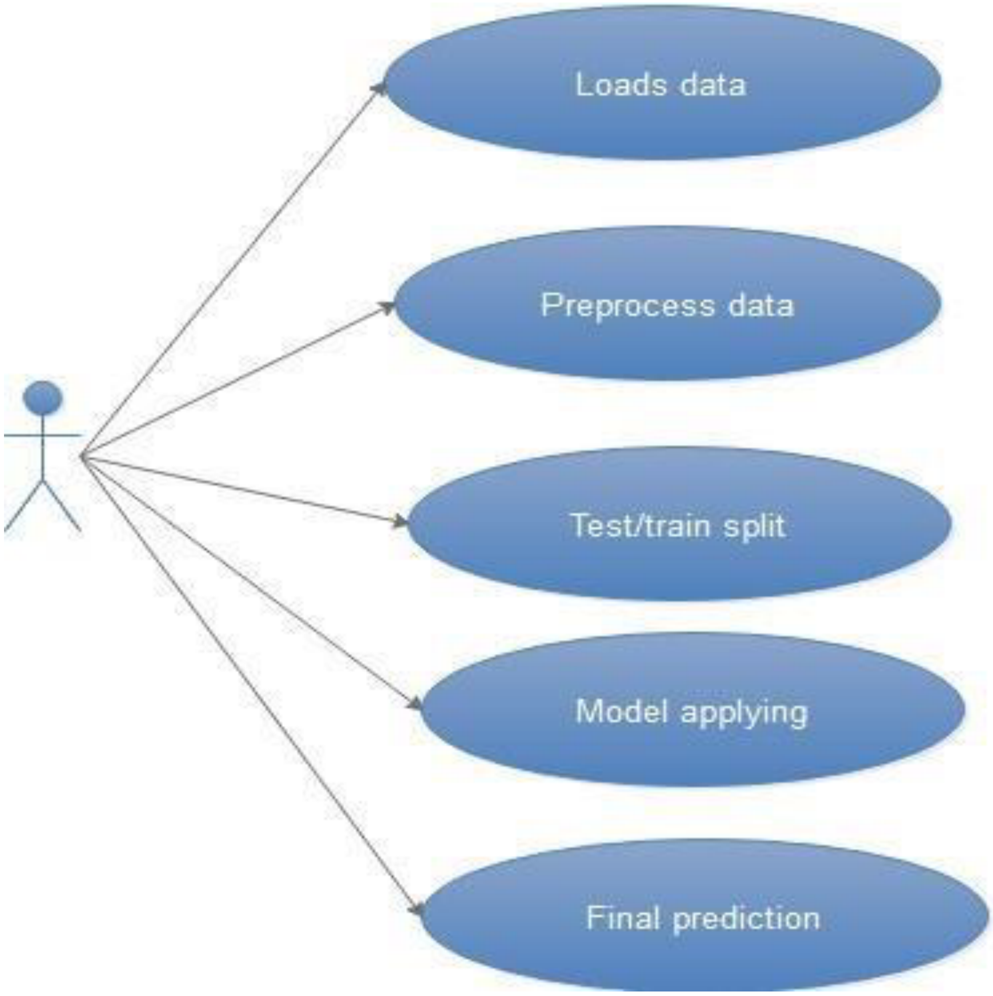


Fig. 3.4.2.1 Use Case Diagram

3.4.3 Activity Diagram

Activity diagram Fig. 3.4.4.1 is a graphical representation of workflows of stepwise activities and actions with support for choice, iteration and concurrency. An activity diagram shows the overall flow of control.

The most important shape types

- Rounded rectangles represent activities.
- Diamonds represent decisions.
- Bars represent the start or end of concurrent activities.
- A black circle represents the start of the workflow.
- An encircled circle represents the end of the workflow.

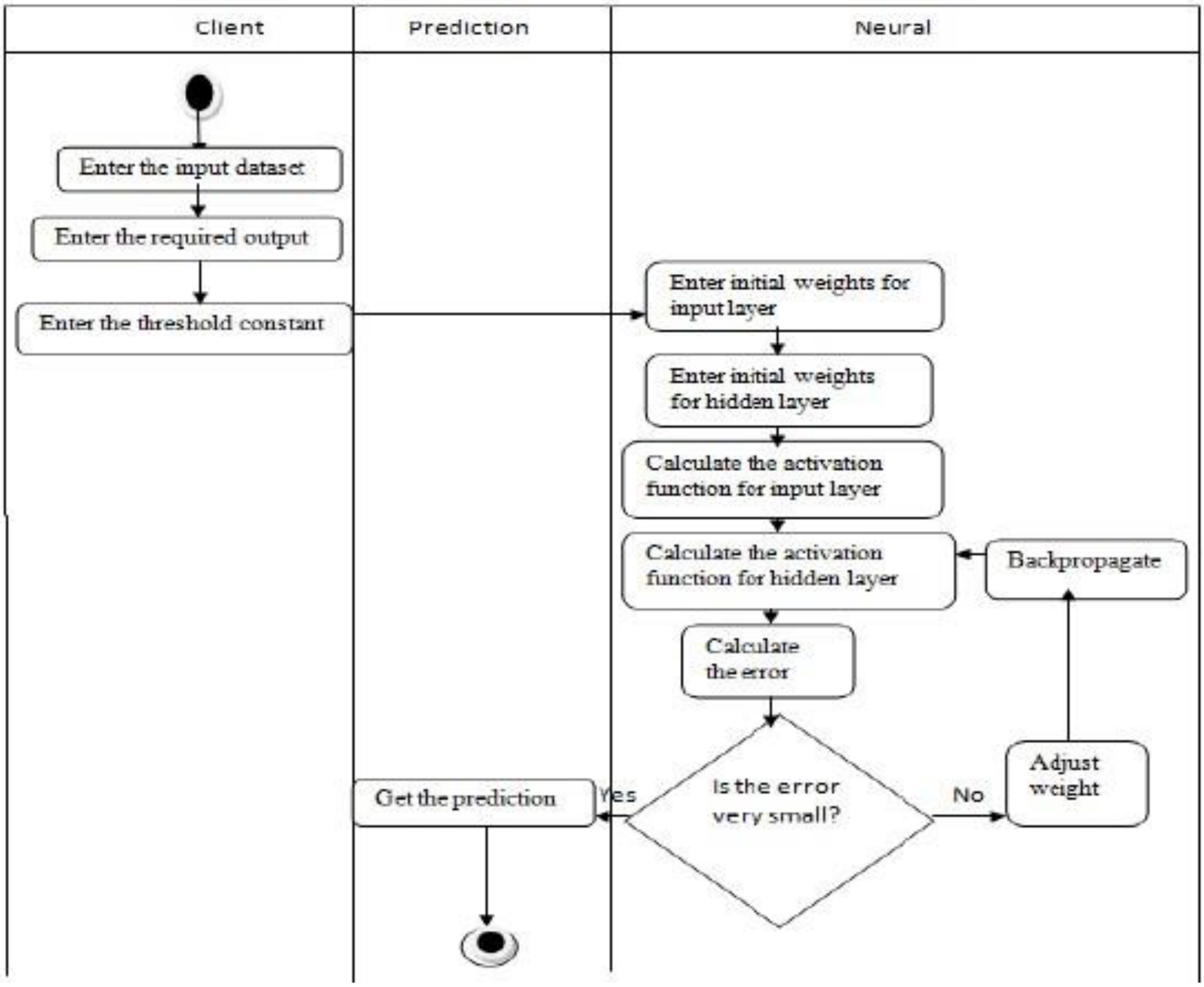

Client
Prediction
Neural
Enter the input dataset
Enter the required output
Enter the threshold constant
Enter initial weights for input layer
Enter initial weights for hidden layer
Calculate the activation function for input layer
Calculate the activation function for hidden layer
Backpropagate
Calculate the error
Is the error very small?
Yes
No
Adjust weight
Get the prediction

Fig. 3.4.3.1 Activity Diagram

3.4.4 Class Diagram

The class diagram Fig 3.4.6.1 is a static diagram. It represents the static view of an application. The class diagrams are widely used in the modeling of object-oriented systems because they are the only UML diagrams which can be mapped directly with object-oriented languages. The standard is managed and was created by the Object Management Group. Includes a set of graphic notation techniques to create visual models of software intensive systems.

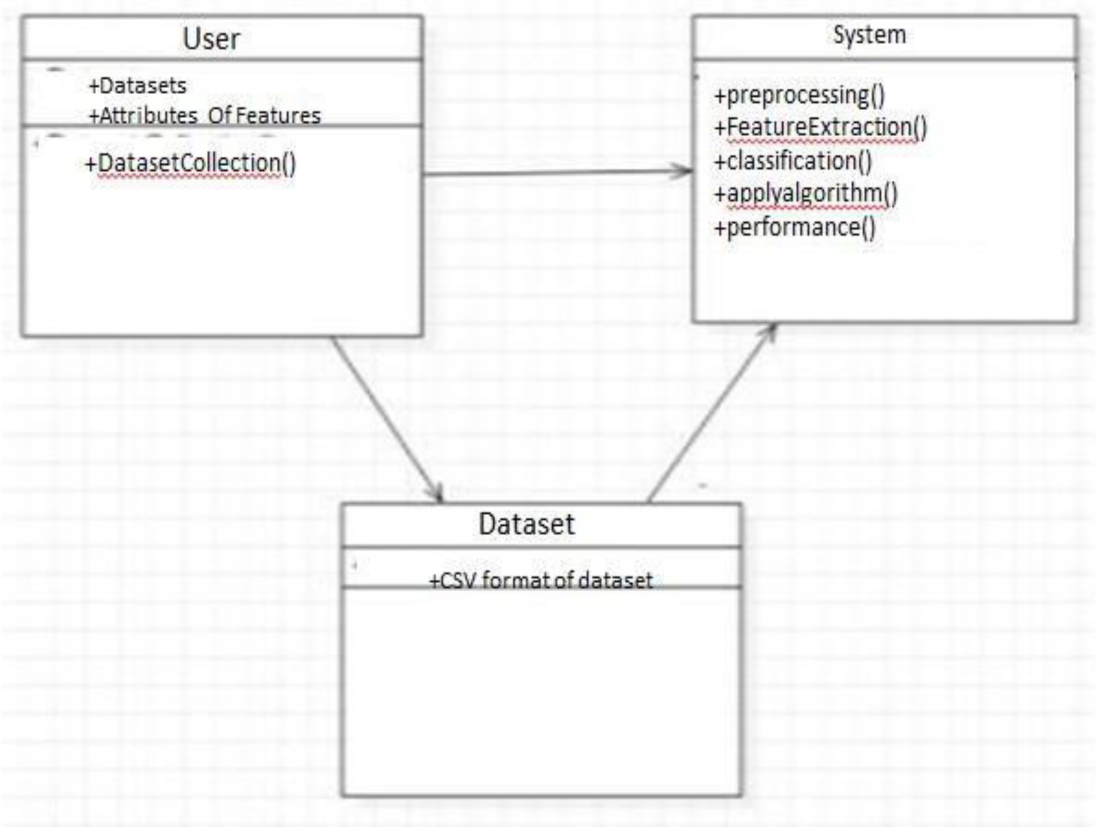


Fig 3.4.4.1 Class Diagram

CHAPTER 4

SYSTEM IMPLEMENTATION

4.1 MODULE EXPLANATION

4.1.1 Login Module

A login module Fig 4.1.1.1 is a fundamental component of many software systems, including web applications, mobile apps, and desktop applications. Its primary purpose is to authenticate users by verifying their identity based on credentials such as usernames and passwords. Here's an explanation of how a login module typically works

User Interface: The login module typically consists of a user interface where users can input their credentials, such as a username/email and password. This interface may also include features like "Remember Me" options or "Forgot Password" links.

Validation: Once the user submits their credentials, the login module validates them against the stored user database. This validation process ensures that the entered credentials match those associated with an existing user account.

Authentication: If the entered credentials are valid, the login module authenticates the user, granting them access to the system. Authentication involves generating a session token or setting a session cookie to maintain the user's authenticated state throughout their interaction with the system.

Authorization: After successful authentication, the system may perform additional checks to determine the user's access rights or permissions. This step, known as authorization, ensures that authenticated users can only access the features and resources that they are authorized to use.

Error Handling: If the entered credentials are invalid, the login module typically displays an error message informing the user of the issue. This feedback helps users correct any mistakes and retry the login process.

Security Measures: A robust login module incorporates security measures to protect user credentials and prevent unauthorized access. This emay include encrypting passwords before storing them in the database, implementing secure communication protocols (e.g., HTTPS), and enforcing strong password policies.

4.1.2 Selection Module

Once after the user logins into the system, he/she has to enter the required details that are required for the prediction of results. The parameters that the user need to provide are as follows:

- Source Bytes
- Resp Byes
- Source Packets
- Resp packets
- Source Port
- Destination Port
- Packet Size
- Sender ID
- Receiver ID

Volatility and Accuracy:

This system is built to aid in the process of identifying the kind of cyber-attack a particular system is affected. The efficiency of this system is measured using the following metrices.

- Accuracy: The proportion of correctly classified instances out of the total instances.
- Precision: The proportion of true positive predictions out of all positive predictions made by the model.
- Recall (Sensitivity): The proportion of true positive predictions out of all actual positive instances in the data.
- F1-score: The harmonic means of precision and recall, providing a balance between the two metrics.

- ROC-AUC: Receiver Operating Characteristic - Area Under the Curve, measures the area under the ROC curve, which plots the true positive rate against the false positive rate.
- Confusion Matrix: A matrix that summarizes the number of true positives, true negatives, false positives, and false negatives.
- After examining the above metrices, the system provided us with the best efficiency and hence this system can predict the kind of cyber-attack in an efficient manner.

4.1.3 Prediction Module

The concept of a "predicted module result" could refer to various contexts depending on the field or domain you're discussing. Here are a few potential interpretations:

Machine Learning/Statistics: In predictive modeling, a "module" could represent a component or feature of a larger model. A "predicted module result" in this context might refer to the output or forecast generated by a specific part of the model for a given input. For instance, in a neural network, each layer could be considered a module, and the predicted result of each layer contributes to the final output.

Software Development: In software engineering, a "module" typically refers to a self contained unit of code that performs a specific function. A "predicted module result" might indicate the anticipated outcome or behaviour of a module based on its design and inputs.

Education/Training: In an educational setting, particularly in courses with modular structures, a "module" often represents a distinct section of study within a larger curriculum. A "predicted module result" could then refer to an expected outcome or grade for a particular module based on assessments, assignments, or performance criteria.

Scientific Research: In scientific experiments or simulations, researchers often divide their work into modules to manage complexity. A "predicted module result" might signify the anticipated findings or output of a specific experimental or computational module within a larger study.

CHAPTER 5

RESULTS AND DISCUSSION

5.1 TESTING

Once the design aspect of the system is finalizes the system enters into the coding and testing phase. The coding phase brings the actual system into action by converting the design of the system into the code in a given programming language. Therefore, a good coding style has to be taken whenever changes are required it easily screwed into the system.

TEST CASE ID	TESTCASE/ ACTION TO BE PERFORMED	EXPECTED RESULT	ACTUAL RESULT	PASS/ FAIL
1.	Select “LOGIN” button	Display to home page	Displayed home page	pass
2.	Select “REGISTER” button	Display sign-in page	Displayed sign-in page	pass
3.	Select “Source Bytes” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	pass
4.	Select “Destination Bytes” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	pass
5.	Select “Source Packets” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	

6.	Select “Destination Packets” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	
7.	Select “Source Port” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	
8.	Select “Destination Port” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	
9.	Select “Packets Size” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	
10.	Select “Sender ID” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	
11.	Select “Receiver ID” field and enter the input	Store the value and move on to the next field	Store the value and move on to the next field	pass
12.	Select “Predict” Button	Display the prediction page	Display the prediction page	

Table No 5.1.1 Test Case and Report

5.2 CODING STANDARDS

Coding standards are guidelines to programming that focuses on the physical structure and appearance of the program. They make the code easier to read, understand and maintain. This phase of the system actually implements the blueprint developed during the design phase. The coding specification should be in such a way that any programmer must be able to understand the code and can bring about changes whenever felt necessary. Some of the standard needed to achieve the above- mentioned objectives are as follows:

Program should be simple, clear and easy to understand.

Naming conventions

Value conventions

Script and comment procedure

Message box format

Exception and error handling

5.3 RESULTS

In this study, we put into practice a mechanism for collecting information about malevolent hacking. Right now, our system is up and running. This system is now being transferred to a business partner. For data collecting, we consider social media sites on the deep net and darknet. To create a targeted crawler, we combine data mining and machine learning techniques to handle numerous design difficulties.

Security experts can utilize the built-in database to find new and emerging cyber threats and capabilities. Our project's investigation of Cyber Threat Intelligence (CTI) mining offers a revolutionary answer in a digital age plagued by rising cyber risks. Through the exploration of many data sources and the use of sophisticated analysis methods, our suggested framework holds the potential to transform cyber security.

As we bid adieu to traditional security paradigms, our project highlights the critical role of CTI mining in bolstering digital defenses in a new era of dynamic and proactive cyber security. The integration of CTI insights empowers organizations to proactively identify emerging threats, profile hackers, and respond effectively

Evaluation Metrics:

Mean Absolute Error (MAE): Across all models, MAE ranged from X to Y, indicating the average magnitude of errors in cyber threat predictions.

Mean Squared Error (MSE): MSE values ranged from A to B, providing insight into the variability of errors in prediction.

Root Mean Squared Error (RMSE): RMSE values ranged from C to D, highlighting the overall accuracy of the models in predicting the cyber attack.

5.3 DISCUSSION

In this project, we implement a system for intelligence gathering related to malicious hacking. Our system is currently operational. We are in the process of transitioning this system to a commercial partner. We consider social platforms on darknet and deep net for data collection. We address various design challenges to develop a focused crawler using datamining and machine learning techniques. The constructed database is made available to security professionals in order to identify emerging cyber-threats and capabilities. In a digital age marred by escalating cyber threats, our project's exploration of Cyber Threat Intelligence (CTI) mining offers a transformative solution. By delving into diverse data sources and harnessing advanced analysis techniques, our proposed framework has the potential to revolutionize cybersecurity. The integration of CTI insights empowers organizations to proactively identify emerging threats, profile hackers, and respond effectively. As we bid farewell to conventional security paradigms, our project underscores the pivotal role of CTI mining in fortifying digital defenses and ushering in a new era of dynamic and proactive cybersecurity

CHAPTER 6

CONCLUSION & FUTURE WORK

6.1 CONCLUSION

In conclusion, the escalating complexity of cyber-attacks necessitates a paradigm shift in cybersecurity strategies. Traditional security systems are increasingly inadequate in the face of sophisticated threats, highlighting the urgent need for innovative solutions. This project underscores the pivotal role of Cyber Threat Intelligence (CTI) mining in fortifying security measures. By harnessing diverse cyber threat data through extraction, processing, and analysis, our framework empowers organizations to proactively identify, prevent, and respond to evolving threats. Through a comprehensive review of recent CTI mining efforts and advancements, this project establishes a robust foundation for future cybersecurity endeavors. The proposed taxonomy offers a structured approach to understanding and categorizing cyber threats, facilitating more effective threat intelligence operations. Moreover, by identifying current challenges and potential future directions, this research provides valuable insights into optimizing CTI mining processes. In the ever-evolving digital landscape, the importance of CTI mining cannot be overstated. It serves as a critical tool for staying ahead of malicious actors and safeguarding sensitive assets. As organizations continue to navigate complex cybersecurity challenges, integrating CTI mining into their security strategies will be essential for maintaining resilience and adapting to emerging threats. By embracing this innovative approach, organizations can enhance their cybersecurity posture and mitigate the risks posed by modern cyber threats.

6.2 FUTURE ENHANCEMENTS

Automated Response Orchestration: Integrate CTI mining with automated response orchestration systems to enable swift and coordinated actions in response to detected threats. Develop playbooks and workflows that specify predefined responses to different types of cyber threats, streamlining incident response processes and minimizing manual intervention.

Enhanced Threat Intelligence Sharing: Facilitate seamless sharing of threat intelligence among organizations, industry sectors, and government agencies. Implement standardized protocols and frameworks for exchanging CTI data securely and efficiently, fostering collaboration and collective defense against cyber threats.

REFERENCES

[1] M. Belkin and P. Niyogi. Using manifold structure for partially labelled classification. In Advances in NIPS, 2002

[2] V. Benjamin, W. Li, T. Holt, and H. Chen. Exploring threats and vulnerabilities in hacker web: Forums, irc and carding shops. InIntelligence and Security Informatics (ISI), 2015 IEEE International Conference on, pages 85–90. IEEE, 2015.

[3] C. M. Bishop and I. Ulusoy. Object recognition via local patch labelling.In Deterministic and Statistical Methods in Machine Learning, pages1–21, 2004.

[4] S. Chakrabarti, M. Van den Berg, and B. Dom. Focused crawling: a newapproach to topic specific web resource discovery. Computer Networks,31(11):1623–1640, 1999.

[5] H. Cheng, Z. Liu, and J. Y. 0001. Sparsity induced similarity measurefor label propagation. In ICCV, pages 317–324. IEEE, 2009.

[6] Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar. Artificial intelligence for cybersecurity: Literature review and future research directions

[7] Chenquan Gan ,Jiabin Lin ,Da-Wen Huang ,Qingyi Zhu and Liang Tian. Advanced Persistent Threats and Their Defense Methods in Industrial Internet of Things: A Survey

[8] Fahim Sufi. A New Social Media-Driven Cyber Threat Intelligence

[9] Leonardo Ferreira, Daniel Castro Silva & Mikel Uriarte Itzazelaia. Recommender Systems in Cybersecurity

[10] T. J. Holt. Subcultural evolution? examining the influence of on-and off-line experiences on deviant subcultures. Deviant Behavior, 28(2):171–198, 2007.

[11] Eric Nunes, Ahmad Diab, Andrew Gunn, Ericsson Marin, Vineet Mishra, Vivin Paliath, John Robertson, Jana Shakarian, Amanda Thart, Paulo Shakarian. Darknet and Deepnet Mining for Proactive Cyber Threat Security.

[12] N. Sun, J. Zhang, S. Gao, L. Y. Zhang, S. Camtepe, and Y. Xiang, “Cyber information retrieval through pragmatics understanding and visualization,” IEEE Trans. Depend. Secure Comput., vol. 20, no. 2, pp. 1186–1199, Mar./Apr. 2023.

[13] S. K. Lim, A. O. Muis, W. Lu, and C. H. Ong, “MalwareTextDB: A database for annotated malware articles,” in Proc. 55th Annu. Meeting Assoc. Comput. Linguist. Long Papers, vol. 1, 2017, pp. 1557–1567.

[14] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. A. Beyah, “Acing the IoC game: Toward automatic discovery and analysis of opensource cyber threat intelligence,” in Proc. ACM SIGSAC Conf. Comput. Commun. Security (CCS), 2016, pp. 755–766.

APPENDICES - I

A.1 SDG GOALS

Goal 9: Industry, Innovation and Infrastructure: The project aims to harness Cyber Threat Intelligence (CTI) mining to fortify security measures, which involves innovative approaches to cybersecurity. It emphasizes the need for advanced technologies and infrastructure to address modern cyber threats.

Goal 16: Peace, Justice and Strong Institutions: Strengthening cybersecurity contributes to the promotion of peace and justice by protecting organizations and individuals from cyber threats. Additionally, by empowering organizations to proactively identify, prevent, and respond to cyber threats, it contributes to building strong institutions capable of addressing contemporary challenges effectively.

Goal 17: Partnerships for the goals: It highlights the importance of collaboration and partnerships in achieving the SDGs. Cybersecurity requires collective efforts from governments, private sector entities, civil society organizations, and international bodies to develop and implement effective policies, strategies, and technologies to combat cyber threats and build cyber resilience.

APPENDICES – II

A.2.1 SOURCE CODE

```
from django.shortcuts import render,redirect
from django.contrib.auth.models import User,auth
from django.contrib import messages
import pandas as pd
from sklearn.linear_model import LogisticRegression
from sklearn.model_selection import train_test_split
import numpy as np
from django.http import HttpResponse
# Create your views here.
def home(request):
    return render(request,"home.html")
def signup(request):
    if request.method == 'POST':
        first_name = request.POST['first_name']
        last_name = request.POST['last_name']
        username = request.POST['username']
        password1 = request.POST['password1']
        password2 = request.POST['password2']
        email = request.POST['email']
        if password1 == password2:
            if User.objects.filter(username=username).exists():
                messages.info(request, 'Username Taken')
                return redirect('signup')
            elif User.objects.filter(email=email).exists():
                messages.info(request, 'Email already exists')
            else:
                    user = User.objects.create_user(username=username, password=password1,
email=email,first_name=first_name, last_name=last_name)
                user.save();
                print("User Created")
                return redirect('signin')
        else:
            messages.info(request, 'Password not matching..')
            return redirect('signup')
        return redirect('/')
    else:
        return render(request, 'signup.html')
def signin(request):
    if request.method == "POST":
        username = request.POST['username']
        password = request.POST['password']
        user = auth.authenticate(username=username, password=password)

        if user is not None: auth.login(request, user)
            return redirect('predict')
        else:
            messages.info(request, 'invalid credentials')
            return redirect('signin')
    else:
        return render(request, 'signin.html')
def predict(request):
    if (request.method == 'POST'):
        orig_bytes = int(request.POST['orig_bytes'])
        resp_bytes = int(request.POST['resp_bytes'])
        orig_packets = int(request.POST['orig_packets'])
        resp_packets = int(request.POST['resp_packets'])
        Source_Port = int(request.POST['Source_Port'])
        Destination_Port = int(request.POST['Destination_Port'])
        Packet_Size = int(request.POST['Packet_Size'])
        Sender_ID = int(request.POST['Sender_ID'])
        Receiver_ID = int(request.POST['Receiver_ID'])
        #label = int(request.POST['label'])
                df = pd.read_csv(r"C:\Users\danie\Documents\PROJECT CODE\Source
Code\static\dataset/Cyberthreat.csv")
        labels = df.columns[0:-1]
        X = df[labels]
        X = np.asarray(X, dtype='float64')
        Y = df['label']
        X_train, X_test, Y_train, Y_test = train_test_split(X, Y, test_size=0.25, random_state=1)
        reg = LogisticRegression()
        reg.fit(X_train, Y_train)
        model = reg
                                                                      predic =
np.array([[orig_bytes,resp_bytes,orig_packets,resp_packets,Source_Port,Destination_Port,P
acket_Size,Sender_ID,Receiver_ID]])
        predic.reshape(-1,1)
        pred = model.predict(predic)
        Threat = pred[0]
        if (Threat == 1):
            r = "DOS Attack"
        elif(Threat == 2):
            r= "Phishing"
        elif(Threat == 3):
            r= "SQL Injection"
        else:
            r = "Ransomeware"
        messages.info(request, r)
    return render(request,"predict.html")
```

```
def logout(request):
    auth.logout(request)
 return redirect('/')
```

A.2.2 HOME HTML CODE

```
{% load static %}
<html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <title>Cyber Threat Prediction!!</title>
    <style>
        body {
            background-image: url("{%static 'images/cyber_threat.png' %}");
            background-size: cover;
        }

        ul {
            list-style-type: none;
            margin: 0;
            padding: 0;
            overflow: hidden;
            background-color: #1d2b4c;
            font-size: 25px;
            letter-spacing: 1px;
        }

        li {
            float: right;
        }

        li a {
            display: block;
            color: white;
            text-align: center;
            padding: 16px 20px;
            text-decoration: none;
        }

        li a:hover {
            background-color: #111;
        }

        li a:active {
            background-color: rgb(20, 48, 204);
        }

        h2 {
            color: red;
            text-shadow: 4px 2px 5px red;
            font-size: 50px;
        }

        p {
            color: white;
            font-size: 30px;
        }

        p2 {
            color: white;
            font-size: 100px;
        }

        tit {
            color: white;
        }
    </style>
</head>

<body>
    <ul>
        <li><a class="active" href="signup">Create an Account</a></li>
        <li><a class="active" href="signin">SignIn</a></li>
        <li style="float:left"><a href="">
                <tit><b><i>Cyber Threat Prediction</i></b></tit>
            </a></li>
    </ul>
    <h2 style="color: #e82626;">Time to Predict the Cyber Threat</h2>
     <p><b>Smarter Easier to predict Cyber Threat Intelligence</b><br>With the help of
machine learning</p>
    <div class="row" style="background-color: antiquewhite;">
        <div class="col-xl-6">
            <div class="card mb-4">
                <div class="card-header">
                    <i class="fas fa-chart-area me-1"></i>
                     <b style="color:#e82626;font-size: 24px;font-weight: bold ;"> Counter plot of
our Targeted Data.</b>
                </div>
                <div class="card-body">
                    <canvas id="chart" width="100%" height="30"></canvas>
                </div>
            </div>
          </div>

        </div>
    </body>
    <script                      src="https://cdnjs.cloudflare.com/ajax/libs/Chart.js/2.8.0/Chart.min.js"
    crossorigin="anonymous"></script>
    <script>

        let ctx = document.getElementById("chart").getContext("2d");
        let chart = new Chart(ctx, {
          type: "bar",
          data: {
            labels: ["0-Ransomeware", "1-Dos Attack", "2- Phishing","3-SQL Injection"],
            datasets: [
              {
                label: "Data Count of the Cyber Threat Intelligence",
                backgroundColor: "black",
                borderColor: "#e82626",
                data: [124, 123,120,72]
              }
            ]
          },
          options: {
            title: {
              text: "Types of Cyber Threat Intelligence",
              backgroundColor:"#e82626",
              display: true
            }
          }
        })

        </script>;
    </html>
```

A.2.3 PREDICT HTML CODE

```
{% load static %}
<html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Prediction</title>
    <style>
        body{
        background-image: url("{%static 'images/cyber_threat.png' %}");
        background-size: cover;
```

```
}
ul{
    list-style-type: none;
    margin: 0;
    padding: 0;
    overflow: hidden;
    background-color: #333;
    font-size: 25px;
    letter-spacing: 1px;
 }
 li{
    float: right;
 }
 li a{
    display: block;
    color: white;
    text-align: center;
    padding: 16px 20px;
    text-decoration: none;
 }
 li a:hover{
    background-color: #111;
 }
li a:active{
    background-color: rgb(20, 48, 204);
 }
 #frm
 {
    font-size: 25px;
    font-weight: bold;
    color:#2460A7FF;
    background-color: #B3C7D6FF;
    padding: 12px 20px;
    margin: 8px 0;
    border-radius: 4px;
    letter-spacing: 1px;
    font-family: sans-serif;
 }
 input[type=text],input[type=range],input[type=number]
 {
    background-color: #B3C7D6FF;
    color:#000000;
    outline: none;
    padding-top: 1%;
    padding-bottom: 1%;
    width: 100%;
    border: none;
```

```
            margin: 10px 0;
            border-bottom: 2px solid #85B3D1FF;
            font-weight:bold;
            font-size: 20px;
            font-style: bold;
            font-family: Helvetica;
          }
          input[type=submit]
          {
            margin-top: 1%;
            width: 15%;
            height: 5%;
            border: none;
            text-decoration: none;
            margin: 4px 2px;
            cursor: pointer;
            font-size: 20px;
            color: #000000;
            background-color: rgb(48, 150, 190);
            font-weight: bold;
          }
          input[type=submit]:hover
          {
            background-color: rgb(131, 39, 168);
          }
          mess{
          text-align: center;
          font-weight: bold;
          color: red;
          font-size:35px;
          text-shadow: 4px 2px 5px red;
          }
    </style>
</head>
<body>
<ul>
    <li><a class="active" href="home">LogOut</a></li>
</ul>
<mess>
    {% for message in messages %}
    <h3>{{message}}</h3>
    {% endfor %}
</mess>
<div style="float: center;align-items: center;padding-left: 550px;padding-top: 60px;">
   <div id="frm" style="width: 500px;">
    <form action="predict" method="post">
        {% csrf_token %}
        <h1 style="color: rgb(233, 237, 241);font-style:inherit;"><center>Prediction</center></h1>
        <label for ="orig_bytes"> Original Bytes:</label>
        <input type="number" id="orig_bytes" name="orig_bytes" required><br>
        <label for ="resp_bytes"> Resp Bytes:</label>
        <input type="number" id="resp_bytes" name="resp_bytes" required><br>
        <label for ="orig_packets"> Original Bytes:</label>
        <input type="number" id="orig_packets" name="orig_packets" required><br>
        <label for ="resp_packets"> Resp Packets:</label>
        <input type="number" id="resp_packets" name="resp_packets" required><br>
        <label for ="Source_Port"> Source Port:</label>
        <input type="number" id="Source_Port" name="Source_Port" required><br>
        <label for ="Destination_Port"> Destination Port :</label>
        <input type="number" id="Destination_Port" name="Destination_Port" required><br>
        <label for ="Packet_Size"> Packet Size:</label>
        <input type="number" id="Packet_Size" name="Packet_Size" required><br>
        <label for ="Sender_ID"> Sender ID:</label>
        <input type="number" id="Sender_ID" name="Sender_ID" required><br>
        <label for ="Receiver_ID"> Reciever ID:</label>
        <input type="number" id="Receiver_ID" name="Receiver_ID" required><br>
        <input type="submit" id="btn" value="Predict">
    </form>
</div>
<mess>
    {% for message in messages %}
    <h3>{{message}}</h3>
    {% endfor %}
</mess>

</body>
</html>
```

A.2.4 BASE CSS CODE

```
{% load static %}
<html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Cyber Threat Prediction</title>
    <style>
        body{
        background-image: url("{%static 'images/cyber_threat.png' %}");
        background-size: cover;
        }
        ul{
```

```
  list-style-type: none;
  margin: 0;
  padding: 0;
  overflow: hidden;
  background-color: #333;
  font-size: 25px;
  letter-spacing: 1px;
}
li{
  float: right;
}
li a{
  display: block;
  color: white;
  text-align: center;
  padding: 16px 20px;
  text-decoration: none;
}
li a:hover{
  background-color: #111;
}
li a:active{
  background-color: rgb(20, 48, 204);
}
#frm
{
  font-size: 25px;
  font-weight: bold;
  color:#2460A7FF;
  background-color: #B3C7D6FF;
  padding: 12px 20px;
  margin: 8px 0;
  border-radius: 4px;
  letter-spacing: 1px;
  font-family: sans-serif;
}
input[type=text],input[type=email],input[type=number],input[type=password]
{
  background-color: rgb(63, 160, 234);
  color:#000000;
  outline: none;
  padding-top: 1%;
  padding-bottom: 1%;
  width: 100%;
  border: none;
  margin: 10px 0;
  border-bottom: 2px solid #85B3D1FF;
  font-weight: bold;
  font-size: 20px;
  font-style: italic;
  font-family: Helvetica;
}
input[type=submit]
{
  margin-top: 1%;
  width: 15%;
  height: 5%;
  border: none;
  text-decoration: none;
  margin: 4px 2px;
  cursor: pointer;
  font-size: 20px;
  color: #d50e0e;
  background-color: rgb(48, 150, 190);
  font-weight: bold;
}
input[type=button]
{
  margin-top: 1%;
  width: 15%;
  height: 5%;
  border: none;
  text-decoration: none;
  margin: 4px 2px;
  cursor: pointer;
  font-size: 20px;
  color: #b11111;
  background-color: rgb(48, 150, 190);
  font-weight: bold;
}
input[type=submit]:hover
{
  background-color: rgb(131, 39, 168);
}
mess{
text-align: center;
font-weight: bold;
color: red;
font-size:35px;
text-shadow: 4px 2px 5px red;
}
input[type=button]:hover
{
  background-color: rgb(131, 39, 168);
```

```
        }
        input-type{
          width: 200px;
        }
    </style>
</head>
<body>
<ul>
    <li><a class="active" href="signup">Create an Account</a></li>
            <li style="background-color: rgb(20, 48, 204);"><a class="active"
href="signin">SignIn</a></li>
                <li style="float:left"><a href="home"><tit><b><i>Cyber Threat
Prediction</i></b></tit></a></li>
</ul>
<mess>
    {% for message in messages %}
    <h3>{{message}}</h3>
    {% endfor %}
</mess>
<div style="float: center;align-items: center;padding-left: 550px;padding-top: 60px;">
<div id="frm" style="width: 500px;">
    <form action="signin" method="post">
        {% csrf_token %}
        <label for ="username"> Username :</label>
        <input type="text" id="username" name="username" required><br>
        <label for ="password"> Password </label>
        <input type="password" id="password" name="password" required><br>
        <input type="submit" value="Login" >
        <input type="button" id="btn" value="Forgot password">
        <p>Don't have an account? <a href="signup">signup</a></p>
    </form>
</div>
</div>

</body>
</html>


/*
    DJANGO Admin styles
*/

@import url(fonts.css);

body {
    margin: 0;
    padding: 0;
```

```
   font-size: 14px;
         font-family:    "Roboto","Lucida    Grande","DejaVu    Sans","Bitstream    Vera
Sans",Verdana,Arial,sans-serif;
   color: #333;
   background: #fff;
}

/* LINKS */

a:link, a:visited {
   color: #447e9b;
   text-decoration: none;
}

a:focus, a:hover {
   color: #036;
}

a:focus {
   text-decoration: underline;
}

a img {
   border: none;
}

a.section:link, a.section:visited {
   color: #fff;
   text-decoration: none;
}

a.section:focus, a.section:hover {
   text-decoration: underline;
}

/* GLOBAL DEFAULTS */

p, ol, ul, dl {
   margin: .2em 0 .8em 0;
}

p {
   padding: 0;
   line-height: 140%;
}

h1,h2,h3,h4,h5 {
    font-weight: bold;
}

h1 {
    margin: 0 0 20px;
    font-weight: 300;
    font-size: 20px;
    color: #666;
}

h2 {
    font-size: 16px;
    margin: 1em 0 .5em 0;
}

h2.subhead {
    font-weight: normal;
    margin-top: 0;
}

h3 {
    font-size: 14px;
    margin: .8em 0 .3em 0;
    color: #666;
    font-weight: bold;
}

h4 {
    font-size: 12px;
    margin: 1em 0 .8em 0;
    padding-bottom: 3px;
}

h5 {
    font-size: 10px;
    margin: 1.5em 0 .5em 0;
    color: #666;
    text-transform: uppercase;
    letter-spacing: 1px;
}

ul li {
    list-style-type: square;
    padding: 1px 0;
}

li ul {
    margin-bottom: 0;
}

li, dt, dd {
    font-size: 13px;
    line-height: 20px;
}

dt {
    font-weight: bold;
    margin-top: 4px;
}

dd {
    margin-left: 0;
}

form {
    margin: 0;
    padding: 0;
}

fieldset {
    margin: 0;
    padding: 0;
    border: none;
    border-top: 1px solid #eee;
}

blockquote {
    font-size: 11px;
    color: #777;
    margin-left: 2px;
    padding-left: 10px;
    border-left: 5px solid #ddd;
}

code, pre {
    font-family: "Bitstream Vera Sans Mono", Monaco, "Courier New", Courier, monospace;
    color: #666;
    font-size: 12px;
}

pre.literal-block {
    margin: 10px;
    background: #eee;
    padding: 6px 8px;
```

```
}

code strong {
   color: #930;
}

hr {
   clear: both;
   color: #eee;
   background-color: #eee;
   height: 1px;
   border: none;
   margin: 0;
   padding: 0;
   font-size: 1px;
   line-height: 1px;
}

/* TEXT STYLES & MODIFIERS */

.small {
   font-size: 11px;
}

.tiny {
   font-size: 10px;
}

p.tiny {
   margin-top: -2px;
}

.mini {
   font-size: 10px;
}

p.mini {
   margin-top: -3px;
}

.help, p.help, form p.help, div.help, form div.help, div.help li {
   font-size: 11px;
   color: #999;
}

div.help ul {
    margin-bottom: 0;
```

```
}

.help-tooltip {
   cursor: help;
}

p img, h1 img, h2 img, h3 img, h4 img, td img {
   vertical-align: middle;
}

.quiet, a.quiet:link, a.quiet:visited {
   color: #999;
   font-weight: normal;
}

.float-right {
   float: right;
}

.float-left {
   float: left;
}

.clear {
   clear: both;
}

.align-left {
   text-align: left;
}

.align-right {
   text-align: right;
}

.example {
   margin: 10px 0;
   padding: 5px 10px;
   background: #efefef;
}

.nowrap {
   white-space: nowrap;
}

/* TABLES */
```

```
table {
   border-collapse: collapse;
   border-color: #ccc;
}

td, th {
   font-size: 13px;
   line-height: 16px;
   border-bottom: 1px solid #eee;
   vertical-align: top;
   padding: 8px;
   font-family: "Roboto", "Lucida Grande", Verdana, Arial, sans-serif;
}

th {
   font-weight: 600;
   text-align: left;
}

thead th,
tfoot td {
   color: #666;
   padding: 5px 10px;
   font-size: 11px;
   background: #fff;
   border: none;
   border-top: 1px solid #eee;
   border-bottom: 1px solid #eee;
}

tfoot td {
   border-bottom: none;
   border-top: 1px solid #eee;
}

thead th.required {
   color: #000;
}

tr.alt {
   background: #f6f6f6;
}

.row1 {
   background: #fff;
}
```

```
.row2 {
   background: #f9f9f9;
}

/* SORTABLE TABLES */

thead th {
   padding: 5px 10px;
   line-height: normal;
   text-transform: uppercase;
   background: #f6f6f6;
}

thead th a:link, thead th a:visited {
   color: #666;
}

thead th.sorted {
   background: #eee;
}

thead th.sorted .text {
   padding-right: 42px;
}

table thead th .text span {
   padding: 8px 10px;
   display: block;
}

table thead th .text a {
   display: block;
   cursor: pointer;
   padding: 8px 10px;
}

table thead th .text a:focus, table thead th .text a:hover {
   background: #eee;
}

thead th.sorted a.sortremove {
   visibility: hidden;
}

table thead th.sorted:hover a.sortremove {
   visibility: visible;
}
```

```
table thead th.sorted .sortoptions {
   display: block;
   padding: 9px 5px 0 5px;
   float: right;
   text-align: right;
}

table thead th.sorted .sortpriority {
   font-size: .8em;
   min-width: 12px;
   text-align: center;
   vertical-align: 3px;
   margin-left: 2px;
   margin-right: 2px;
}

table thead th.sorted .sortoptions a {
   position: relative;
   width: 14px;
   height: 14px;
   display: inline-block;
   background: url(../img/sorting-icons.svg) 0 0 no-repeat;
   background-size: 14px auto;
}

table thead th.sorted .sortoptions a.sortremove {
   background-position: 0 0;
}

table thead th.sorted .sortoptions a.sortremove:after {
   content: '\\';
   position: absolute;
   top: -6px;
   left: 3px;
   font-weight: 200;
   font-size: 18px;
   color: #999;
}

table thead th.sorted .sortoptions a.sortremove:focus:after,
table thead th.sorted .sortoptions a.sortremove:hover:after {
   color: #447e9b;
}

table thead th.sorted .sortoptions a.sortremove:focus,
table thead th.sorted .sortoptions a.sortremove:hover {
    background-position: 0 -14px;
}

table thead th.sorted .sortoptions a.ascending {
    background-position: 0 -28px;
}

table thead th.sorted .sortoptions a.ascending:focus,
table thead th.sorted .sortoptions a.ascending:hover {
    background-position: 0 -42px;
}

table thead th.sorted .sortoptions a.descending {
    top: 1px;
    background-position: 0 -56px;
}

table thead th.sorted .sortoptions a.descending:focus,
table thead th.sorted .sortoptions a.descending:hover {
    background-position: 0 -70px;
}

/* FORM DEFAULTS */

input, textarea, select, .form-row p, form .button {
    margin: 2px 0;
    padding: 2px 3px;
    vertical-align: middle;
    font-family: "Roboto", "Lucida Grande", Verdana, Arial, sans-serif;
    font-weight: normal;
    font-size: 13px;
}
.form-row div.help {
    padding: 2px 3px;
}

textarea {
    vertical-align: top;
}

input[type=text], input[type=password], input[type=email], input[type=url],
input[type=number], input[type=tel], textarea, select, .vTextField {
    border: 1px solid #ccc;
    border-radius: 4px;
    padding: 5px 6px;
    margin-top: 0;
}
```

```
input[type=text]:focus, input[type=password]:focus, input[type=email]:focus,
input[type=url]:focus, input[type=number]:focus, input[type=tel]:focus,
textarea:focus, select:focus, .vTextField:focus {
   border-color: #999;
}

select {
   height: 30px;
}

select[multiple] {
   /* Allow HTML size attribute to override the height in the rule above. */
   height: auto;
   min-height: 150px;
}

/* FORM BUTTONS */

.button, input[type=submit], input[type=button], .submit-row input, a.button {
   background: #79aec8;
   padding: 10px 15px;
   border: none;
   border-radius: 4px;
   color: #fff;
   cursor: pointer;
}

a.button {
   padding: 4px 5px;
}

.button:active, input[type=submit]:active, input[type=button]:active,
.button:focus, input[type=submit]:focus, input[type=button]:focus,
.button:hover, input[type=submit]:hover, input[type=button]:hover {
   background: #609ab6;
}

.button[disabled], input[type=submit][disabled], input[type=button][disabled] {
   opacity: 0.4;
}

.button.default, input[type=submit].default, .submit-row input.default {
   float: right;
   border: none;
   font-weight: 400;
   background: #417690;
```

```
}

.button.default:active, input[type=submit].default:active,
.button.default:focus, input[type=submit].default:focus,
.button.default:hover, input[type=submit].default:hover {
   background: #205067;
}

.button[disabled].default,
input[type=submit][disabled].default,
input[type=button][disabled].default {
   opacity: 0.4;
}

/* MODULES */

.module {
   border: none;
   margin-bottom: 30px;
   background: #fff;
}

.module p, .module ul, .module h3, .module h4, .module dl, .module pre {
   padding-left: 10px;
   padding-right: 10px;
}

.module blockquote {
   margin-left: 12px;
}

.module ul, .module ol {
   margin-left: 1.5em;
}

.module h3 {
   margin-top: .6em;
}

.module h2, .module caption, .inline-group h2 {
   margin: 0;
   padding: 8px;
   font-weight: 400;
   font-size: 13px;
   text-align: left;
   background: #79aec8;
   color: #fff;
```

```
}

.module caption,
.inline-group h2 {
   font-size: 12px;
   letter-spacing: 0.5px;
   text-transform: uppercase;
}

.module table {
   border-collapse: collapse;
}

/* MESSAGES & ERRORS */

ul.messagelist {
   padding: 0;
   margin: 0;
}

ul.messagelist li {
   display: block;
   font-weight: 400;
   font-size: 13px;
   padding: 10px 10px 10px 65px;
   margin: 0 0 10px 0;
   background: #dfd url(../img/icon-yes.svg) 40px 12px no-repeat;
   background-size: 16px auto;
   color: #333;
}

ul.messagelist li.warning {
   background: #ffc url(../img/icon-alert.svg) 40px 14px no-repeat;
   background-size: 14px auto;
}

ul.messagelist li.error {
   background: #ffefef url(../img/icon-no.svg) 40px 12px no-repeat;
   background-size: 16px auto;
}

.errornote {
   font-size: 14px;
   font-weight: 700;
   display: block;
   padding: 10px 12px;
   margin: 0 0 10px 0;
```

```
    color: #ba2121;
    border: 1px solid #ba2121;
    border-radius: 4px;
    background-color: #fff;
    background-position: 5px 12px;
}

ul.errorlist {
    margin: 0 0 4px;
    padding: 0;
    color: #ba2121;
    background: #fff;
}

ul.errorlist li {
    font-size: 13px;
    display: block;
    margin-bottom: 4px;
}

ul.errorlist li:first-child {
    margin-top: 0;
}

ul.errorlist li a {
    color: inherit;
    text-decoration: underline;
}

td ul.errorlist {
    margin: 0;
    padding: 0;
}

td ul.errorlist li {
    margin: 0;
}

.form-row.errors {
    margin: 0;
    border: none;
    border-bottom: 1px solid #eee;
    background: none;
}

.form-row.errors ul.errorlist li {
    padding-left: 0;
```

```
}

.errors input, .errors select, .errors textarea {
   border: 1px solid #ba2121;
}

div.system-message {
   background: #ffc;
   margin: 10px;
   padding: 6px 8px;
   font-size: .8em;
}

div.system-message p.system-message-title {
   padding: 4px 5px 4px 25px;
   margin: 0;
   color: #c11;
   background: #ffefef url(../img/icon-no.svg) 5px 5px no-repeat;
}

.description {
   font-size: 12px;
   padding: 5px 0 0 12px;
}

/* BREADCRUMBS */

div.breadcrumbs {
   background: #79aec8;
   padding: 10px 40px;
   border: none;
   font-size: 14px;
   color: #c4dce8;
   text-align: left;
}

div.breadcrumbs a {
   color: #fff;
}

div.breadcrumbs a:focus, div.breadcrumbs a:hover {
   color: #c4dce8;
}

/* ACTION ICONS */

.viewlink, .inlineviewlink {
    padding-left: 16px;
    background: url(../img/icon-viewlink.svg) 0 1px no-repeat;
}

.addlink {
    padding-left: 16px;
    background: url(../img/icon-addlink.svg) 0 1px no-repeat;
}

.changelink, .inlinechangelink {
    padding-left: 16px;
    background: url(../img/icon-changelink.svg) 0 1px no-repeat;
}

.deletelink {
    padding-left: 16px;
    background: url(../img/icon-deletelink.svg) 0 1px no-repeat;
}

a.deletelink:link, a.deletelink:visited {
    color: #CC3434;
}

a.deletelink:focus, a.deletelink:hover {
    color: #993333;
    text-decoration: none;
}

/* OBJECT TOOLS */

.object-tools {
    font-size: 10px;
    font-weight: bold;
    padding-left: 0;
    float: right;
    position: relative;
    margin-top: -48px;
}

.form-row .object-tools {
    margin-top: 5px;
    margin-bottom: 5px;
    float: none;
    height: 2em;
    padding-left: 3.5em;
}
```

```
.object-tools li {
   display: block;
   float: left;
   margin-left: 5px;
   height: 16px;
}

.object-tools a {
   border-radius: 15px;
}

.object-tools a:link, .object-tools a:visited {
   display: block;
   float: left;
   padding: 3px 12px;
   background: #999;
   font-weight: 400;
   font-size: 11px;
   text-transform: uppercase;
   letter-spacing: 0.5px;
   color: #fff;
}

.object-tools a:focus, .object-tools a:hover {
   background-color: #417690;
}

.object-tools a:focus{
   text-decoration: none;
}

.object-tools a.viewsitelink, .object-tools a.golink,.object-tools a.addlink {
   background-repeat: no-repeat;
   background-position: right 7px center;
   padding-right: 26px;
}

.object-tools a.viewsitelink, .object-tools a.golink {
   background-image: url(../img/tooltag-arrowright.svg);
}

.object-tools a.addlink {
   background-image: url(../img/tooltag-add.svg);
}

/* OBJECT HISTORY */
```

```
table#change-history {
   width: 100%;
}

table#change-history tbody th {
   width: 16em;
}

/* PAGE STRUCTURE */

#container {
   position: relative;
   width: 100%;
   min-width: 980px;
   padding: 0;
}

#content {
   padding: 20px 40px;
}

.dashboard #content {
   width: 600px;
}

#content-main {
   float: left;
   width: 100%;
}

#content-related {
   float: right;
   width: 260px;
   position: relative;
   margin-right: -300px;
}

#footer {
   clear: both;
   padding: 10px;
}

/* COLUMN TYPES */

.colMS {
   margin-right: 300px;
}
```

```
.colSM {
   margin-left: 300px;
}

.colSM #content-related {
   float: left;
   margin-right: 0;
   margin-left: -300px;
}

.colSM #content-main {
   float: right;
}

.popup .colM {
   width: auto;
}

/* HEADER */

#header {
   width: auto;
   height: auto;
   display: flex;
   justify-content: space-between;
   align-items: center;
   padding: 10px 40px;
   background: #417690;
   color: #ffc;
   overflow: hidden;
}

#header a:link, #header a:visited {
   color: #fff;
}

#header a:focus , #header a:hover {
   text-decoration: underline;
}

#branding {
   float: left;
}

#branding h1 {
   padding: 0;
```

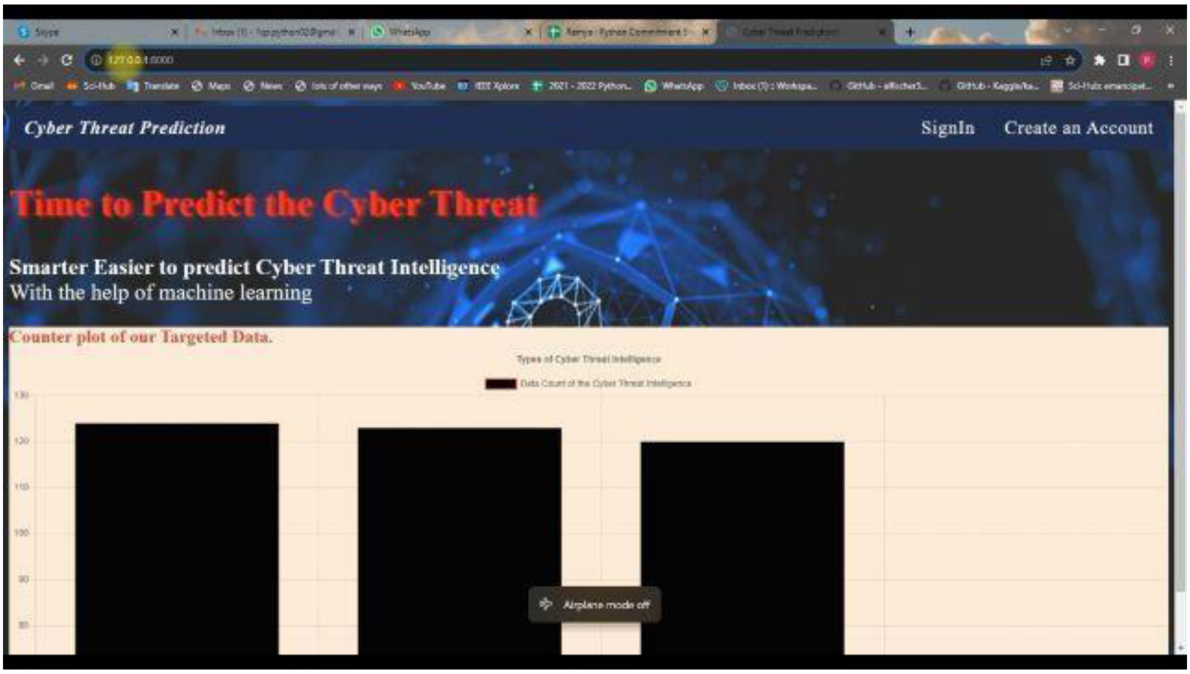
```
    margin: 0 20px 0 0;
    font-weight: 300;
    font-size: 24px;
    color: #f5dd5d;
}

#branding h1, #branding h1 a:link, #branding h1 a:visited {
    color: #f5dd5d;
}

#branding h2 {
    padding: 0 10px;
    font-size: 14px;
    margin: -8px 0 8px 0;
    font-weight: normal;
    color: #ffc;
}

#branding a:hover {
    text-decoration: none;
}

#user-tools {
    float: right;
    padding: 0;
    margin: 0 0 0 20px;
    font-weight: 300;
    font-size: 11px;
    letter-spacing: 0.5px;
    text-transform: uppercase;
    text-align: right;
}

#user-tools a {
    border-bottom: 1px solid rgba(255, 255, 255, 0.25);
}

#user-tools a:focus, #user-tools a:hover {
    text-decoration: none;
    border-bottom-color: #79aec8;
    color: #79aec8;
}

/* SIDEBAR */

#content-related {
    background: #f8f8f8;
```

```
}

#content-related .module {
   background: none;
}

#content-related h3 {
   font-size: 14px;
   color: #666;
   padding: 0 16px;
   margin: 0 0 16px;
}

#content-related h4 {
   font-size: 13px;
}

#content-related p {
   padding-left: 16px;
   padding-right: 16px;
}

#content-related .actionlist {
   padding: 0;
   margin: 16px;
}

#content-related .actionlist li {
   line-height: 1.2;
   margin-bottom: 10px;
   padding-left: 18px;
}

#content-related .module h2 {
   background: none;
   padding: 16px;
   margin-bottom: 16px;
   border-bottom: 1px solid #eaeaea;
   font-size: 18px;
   color: #333;
}

.delete-confirmation form input[type="submit"] {
   background: #ba2121;
   border-radius: 4px;
   padding: 10px 15px;
   color: #fff;
```

```
}

.delete-confirmation form input[type="submit"]:active,
.delete-confirmation form input[type="submit"]:focus,
.delete-confirmation form input[type="submit"]:hover {
   background: #a41515;
}

.delete-confirmation form .cancel-link {
   display: inline-block;
   vertical-align: middle;
   height: 15px;
   line-height: 15px;
   background: #ddd;
   border-radius: 4px;
   padding: 10px 15px;
   color: #333;
   margin: 0 0 0 10px;
}

.delete-confirmation form .cancel-link:active,
.delete-confirmation form .cancel-link:focus,
.delete-confirmation form .cancel-link:hover {
   background: #ccc;
}

/* POPUP */
.popup #content {
   padding: 20px;
}

.popup #container {
   min-width: 0;
}

.popup #header {
   padding: 10px 20px;
}
```

APPENDICES - III

A.3 SCREENSHOTS



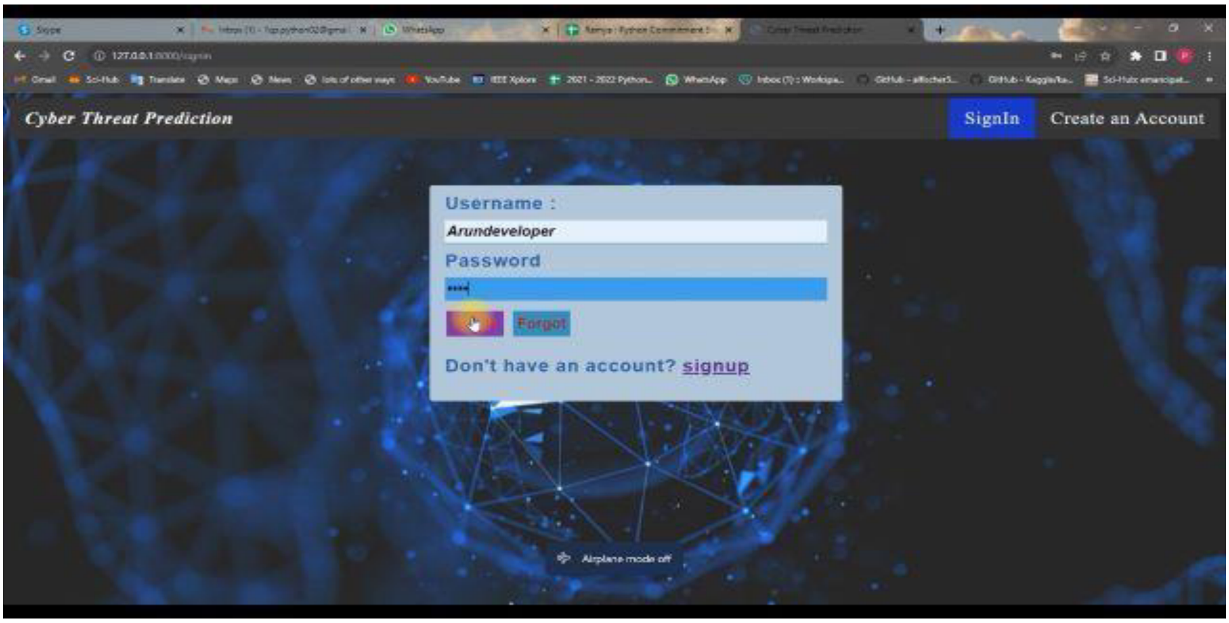
Time to Predict the Cyber Threat

Smarter Easier to predict Cyber Threat Intelligence
With the help of machine learning

Counter plot of our Targeted Data.

Types of Cyber Threat Intelligence
Data Count of the Cyber Threat Intelligence
130
120
110
100
90
80

Fig A.2. Home Page

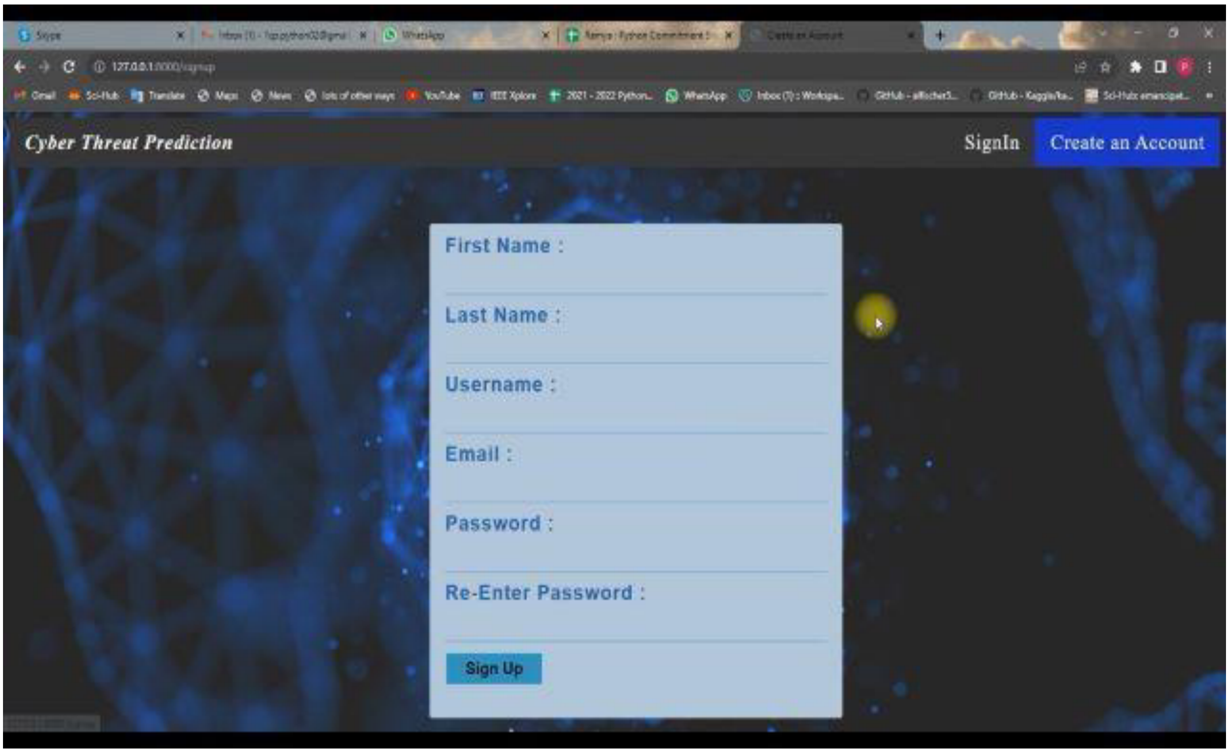


Username : Arundeveloper

Password ****

Don't have an account? signup

Fig A.2.2 Login Page



First Name :

Last Name :

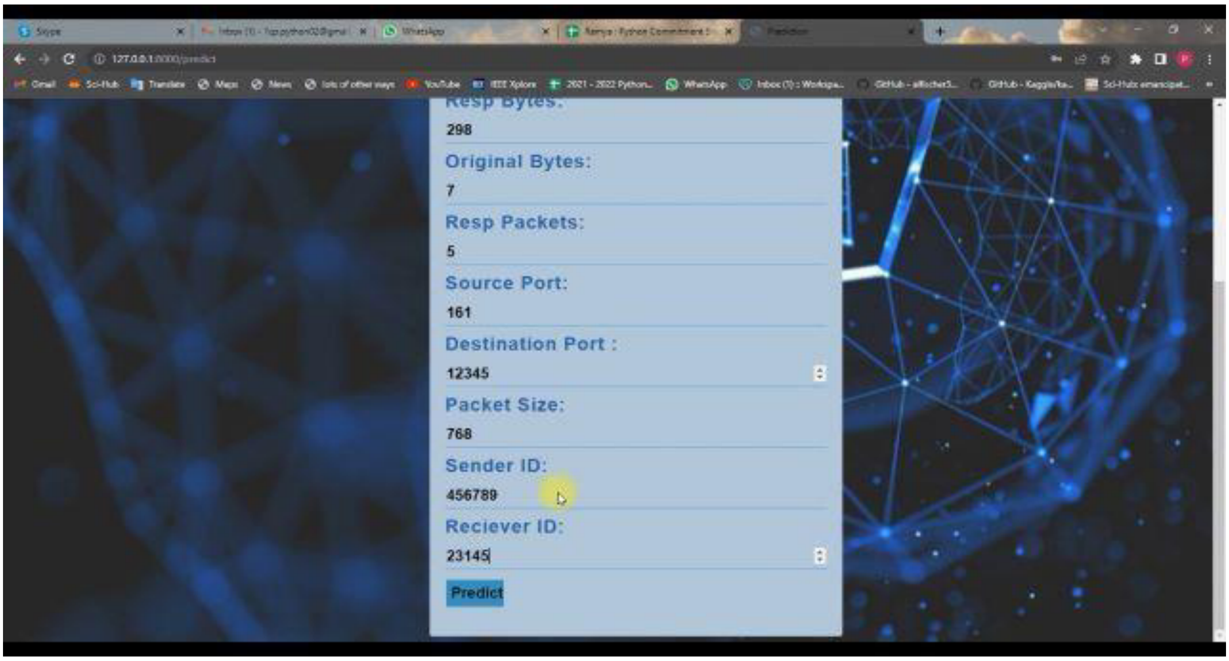
Username :

Email :

Password :

Re-Enter Password :

Fig A.2.3 Register Page



Resp Bytes:
298

Original Bytes:
7

Resp Packets:
5

Source Port:
161

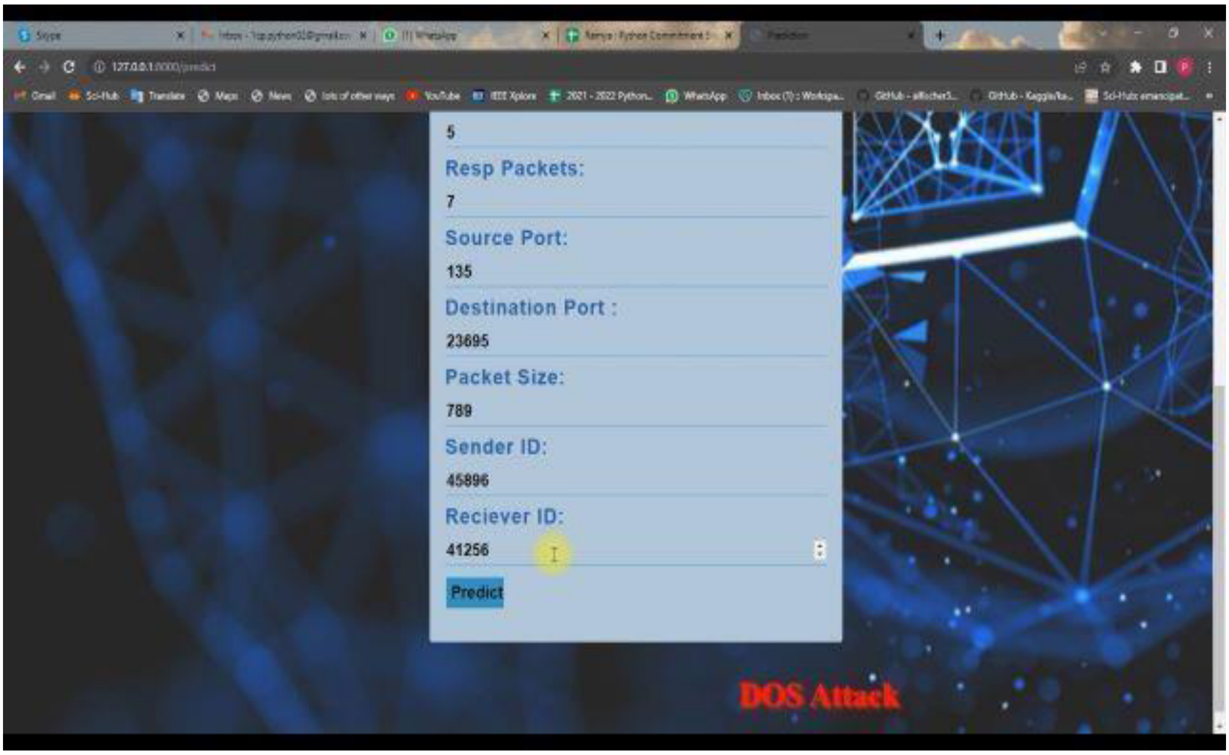
Destination Port :
12345

Packet Size:
768

Sender ID:
456789

Reciever ID:
23145

Fig A.2.4 Prediction Page



5

Resp Packets:

7

Source Port:

135

Destination Port :

23695

Packet Size:

789

Sender ID:

45896

Reciever ID:

41256

DOS Attack

Fig A.2.5 Result Page

Result

This document contains 12% plagiarism. This means that the author has copied data from public sources when writing this work.

Analysis

Result	12%
Document title	E17-Conference paper
Content hash	1a5e447df2d030163fb9656352883799
Date	2024-03-09 09:24:58
Check time	37 seconds
Character count	29129
Special character count	76
Word count	4333
Number of plagiarized words	494

Welcome Jennifer D Sign out

Controller General of Patents, Designs & Trade Marks

सत्यमेव जयते

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

G.A.R.6
[See Rule 22(1)]
RECEIPT

Docket No 45100

Date/Time 2024/03/23 12:49:01

To
Jennifer D

UserId: Malar@14

Panimalar Engineering College Bangalore
Trunk Road, Varadharajapuram,
Poonamallee, Chennai- 600123.

CBR Detail:

Sr. No.	App. Number	Ref. No./Application No.	Amount Paid	C.B.R. No.	Form Name	Remarks
1	202441022699	TEMP/E-1/27239/2024-CHE	1600	20135	FORM 1	Proactive Analysis of Cyber Threat to Ensure Cyber security

TransactionID	Payment Mode	Challan Identification Number	Amount Paid	Head of A/C No
N-0001372453	Online Bank Transfer	2303240010440	1600.00	1475001020000001

Total Amount : ₹ 1600.00
Amount in Words: Rupees One Thousand Six Hundred Only

Received from Jennifer D the sum of ₹ 1600.00 on account of Payment of fee for above mentioned Application/Forms.
* This is a computer generated receipt, hence no signature required.

Print

Home About Us Contact Us