

A PROPOSED FRAMEWORK FOR CONTROLLING CYBER CRIME USING PYTHON

Submitted in partial fulfilment of the requirements
for the award of
Bachelor of Engineering degree in Computer Science and Engineering

by

Talluri Ramakrishna(Reg.No.37110766)

Reddy Mohan Chandu(Reg.No.37110636)



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600 119

MARCH - 2021



SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with "A" grade by NAAC
Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this project report is the bonafide work of **TALLURI RAMAKRISHNA(Reg. No. 37110766)** and **REDDY MOHAN CHANDU(Reg. No. 37110636)** who carried out the project entitled "**A PROPOSED FRAMEWORK FOR CONTROLLING CYBER CRIME USING PYTHON**" under my supervision from **March 2021**.

Internal Guide
Dr. V.NIRMALRANI

Head of the Department

Submitted for Viva voce Examination held on _____

Internal Examiner

External Examiner

DECLARATION

I **TALLURI RAMAKRISHNA** hereby declare that the Project Report entitled **“A PROPOSED FRAMEWORK FOR CONTROLLING CYBER CRIME USING PYTHON”** is done by me under the guidance of **Dr.V.NIRMALRANI**, Department of Computer Science and Engineering at Sathyabama Institute of Science and Technology is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in Computer Science and Engineering.

DATE:

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala ,Dean**, School of Computing, **Dr. S. Vigneswari, M.E., Ph.D., and Dr. L. Lakshmanan ,Heads of the Department** of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr.V.NIRMALRANI , Associate Professor**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

The usage of the internet as part of our daily routine has brought many advantages and has also facilitated our lifestyle, the activities that required hours or days to be solved like sending a message to a far person has been reduced to a short time. The Internet has not only brought advantages to our community but also disadvantages, among the drawbacks of the internet we have cyber-crime activity. Cyber-crime activity is one of the biggest challenges that the world is facing. It is the concern of everyone as the main goal is to bring cybersecurity to reduce the number of losses that the crime generates across the globe. Cybercrime is happening every second anywhere, and it is causing much damage not only in terms of data or privacy breaches but financially also. Many countries are lacking an excellent policy to tackle cybercrime, and for that reason, the number of crimes is increasing day by day. As much as the number of crimes is increasing, likewise, the number of financial losses is also increasing. In this project, we proposed a framework that will help us fight against cybercrime regardless of the place we are located by monitoring the activities done on our electronic devices.

TABLE OF CONTENTS

ABSTRACT

v

LIST OF FIGURES

viii

CHAPTER NO	TITLE	PAGE NO
1	INTRODUCTION	1
	1.1 OVERVIEW	1
	1.2 MACHINE LEARNING	3
	1.3 MACHINE LEARNING METHODS	3
	1.3.1 SUPERVISED LEARNING	3
	1.3.2 UNSUPERVISED LEARNING	4
2	LITERATURE SURVEY	4
	2.1 AN ASSESSMENT OF U.S LEGISLATION	5
	2.2 ON THE DEFINITION AND CLASSIFICATION	5
	2.3 COMPUTER CRIME AND ABUSE	5
	2.4 HATE IN CYBERSPACE	5
	2.5 IMPOSSIBLE TO REGULATE	5
3	METHODOLOGY	6
	3.1 EXISTING SYSTEM	

3.2	PROPOSED SYSTEM	6
3.3	OBJECTIVE OF THE PROJECT	7
3.4	SOFTWARE AND HARDWARE SPECIFICATION	8
3.4.1	SOFTWARE REQUIREMENTS	8
3.4.2	HARDWARE REQUIREMENTS	8
3.4.3	LIBRARIES	9
3.5	PROGRAMMING LANGUAGES	9
3.5.1	PYHTON	9
3.5.2	DOMAIN	9
3.6	SYSTEM ARCHITECTURE	10
3.7	MODULES	10
3.7.1	PHISHING	10
3.7.2	CYBER LAUNDERING	10
3.7.3	CYBERWARFARE	11
3.7.4	IDENTIFYING CYBERCRIME FEATURES	11
	ELEMENTS	11
3.7.5	DECISION TREE	
3.7.6	RANDOM FOREST	12

3.8	DIAGRAMS	13
3.8.1	DATA FLOW DIAGRAM	16
3.8.2	UML DIAGRAM	16
3.8.3	USE CASE DIAGRAM	17
3.8.4	CLASS DIAGRAMS	17
3.8.5	SEQUENCE DIAGRAM	18
4	RESULT AND DISCUSSION	19
4.1	BENIFITS	21
5	CONCLUSION	21
5.1	CONCLUSION	22
5.2	FUTURE WORK	22
	REFERNCES	22
	APPENDIX	23
	A.SCREEN SHOTS	
	B.SAMPLE CODE	25
	C.PLAGIARISM REPORT	26
	D.JOURNAL PAPER	27
		30

LIST OF FIGURES

FIGURE No.	FIGURE NAME	PAGE No.
3.1	SYSTEM ARCHITETURE	15
3.2	DATA FLOW DIAGRAM	18
3.3	USE CASE DIAGRAM	20
3.4	CLASS DAIGRAM	21
3.5	SEQUENCE DIAGRAM	22

CHAPTER 1

INTRODUCTION

CYBERCRIME involves a mixture of diverse typical crimes with new illegal acts. Individual cybercrime incidents are occurrences of particular criminal offences and, as multiple national crime statistics and surveys demonstrate, are steadily increasing. According to the Federal Bureau of Investigation, the Internet Complaint Center received 269 422 complaints of Internet crime in 2014, which indicates a rise of 1600% in comparison to the 16 838 complains included in the initial report. In a worldwide study released by PricewaterhouseCoopers, the number of reported information security incidents around the world rose 48% in 2014, the equivalent of 117 339 attacks per day. Similarly, the German Crime Statistics indicated a 23.6% increase in the number of cybercrime incident from 2007 to 2008. The various offences of cybercrime pose a serious threat to the global economy, safety, and well-being of the society. In a PricewaterhouseCoopers report, it is highlighted that cyber-security incidents are not only increasing in number but they are also becoming progressively destructive and target a broadening array of information and attack vectors.

The various offences of cybercrime pose a serious threat to the global economy, safety, and well-being of the society. In a PricewaterhouseCoopers report, it is highlighted that cyber-security incidents are not only increasing in number but they are also becoming progressively destructive and target a broadening array of information and attack vectors. This advancement poses a serious threat to the operations of businesses, organizations and national economies as the global financial damage is estimated around \$225 billion. Moreover, the impact of cybercrime offences to individuals is also immense; from identity theft to sexual exploitation of children and cyber-harassment, the various cybercrime offences provoke from a slight discomfort to severe mental harm, public fear and financial loss. Due to its complex nature, a series of definitions of cybercrime exist in literature and in different agencies responsible to tackle it.

1.1 OVERVIEW

The U.S. Government does not have an official definition of cybercrime that distinguishes it from common criminal offences. Similarly, there is not a definition of cybercrime that

differentiates it from other forms of cyber threats, and the term is often used interchangeably with other Internet- or technology-linked malicious acts such as cyber warfare, and cyber terrorism. A more coordinated attempt aiming to the perception of a widely accepted definition was proposed in the Convention on Cybercrime [10]. In the summary of the treaty, cybercrimes are defined as “crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, and violations of network security.” In the accompanying explanatory report, cybercrimes are also referred to as “cyber-space offences” that are “either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks, or they consist of the use of such networks of their services to commit traditional offences.” Nevertheless, even though this implementation is relatively thorough, there are considerable gaps regarding the specification of each feature of the above definition.

Gordon and Ford proposed a typology consisted of two categories. Type I offences characterize singular or discrete events facilitated by the introduction of malware programs such as keystroke loggers, viruses, and rootkits. Type II offences are facilitated by programs that are not classified as crime ware, and they are generally repeated contacts or events from the perspective of the user. A much broader classification, was recommended by Wall [15] proposing three distinct categories. The first is Computer Integrity Crimes including the illegal activities of cracking, hacking and denial of service (DoS). In the second category of Computer-Assisted Crimes the offences of virtual robberies, scams, and thefts are included. The third category is Computer Content Crimes including pornography, violence, and offensive communications. Legal approaches have adopted different perceptions regarding cybercrime types in need of criminalization. In the U.S. Computer Fraud and Abuse Act 1986, an initial enumeration of computer criminal acts was introduced, serving as a federal statute with no concise classes incorporated in an early system. The need, though, for legislative reform, induced policy makers in the USA to organize the distinct offences committed in a single cybercrime incident across a range of offence categories. Toward this direction, the U.S. Department of Justice differentiated cybercrimes in three distinct categories depending on: 1) whether the computer is the instrument used to commit the offence; 2) the target of the offence; or 3)

incidental to the offence. In regards to monitoring of computer-related offences, organizations and agencies such as EUROPOL, FBI, and European Union Agency for Network and Information Security (ENISA) compose annual reports for cybercrime and cyber threats, bringing about threat trends on a yearly basis. However, it is arduous undertaking to quantify the impact of computer related offences on societies, on the basis of the number of offences carried out in a given time-frame. Another important fact about these statistics is that they deal with cybercrimes that are detected and reported, which can lead to the assumption that the actual number of cybercrimes is significantly larger. Also, many of these reports do not provide a direct matching of particular offences with concrete actions, counter-measures, and policies that are appropriate and essential for the elimination of particular cybercrime incidents.

1.2 MACHINE LEARNING

Machine learning is a subfield of artificial intelligence (AI). The goal of machine learning generally is to understand the structure of data and fit that data into models that can be understood and utilized by people.

Although machine learning is a field within computer science, it differs from traditional computational approaches. In traditional computing, algorithms are sets of explicitly programmed instructions used by computers to calculate or problem solve. Machine learning algorithms instead allow for computers to train on data inputs and use statistical analysis in order to output values that fall within a specific range. Because of this, machine learning facilitates computers in building models from sample data in order to automate decision-making processes based on data inputs.

1.3 Machine Learning Methods

In machine learning, tasks are generally classified into broad categories. These categories are based on how learning is received or how feedback on the learning is given to the system developed.

Two of the most widely adopted machine learning methods are **supervised learning** which trains algorithms based on example input and output data that is labelled

by humans, and **unsupervised learning** which provides the algorithm with no labelled data in order to allow it to find structure within its input data.

1.3.1 Supervised Learning

In supervised learning, the computer is provided with example inputs that are labeled with their desired outputs. The purpose of this method is for the algorithm to be able to “learn” by comparing its actual output with the “taught” outputs to find errors, and modify the model accordingly. Supervised learning therefore uses patterns to predict label values on additional unlabelled data.

For example, with supervised learning, an algorithm may be fed data with images of sharks labelled as fish and images of oceans labelled as water. By being trained on this data, the supervised learning algorithm should be able to later identify unlabelled shark images as fish and unlabelled ocean images as water.

A common use case of supervised learning is to use historical data to predict statistically likely future events. It may use historical stock market information to anticipate upcoming fluctuations, or be employed to filter out spam emails. In supervised learning, tagged photos of dogs can be used as input data to classify untagged photos of dogs.

1.3.2 Unsupervised Learning

In unsupervised learning, data is unlabelled, so the learning algorithm is left to find commonalities among its input data. As unlabelled data are more abundant than labelled data, machine learning methods that facilitate unsupervised learning are particularly valuable.

The goal of unsupervised learning may be as straightforward as discovering hidden patterns within a dataset, but it may also have a goal of feature learning, which allows the computational machine to automatically discover the representations that are needed to classify raw data.

Unsupervised learning is commonly used for transactional data. You may have a large dataset of customers and their purchases, but as a human you will likely not be able to make sense of what similar attributes can be drawn from customer profiles and their types of purchases. With this data fed into an unsupervised learning algorithm, it may be

determined that women of a certain age range who buy unscented soaps are likely to be pregnant, and therefore a marketing campaign related to pregnancy and baby products can be targeted to this audience in order to increase their number of purchases.

CHAPTER 2

LITURATURE SURVEY

2.1 An assessment of U.S. legislation on cybersecurity

Cybercrime continues to be on the rise and cybercriminals are launching increasingly sophisticated cyber attacks aimed at disrupting businesses through denial of service attacks and stealing personal information all with serious economic consequences. Law and policy makers are under increasing pressure to develop timely legislations to address cybercrime issues and provide effective measures to prosecute cybercriminals. We present a comprehensive review of the various laws that are currently available in the Unites States to control cybercrime and support cybersecurity. We also discuss proposed bills in light of how they address cybersecurity challenges in current legislations. Finally, we briefly present recent regulations and proposed bills related to cybersecurity in a few other countries which have set up various government initiatives in this area.

2.2 On the definition and classification of cybercrime

The idea of Cybercrime is not new, yet there is significant confusion amongst academics, computer security experts and users as to the extent of real Cybercrime. In this paper, we explore the breadth of computer-based crime, providing a definition of the emerging terms “Cybercrime” and “crimeware”. We then divide Cybercrime into two distinct categories: Type I Cybercrime, which is mostly technological in nature, and Type II Cybercrime, which has a more pronounced human element. We then use two case studies to illustrate the role of crimeware in different types of Cybercrime, and offer some observations on the role

of cognition in the process of Cybercrime. Finally we provide several suggestions for future work in the area of Cybercrime

2.3 Computer crime and abuse: A survey of public attitudes and awareness

In recent years, a number of surveys have indicated a significant escalation in reported incidents of computer crime and abuse. This rise is coupled with increasing attention to the issue in the mass media, which has the effect of heightening public perceptions of problems with IT and may represent a barrier to the adoption of technologies such as the Internet and World Wide Web.

This paper considers the effects of computer crime and draws upon the results of a survey conducted to assess public attitudes and awareness of the issue. With the mass media playing an important role in shaping individual opinions, this survey considered the effect that the reporting of incidents has upon public perceptions and understanding of computer crime and abuse

2.4 Hate in Cyberspace: Regulating Hate Speech On the Internet

The speed at which information can be spread throughout the United States and other countries has been greatly enhanced by the Internet. This computer-driven, technological medium consists of various modes of transmission, including discussion groups, interactive pages, and mail services. A wide variety of pictorial, auditory, and written information is available on the Internet. Persons with disparate goals can access and affect large audiences through it. Both those seeking social improvement and those promoting racist violence can now increase the magnitude, diversity, and location of their audiences. Persons advancing democratic ideals and those inclined to exclusionary elitism can use emails and electronic chat rooms to communicate with like-minded individuals located in different cities and in other lands.

2.5 Impossible to Regulate: Social Media, Terrorists, and the Role for the U.N.

The posting of journalist beheadings online and the arrests of numerous nationals attempting to join terrorist organizations have shown that terrorists are increasingly using social media to spread ideology and recruit members. The popularity of social media around the world provides a huge potential audience for terrorist content. Unfortunately,

because of states' inability to cooperate, previous attempts to govern and police the Internet have failed. Any regulation of the Internet or social media also raises collective action problems and baseline definition issues. The U.N. is not in the position to pass a binding treaty or convention because use of social media by terrorists is harder to identify than other regulated areas of internet use. Despite these problems, this Comment suggests that the U.N. still has an important role to play in the regulation of terrorist content in social media. By taking a role as a coordinator between states, the U.N. can create an effective monitoring regime that reduces the costs of internet governance and promotes coordination between states.

CHAPTER 3

METHODOLOGY

3.1 EXISTING SYSTEM

Due to its complex nature, a series of definitions of cybercrime exist in literature and in different agencies responsible to tackle it. The U.S. Government does not have an official definition of cybercrime that distinguishes it from common criminal offences. Similarly, there is not a definition of cybercrime that differentiates it from other forms of cyber threats, and the term is often used interchangeably with other Internet- or technology-linked malicious acts such as cyber warfare, and cyber terrorism.

DISADVANTAGES OF EXISTING SYSTEM

The various offences of cybercrime pose a serious threat to the global economy, safety, and well-being of the society. In a recent Waterhouse Coopers report, it is highlighted that cyber-security incidents are not only increasing in number but they are also becoming progressively destructive and target a broadening array of information and attack vectors. This advancement poses a serious threat to the operations of businesses, organizations and national economies as the global financial damage is estimated around \$225 billion. Moreover, the impact of cybercrime offences to individuals is also immense; from identity

theft to sexual exploitation of children and cyber-harassment, the various cybercrime offences provoke from a slight discomfort to severe mental harm, public fear and financial loss

3.2 PROPOSED SYSTEM

The multiple interpretations of what cybercrime entails along with non-systematic classification of the corresponding offences and lack of recommended actions are not contributing toward managing and orchestrating effective directives, policies, and legislative initiatives at local, national, or international level and result in ineffective handling of cybercrime incidents. This project aims to contribute toward better understanding cybercrime by proposing a schema-based cybercrime incident description that: 1) identifies the features of a cybercrime incident and their potential elements and 2) provides a two-level offence classification system based on specific criteria. The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that counteract the offence type and subsequently the particular incident. This matching will enable better monitoring, handling, and moderating the various cybercrime offences and their incarnation in the form of specific incidents.

ADVANTAGES OF PROPOSED SYSTEM

The final feature that the authors suggest is not directly linked with the description of the incident itself but ties it to: 1) immediate actions to handle it; 2) specific measures to prevent similar offences; and 3) elaborate policies that suggest formal action toward a specific category of cybercrime. The authors believe that it is important to properly assign cybercrime incidents to criminal offences utilizing a systematic approach and also allocate specific actions, measures and policies so that an incident is properly addressed in all levels— from immediate actions to national policies. Especially, for cybercrime offences with high frequency of occurrences this can prove quite helpful as a guide. However, this last feature requires further investigation and it is not analyzed further in this project.

3.3 OBJECTIVE OF THE PROJECT

The multiple interpretations of what cybercrime entails along with non-systematic classification of the corresponding offences and lack of recommended actions are not contributing toward managing and orchestrating effective directives, policies, and

legislative initiatives at local, national, or international level and result in ineffective handling of cybercrime incidents. This project aims to contribute toward better understanding cybercrime by proposing a schema-based cybercrime incident description that: 1) identifies the features of a cybercrime incident and their potential elements and 2) provides a two-level offence classification system based on specific criteria. The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that counteract the offence type and subsequently the particular incident. This matching will enable better monitoring, handling, and moderating the various cybercrime offences and their incarnation in the form of specific incidents.

3.4 SOFTWARE AND HARDWARE REQUIREMENTS

3.4.1.1 *Software Requirements:*

- ✓ Python
- ✓ Anaconda
- ✓ Jupyter Notebook

3.4.2 *Hardware Requirements:*

- ✓ Processor: Intel Core i5
- ✓ RAM: 8GB
- ✓ OS: Windows

3.4.3 *Libraries:*

- ✓ Sklearn- used for importing machine learning models, get accuracy, get confusion matrix.
- ✓ Pandas- Used to read the dataset.
- ✓ Matplotlib- Matplotlib is a plotting library for the Python programming language and its numerical mathematical extension NumPy. In this, it is used for data visualisation.
- ✓ Numpy- Numpy is a python library used for working with arrays. It also has functions for domain of linear algebra, fourier transform, and matrices. Numpy stands for Numerical Python.

- ✓ Pandas profiling- Pandas Profiling is an open source Python module with which we can quickly do an exploratory analysis in just few lines of code. In this, it is used to get detailed report of the dataset.

3.5.PROGRAMMING LANGUAGES

3.5.1 PYTHON

- ✓ Python is the best programming language suited for Machine Learning. According to studies and surveys, Python is the fifth most important language as well as the most popular language for machine learning and data science. It is because of the following strengths that Python has –
- ✓ **Easy to learn and understand** – The syntax of Python is simpler; hence it is relatively easy, even for beginners also, to learn and understand the language.
- ✓ **Multi-purpose language** – Python is a multi-purpose programming language because it supports structured programming, object-oriented programming as well as functional programming.
- ✓ **Support of open source community** – As being open source programming language, Python is supported by a very large developer community. Due to this, the bugs are easily fixed by the Python community. This characteristic makes Python very robust and adaptive.

3.5.2 DOMAIN

Machine learning is a subfield of artificial intelligence (AI). The goal of machine learning generally is to understand the structure of data and fit that data into models that can be understood and utilized by people. Although machine learning is a field within computer science, it differs from traditional computational approaches. In traditional computing, algorithms are sets of explicitly programmed instructions used by computers to calculate or problem solve. Machine learning algorithms instead allow for computers to train on data inputs and use statistical analysis in order to output values that fall within a specific range. Because of this, machine learning facilitates computers in building models from sample data in order to automate decision-making processes based on data inputs.

3.6 SYSTEM ARCHITECTURE:



Fig 3.1 System Architecture

3.7 MODULES

3.7.1 Phishing

The offence of phishing is a form of social engineering through which the attacker obtains sensitive information by fraudulently pretending to be a trustworthy third party. The attack is mainly conducted with the use of spoofed e-mails, or through the installation of malware on the victims' computers; however, other methods may exist deriving from the attacker's imagination and technical expertise.

Consequently, the victims perceive these e-mails as legitimate providing sensitive information such as credit card and e-banking account numbers and passwords, thus, circumventing every possible security measure. It is of no interest whether a computer system is equipped with highly sophisticated firewall, anti-virus and encryption software and authentication mechanisms, if the individual using it falls for the phish. Phishing as a digital offence may seem to be a variant of spam, and therefore categorized in the content-related offences.

3.7.2 Cyber Laundering

The Internet provides multiple methods for money-laundering, due to its characteristics that attract criminals. For example, an offender can hide his identity pretending to be someone else, while financial transactions are depersonalized as no face-to-face contact is necessary, and funds can be rapidly transferred throughout the world with little or no expense. Another great advantage for offenders is the fact that several jurisdictions and legal systems are usually involved in the case of cyber-laundering offences, as they are

often cross-border activities. Because of the growing demand for micro-payments and the problematic

use of credit cards, virtual currencies were developed in the last 20 years, providing the opportunity for Internet users to engage in criminal activity. One of the most widespread actualizations of cyber laundering is through virtual currencies, such as Bitcoin that uses peer-to-peer technology.

3.7.3 Cyberwarfare

Cyberwarfare also referred to as electronic warfare, cyberwar, or information war, is used to describe the usage of information technologies in conducting warfare through the Web, having tremendous advantages such as the ability to take down an enemy without getting involved in a fight. In addition, attacks using ICT are generally cheaper and faster than ordinary military attacks, and can even be conducted by small states. In Estonia came under cyber-attack in the wake of relocation of the “Bronze Soldier of Tallinn,” a Second World War memorial. This act apart from street riots, led to coordinated computerrelated attacks originating from multiple countries. Initially Russia was accused as the instigator of the attack, further analysis though, unveiled the participation of computers situated in 178 countries. These attacks targeted mainly government and private sector official websites and online services, causing major economic instability.

3.7.4 Identifying Cybercrime Features And Elements

Type A offences pertain to criminal activity that involves the requisite targeting of information and communication technologies. What can be highlighted is that the actual target is almost always non-ICT-related, as the offender’s objective is to eventually gain profit, damage morality or social values. It is obligatory though that the initial target is ICT either of individuals or entities, or as part of an infrastructure network for the attack to be considered cybercrime. Moreover, as indicated in schema, the harm imposed has two levels of effect. The first immediate level is composed of individual harm, such as instant loss of property and substantial damage, and direct systemic harm which is any harm with instant large scale consequences like shutting down of critical infrastructure and failure of a government function. Subsequently, as time passes,

aggregated and generalized individual harm arise, e.g., in the form of civil disturbance and social disorder. It is also possible that potential inchoate harm is caused, as for example data illegally acquired can be used at a later stage, leading to individual.

3.7.5 Decision Tree

Decision tree learning is a method for approximating discrete-valued target functions.

- The learned function is represented by a decision tree. – A learned decision tree can also be re-represented as a set of if-then rules.
- Decision tree learning is one of the most widely used and practical methods for inductive inference.
- It is robust to noisy data and capable of learning disjunctive expressions.
- Decision tree learning method searches a completely expressive hypothesis . – Avoids the difficulties of restricted hypothesis spaces. – Its inductive bias is a preference for small trees over large trees.
- The decision tree algorithms such as ID3, C4.5 are very popular inductive inference algorithms, and they are successfully applied to many learning tasks.

Decision trees classify instances by sorting them down the tree from the root to some leaf node, which provides the classification of the instance.

- Each node in the tree specifies a test of some attribute of the instance.
- Each branch descending from a node corresponds to one of the possible values for the attribute.
- Each leaf node assigns a classification.
- The instance (Outlook=Sunny, Temperature=Hot, Humidity=High, Wind=Strong) is classified as a negative instance

In the previously introduced paradigm, feature generation and learning were decoupled. However, we may want to learn directly from the data. In the badges game, for example, it was helpful to consider the notion of vowels, which in previously introduced algorithms could be considered a feature to be introduced during generation. Decision trees, however, can learn this notion from the data itself.

Representing Data

Assume a large table with N attributes, and we want to know something about the people represented as entries in this table. Further assume that a label for people:

Own an expensive car Do not own an expensive car A simple way to represent this table is through a histogram on the attribute "own", later on, we may add another attribute gender, which makes the histogram into 4 entries (own & male, own & female, not own & male, not own & female). Let's say there are 16 attributes in total. If we only consider one attribute (1-d histograms), there will be 16 entries in the histograms. Similarly, 2-d histogram has 120 numbers, 3-d has 560 numbers. As number of attributes increases, the problem will be impossible to solve. Thus, we need a way to represent the data more meaningfully such that we can determine which are the most important attributes.

Code

```
# Load the Pandas libraries with alias 'pd'
import pandas as pd
import numpy as np
from sklearn.tree import DecisionTreeRegressor
from sklearn.svm import SVC
def process(input):

X=pd.read_csv("Cleaned.csv",usecols=['Latitude','Longitude','year','month','day','hour',
'min'])
    Y=pd.read_csv("Cleaned.csv",usecols=["PrimaryType"])
    print(Y.values.ravel())
    rf = DecisionTreeRegressor(random_state = 0)
    rf.fit(X,Y)
    X_test = np.array(input).reshape(1,-1)
    y_pred=rf.predict(X_test)
    print(y_pred[0])
    return y_pred[0]
```

3.7.6 Random Forest

Random Forest is a popular machine learning algorithm that belongs to the supervised learning technique. It can be used for both Classification and Regression

problems in ML. It is based on the concept of **ensemble learning**, which is a process of *combining multiple classifiers to solve a complex problem and to improve the performance of the model*.

As the name suggests, **"Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset."** Instead of relying on one decision tree, the random forest takes the prediction from each tree and based on the majority votes of predictions, and it predicts the final output.

Since the random forest combines multiple trees to predict the class of the dataset, it is possible that some decision trees may predict the correct output, while others may not. But together, all the trees predict the correct output. Therefore, below are two assumptions for a better Random forest classifier:

- There should be some actual values in the feature variable of the dataset so that the classifier can predict accurate results rather than a guessed result.
- The predictions from each tree must have very low correlations.

Below are some points that explain why we should use the Random Forest algorithm:

<="" |j="">

- It takes less training time as compared to other algorithms.
- It predicts output with high accuracy, even for the large dataset it runs efficiently.
- It can also maintain accuracy when a large proportion of data is missing.

How does Random Forest algorithm work?

Random Forest works in two-phase first is to create the random forest by combining N decision tree, and second is to make predictions for each tree created in the first phase.

The Working process can be explained in the below steps and diagram:

Step-1: Select random K data points from the training set.

Step-2: Build the decision trees associated with the selected data points (Subsets).

Step-3: Choose the number N for decision trees that you want to build.

Step-4: Repeat Step 1 & 2.

Step-5: For new data points, find the predictions of each decision tree, and assign the new data points to the category that wins the majority votes.

Advantages of Random Forest

- Random Forest is capable of performing both Classification and Regression tasks.
- It is capable of handling large datasets with high dimensionality.
- It enhances the accuracy of the model and prevents the overfitting issue.

Disadvantages of Random Forest

- Although random forest can be used for both classification and regression tasks, it is not more suitable for Regression tasks.

Python Implementation of Random Forest Algorithm

Now we will implement the Random Forest Algorithm tree using Python. For this, we will use the same dataset "user_data.csv", which we have used in previous classification models. By using the same dataset, we can compare the Random Forest classifier with other classification models such as Decision tree Classifier, KNN, SVM, Logistic Regression, etc.

Implementation Steps are given below:

- Data Pre-processing step
- Fitting the Random forest algorithm to the Training set
- Predicting the test result
- Test accuracy of the result (Creation of Confusion matrix)
- Visualizing the test set result.

Coding

```
# Load the Pandas libraries with alias 'pd'
```

```
import pandas as pd
```

```
import numpy as np
```

```
from sklearn.tree import DecisionTreeRegressor
```

```
from sklearn.preprocessing import StandardScaler
```

```
from sklearn.ensemble import RandomForestClassifier
```

```
def process(input):
```

```
X=pd.read_csv("Cleaned.csv",usecols=['Latitude','Longitude','year','month','day','hour',  
, 'min'])
```

```
Y=pd.read_csv("Cleaned.csv",usecols=['PrimaryType'])
```

```
print(Y.values.ravel())
X_test = np.array(input).reshape(1,-1)
clf=RandomForestClassifier()
clf.fit(X,Y)
y_pred = clf.predict(X_test)
print(y_pred[0])
return y_pred[0]
```

3.8 DIAGRAMS

3.8.1 Data Flow Diagram

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.

DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

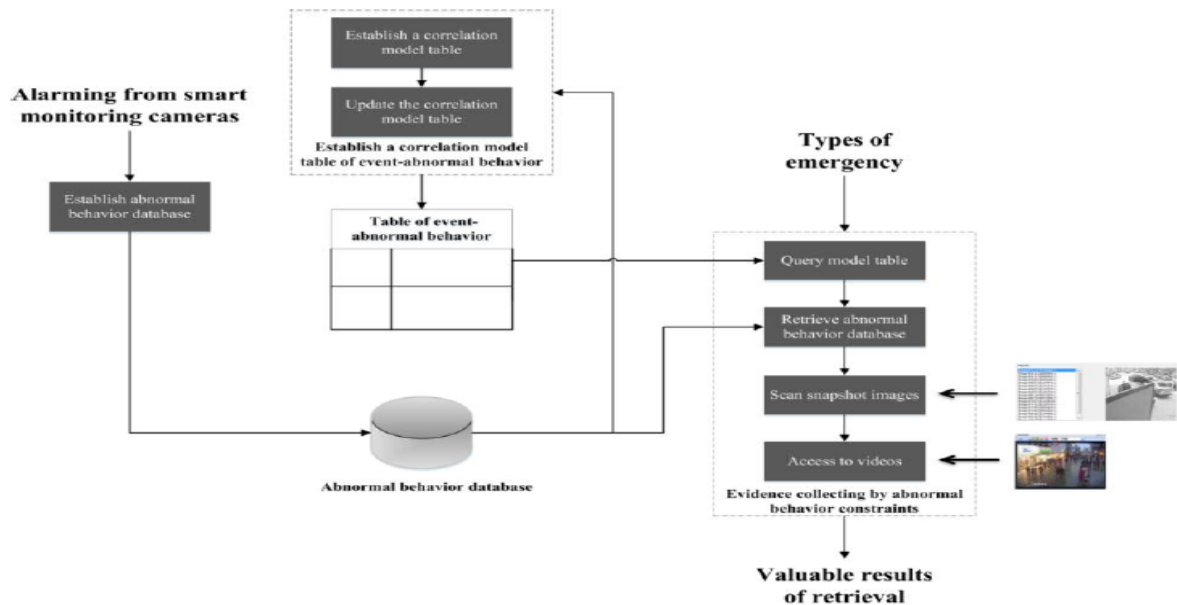


Fig 3.2 Data Flow Diagram

3.8.2 UML DIAGRAM

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

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

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

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

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

GOALS:

- ✓ The Primary goals in the design of the UML are as follows:
- ✓ Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
- ✓ Provide extendibility and specialization mechanisms to extend the core concepts.
- ✓ Be independent of particular programming languages and development process.
- ✓ Provide a formal basis for understanding the modeling language.
- ✓ Encourage the growth of OO tools market.
- ✓ Support higher level development concepts such as collaborations, frameworks, patterns and components.
- ✓ Integrate best practices.

3.8.3 USE CASE DIAGRAM

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

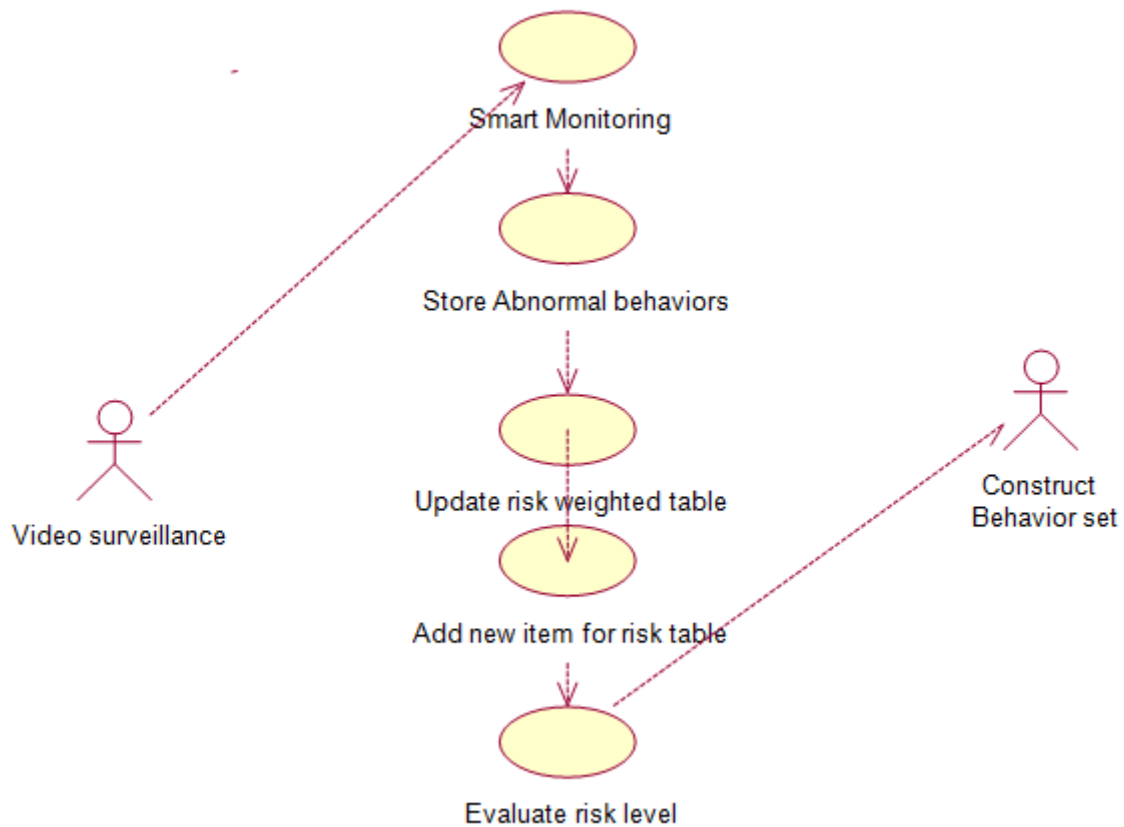


Fig 3.3 Use case diagram

3.8.4 Class Diagram

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

Fig 3.4 CLASS Diagram

diagrams, event scenarios, and timing diagrams.

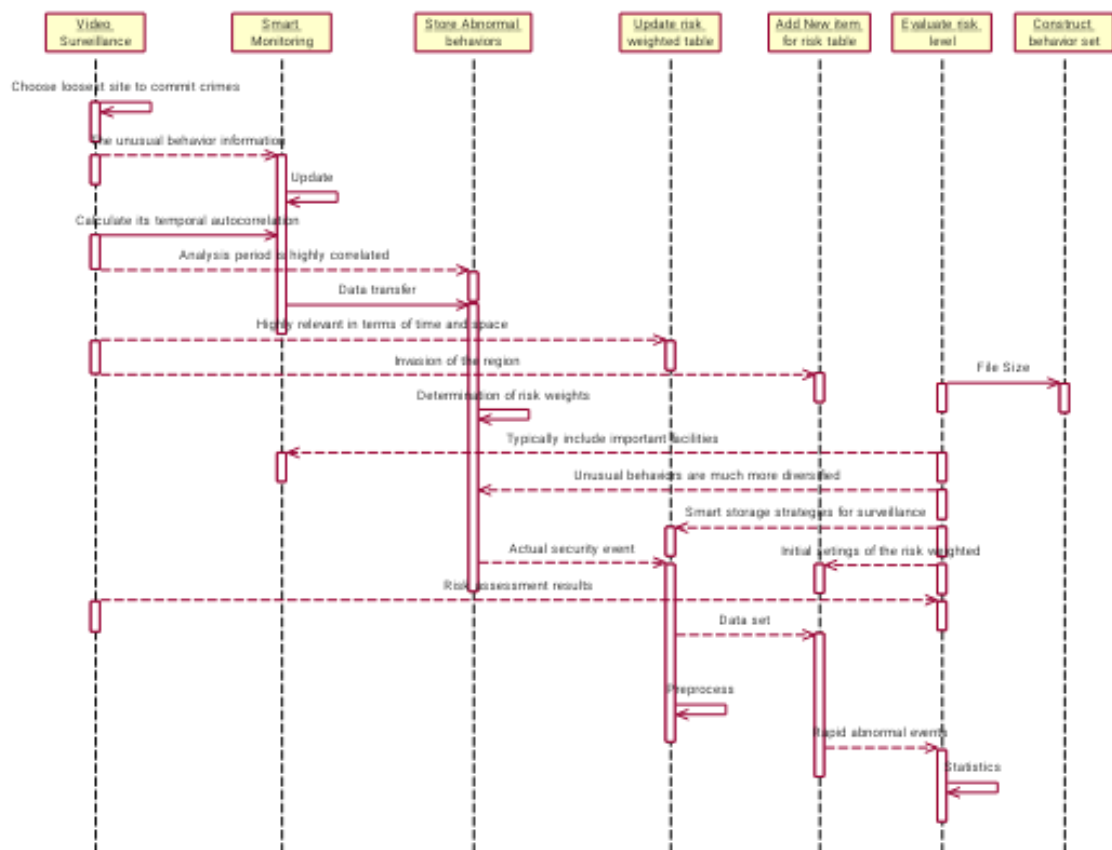


Fig 3.5 CLASS Diagram

CHAPTER 4

RESULT AND DISCUSSION

The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that match with the offence type and subsequently with a particular incident. This matching will enable better monitoring, handling and moderate cybercrime incident occurrences.

The ultimate objective is to incorporate the schema-based description of cybercrime elements to a complete incident management system with standard operating procedures and protocols.

The multiple interpretations of what cybercrime entails along with non-systematic classification of the corresponding offences and lack of recommended actions are not contributing toward managing and orchestrating effective directives, policies, and legislative initiatives at local, national, or international level and result in ineffective handling of cybercrime incidents. This paper aims to contribute toward better understanding cybercrime by proposing a schema-based cybercrime incident description that: 1) identifies the features of a cybercrime incident and their potential elements and 2) provides a two-level offence classification system based on specific criteria. The proposed schema can be extended with a list of recommended actions, corresponding measures and effective policies that counteract the offence type and subsequently the particular incident. This matching will enable better monitoring, handling, and moderating the various cybercrime offences and their incarnation in the form of specific incidents.

4.1 Benefits

The final feature that the authors suggest is not directly linked with the description of the incident itself but ties it to: 1) immediate actions to handle it; 2) specific measures to prevent similar offences; and 3) elaborate policies that suggest formal action toward a specific category of cybercrime. The authors believe that it is important to properly assign cybercrime incidents to criminal offences utilizing a systematic approach and also allocate specific actions, measures and policies so that an incident is properly addressed in all

levels— from immediate actions to national policies. Especially, for cybercrime offences with high frequency of occurrences this can prove quite helpful as a guide.

CHAPTER 5

CONCLUSION

5.1 Conclusion

The authors identified and presented the features of cybercrime incidents, a classification system for related offences and a schema that binds together the various elements and examines their interrelations to better suggest corresponding actions, measures and policies. The process involved revision of reports conducted by authorities, academia and agencies related to information security. The identification of cybercrime features allows for a more comprehensive description of individual incidents that leads to better understanding, handling and management of their occurrences.

The modular feature-based approach toward description of incidents allows for additional features to be included in the future. Also the expansion or consolidation of their respective elements can also be achieved depending on specific perspectives. This paper also proposed a comprehensive two-level classification system of cybercrime offences based on European Union's initial typology and further analysis taking account of the present status and recent forms of cybercrime. The system encompasses the most common forms of computer related offences and can prove useful for law enforcement agencies. Furthermore, the proposed system is included as part of the feature-based description to classify a cybercrime incident under a corresponding criminal offence.

5.2 Future Work

The authors are currently working in automating the proposed approach using the XML-based Structured Threat Information Expression; a structured language for describing cyber threat information so it can be shared, stored, and further analyzed. A future extension could take into account the frequency of occurrences in order to propose custom actions, measures and policies, and finally incorporate the produced schema in an

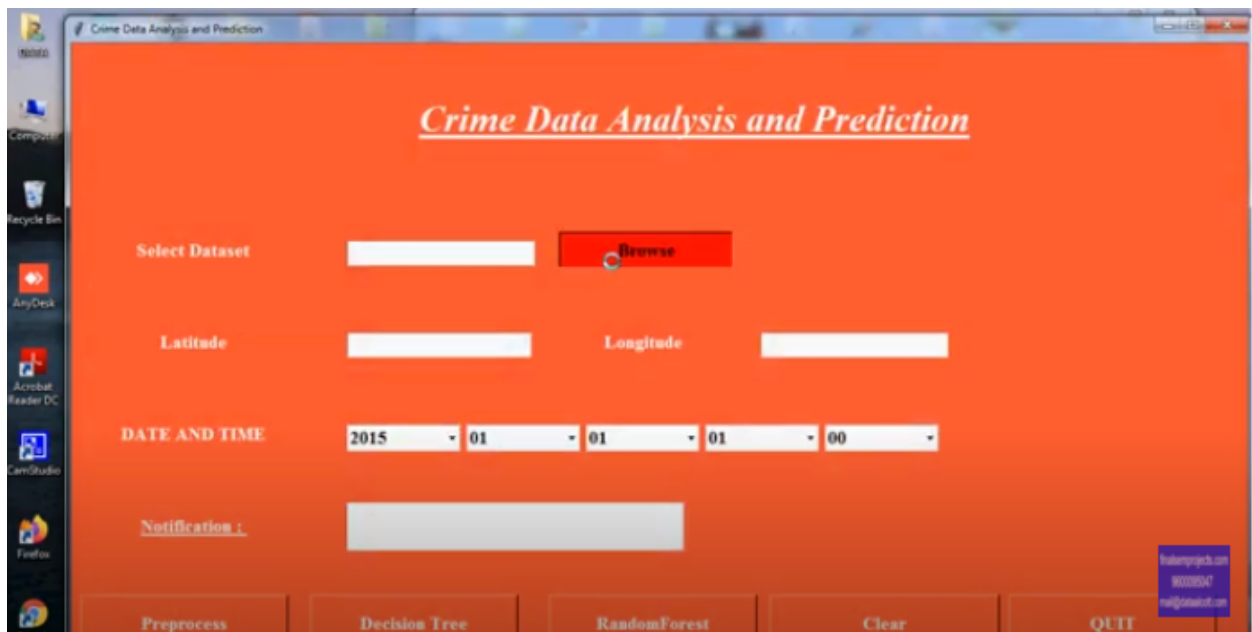
automated incident management system with standard operating procedures and protocols. The operational efficiency of such system would provide automated identification of incidents and emergency response protocols. Furthermore, all information handled by the system would be recorded in the form of an aggregator to produce analytics, statistics and visualizations for gaining insights and future planning, leading to optimization of handling cybercrime incidents by the relevant agencies.

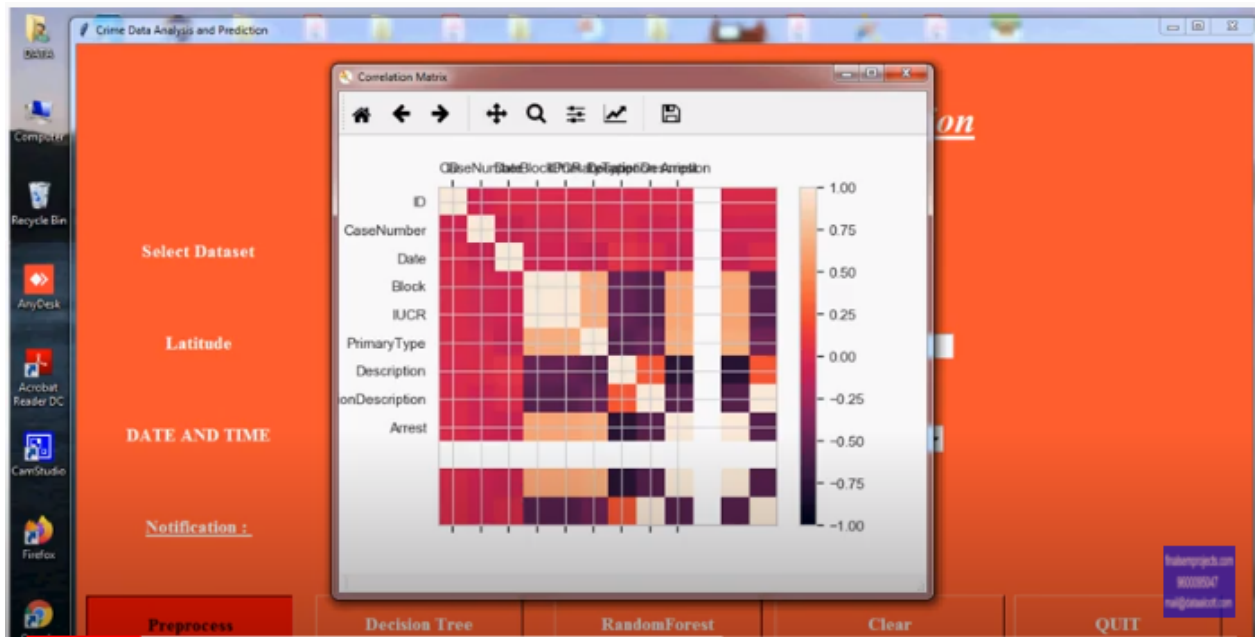
REFERENCES

1. User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.
2. Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.
3. Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.
4. Data Communications and Networking, by Behrouz A Forouzan.
5. Computer Networking: A Top-Down Approach, by James F. Kurose.
6. Operating System Concepts, by Abraham Silberschatz.
7. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
8. "The apache cassandra project," <http://cassandra.apache.org/>.
9. L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.
10. N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficient and differentiated data availability guarantees in data clouds," in Proc. of the ICDE, Long Beach, CA, USA, 2010.

APPENDIX

A) SCREENSHOTS





	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1	Date	PrimaryTy	Latitude	Longitude	year	month	day	hour	min												
2	0	arson	0	41.8914	-87.7444	2015	3	18	19	44											
3	1	arson	1	41.77337	-87.6653	2015	3	18	23	0											
4	2	arson	0	41.8786	-87.5966	2015	3	18	22	45											
5	3	arson	0	41.8008	-87.6226	2015	3	18	22	30											
6	4	arson	2	41.8786	-87.7434	2015	3	18	21	0											
7	5	arson	0	41.80544	-87.6043	2015	3	18	22	0											
8	6	arson	0	41.7664	-87.6493	2015	3	18	23	0											
9	7	arson	0	41.81755	-87.6198	2015	3	18	21	35											
10	8	arson	3	41.82834	-87.6728	2015	3	18	22	9											
11	9	arson	0	41.71745	-87.6177	2015	3	18	21	25											
12	10	arson	4	41.65834	-87.6117	2015	3	18	21	30											
13	11	arson	1	41.75241	-87.6338	2015	3	15	16	10											
14	12	arson	5	41.73856	-87.5527	2015	3	18	21	14											
15	13	arson	0	41.86304	-87.6663	2015	3	18	22	50											
16	14	arson	6	41.89495	-87.7549	2015	3	18	22	31											
17	15	arson	7	41.7546	-87.5627	2015	3	18	12	55											
18	16	arson	8	41.91031	-87.6878	2015	3	18	20	0											
19	17	arson	6	41.76817	-87.6591	2015	3	18	21	0											
20	18	arson	9	41.70285	-87.6246	2015	3	18	22	56											
21	19	arson	6	41.73659	-87.593	2015	3	18	22	45											
22	20	arson	6	41.75781	-87.5861	2015	3	18	22	0											
23	21	arson	2	41.98063	-87.6565	2015	3	18	23	55											
24	22	arson	0	41.75265	-87.5809	2015	3	18	23	40											
25	23	arson	5	41.88093	-87.7649	2015	3	18	21	44											

B)SAMPLE CODE

```
import tkinter as tk
from tkinter import Message ,Text
import shutil
import csv
import numpy as np
from PIL import Image, ImageTk
import pandas as pd
```

```

import datetime
import time
import tkinter.font as font
from tkinter import filedialog
import tkinter.messagebox as tm
import preprocess as pr
import RFALG as rf
import DTALG as dt
from tkinter import ttk

from_date = datetime.datetime.today()
currentDate = time.strftime("%d_%m_%y")
fontScale=1
fontColor=(0,0,0)
cond=0
bgcolor="#FF5733"
fgcolor="white"
window = tk.Tk()
window.title("Crime Data Analysis and Prediction")
window.geometry('1280x720')
window.configure(background=bgcolor)
#window.attributes('-fullscreen', True)
window.grid_rowconfigure(0, weight=1)
window.grid_columnconfigure(0, weight=1)
crim=['BATTERY','OTHER OFFENSE','ROBBERY','NARCOTICS','CRIMINAL
DAMAGE','WEAPONS VIOLATION','THEFT','BURGLARY','MOTOR VEHICLE
THEFT','PUBLIC PEACE VIOLATION','ASSAULT','CRIMINAL TRESPASS','CRIM
SEXUAL ASSAULT','INTERFERENCE WITH PUBLIC OFFICER','ARSON','DECEPTIVE
PRACTICE','LIQUOR LAW VIOLATION','KIDNAPPING','SEX OFFENSE','OFFENSE
INVOLVING
CHILDREN','PROSTITUTION','GAMBLING','INTIMIDATION','STALKING','OBSCENITY','P

```

UBLIC INDECENCY','HUMAN TRAFFICKING','CONCEALED CARRY LICENSE VIOLATION','OTHER NARCOTIC VIOLATION','HOMICIDE','NON-CRIMINAL']

C) PLAGIARISM REPORT

Report Title:	report2
Report Link: (Use this link to send report to anyone)	https://www.check-plagiarism.com/plag-report/22771216ac6bd18f8adef0038bfce674dc7d21615812770
Report Generated Date:	15 March, 2021
Total Words:	2698
Total Characters:	18577
Keywords/Total Words Ratio:	80.98%
Excluded URL:	No
Unique:	87%

Matched:	13%
Sentence wise detail: a proposed framework for controlling cyber crime using python ramakrishna mohan chandu and v. nirmalraniug student assitant professor dept. of cse sathyabama insistute of science and technology chennai. rktalluri0202 gmail. com mohanchowdary8501 gmail. com nirmalrani. it sathyabama. ac. in abstract crime is emerging as one of the most dangerous and dominating problem in world and its prevention is not	

D) JOURNAL PAPER

A PROPOSED FRAMEWORK FOR CONTROLLING CYBER CRIME USING PYTHON

¹Talluri Ramakrishna , ²Reddy Mohan Chandu , and ³Dr. V.Nirmalrani

^{1,2} UG Student, ³ Assistant Professor, Dept.of IT, Sathyabama Insistute of Science and Technology, Chennai.

¹rktalluri0202@gmail.com, ²mohanchowdary8501@gmail.com, ³nirmalrani.it@sathyabama.ac.in

Abstract— Crime is emerging as one of the most dangerous and dominating problem in world and its prevention is not that easy. Daily there are massive numbers of crimes committed frequently. This will require maintaining track of all the crimes and a database for same which may be very useful to reduce cyber crimes. The current cybercrime scenario issues are maintaining of proper dataset of crime and analyzing this data to help in predicting and solving crimes in future. The objective of this paper is to visualize the dataset and predict the type of crime which will happen in future using various conditions present in the dataset. In this

paper, we will be use machine learning and data science for crime prediction. The dataset used is Chicago crime dataset. The data related to crime brought out from the official portal of Chicago police. It takes the information of crime considering features description of location, crime type, and so on. Preprocessing should be done, before training of the model, following feature selection and scaling will be done and this leads to obtain a high amount of accuracy.

Keywords: Cybercrime, Data Science, Machine Learning

1.INTRODUCTION

Cybercrime involves a mix of various typical crimes with new illegitimate acts. Crime is rising in concert of the foremost dangerous and dominating downside in world and its interference isn't that straightforward.

Daily there are massive numbers of crimes committed frequently. This will require maintaining track of all the crimes and a database for same which may be very useful to reduce cybercrimes.

In a worth Water House Coopers report, it's highlighted that cyber-security incidents aren't solely increasing in variety however they're conjointly changing into more and more harmful and target a broadening array of data and attack vectors .

Cybercrime continues to be on the rise and cybercriminals are launching increasingly sophisticated cyber-attacks aimed at disrupting businesses through denial of service attacks and stealing personal information all with serious economic consequences.

Law is beneath most pressure to develop timely legislations to speak concerning crime problems and Implement effective measures to penalize cybercriminals and cut back cybercrimes .

We conjointly discuss projected bills in light-weight of however they address cyber security challenges in current legislations.

The objective of this paper is to check the dataset and predict the kind of crime which is able to happen in future victimization numerous conditions gift within the dataset.

During this paper, we are going to be use machine learning and information science for crime prediction.

The information set used is Chicago crime data set. The information associated with crime brought out from the official portal of Chicago police. It takes the knowledge of crime considering options description of location, crime type, and so on.

Preprocessing ought to be done, before coaching of the model, following feature choice and scaling are done and this ends up in get a high quantity of accuracy.

RELATED WORKS

An assessment of U.S. legislation on cyber-security in [1]

Cybercrime continues to air the increase and cybercriminals are launching progressively refined cyber-attacks aimed toward disrupting businesses through denial of service attacks and stealing personal data all with serious economic consequences . Law and policy manufacturers are beneath increasing pressure to develop timely legislations to handle law-breaking problems and supply effective measures to prosecute cybercriminals . We have a tendency to gift a comprehensive review of the assorted laws that are presently on the market within the Unites States to regulate law-breaking and support cyber-security. We have a tendency to conjointly discuss projected bills in light-weight of however they address cyber-security challenges in current legislations. Finally, we have a tendency to shortly gift recent laws and projected bills associated with cyber-security in an exceedingly few alternative countries that have established numerous government initiatives during this space.

On the definition and classification of law-breaking [2]

The idea of law-breaking isn't new, nevertheless there's important confusion amongst teachers, pc security specialists and users on the extent of real law-breaking. During this paper, we have a tendency to explore the breadth of computer-based crime, providing a definition of the rising terms "Cybercrime" and "crime-ware". We have a tendency to then divide law-breaking into 2 distinct categories: kind I law-breaking, that is usually technological in nature, and kind II law-breaking, that incorporates a lot of pronounced human component. We have a tendency to then use 2 case studies let's say the role of crime-ware in numerous styles of law-breaking, and supply some observations on the role of noesis within the method of law-breaking. Finally we offer many suggestions for future add the realm of law-breaking

Computer crime and abuse: A survey of public attitudes and awareness in [3]

In recent years, variety of surveys have indicated a big increase in reportable incidents of pc crime and abuse. This rise is not to mention increasing attention to the difficulty within the mass media, that has the impact of intensifying public perceptions of issues with IT and will represent a barrier to the adoption of technologies like the web and World Wide net. This paper considers the results of pc crime and attracts upon the results of a survey conducted to assess public attitudes and awareness of the difficulty. With the mass media taking part in a very important role in shaping individual opinions, this survey thought-about the impact that the news of incidents has upon public perceptions and understanding of pc crime and abuse

Hate in Cyberspace: regulation Hate Speech On the web in [4]

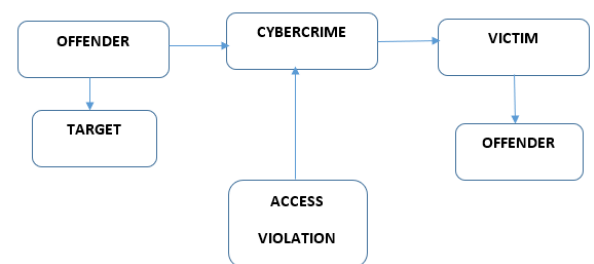
The speed at that data is unfold throughout the u. s. and alternative countries has been greatly increased by the web. This computer-driven, technological medium consists of varied modes of transmission, together with discussion teams, interactive pages, and mail services. a good kind of pictorial, auditory, and written data is offered on the web. Persons with disparate goals will access and have an effect on giant audiences through it. each those seeking social improvement and people promoting racist violence will currently increase the magnitude, diversity, and placement of their audiences. Persons advancing democratic ideals and people inclined to exclusionary ideology will use emails and electronic chat rooms to speak with similar people settled in numerous cities and in alternative lands.

Impossible to Regulate: Social Media, Terrorists, and also the Role for the U.N. in [5]

The posting of journalist beheadings on-line and also the arrests of various nationals trying to hitch terrorist organizations have shown that terrorists ar progressively victimization social media to unfold ideology and recruit members. The recognition of social media round the world provides an enormous potential audience for terrorist content. Sadly, as a result of states' inability to get together, previous tries to manipulate and police the web have unsuccessful. Any regulation of the web or social media conjointly raises collective action issues and baseline definition problems. The U.N. isn't within the position to pass a binding written agreement or convention as a result of use of social media by terrorists is tougher to spot than alternative

regulated areas of web use. Disagreement among U.N. members on whether or not web governance ought to be enforced by the international community conjointly makes a written agreement unlikely. Despite these issues, this Comment suggests that the U.N. still has a very important role to play within the regulation of terrorist content in social media. By taking a task as a arranger between states, the U.N. will produce an efficient watching regime that reduces the prices of web governance and promotes coordination between states.

3. System Architecture



4. MODULE IMPLEMENTATION

Phishing:

The offence of phishing may be a kind of social engineering through that the assailant obtains sensitive info by fraudulently feigning to be a trustworthy third party. The attack is principally conducted with the utilization of spoofed e-mails, or through the installation of malware on the victims computers but, alternative ways might exist account from the attacker's imagination and technical experience. Consequently, the victims understand these e-mails as legitimate providing sensitive info like master card and e-banking account numbers and passwords, thus, circumventing each doable security live. It's of no interest whether or not a automatic data processing system is provided with extremely refined firewall, anti-virus and encoding computer code and authentication mechanisms, if the individual victimization it falls for the phish. Phishing as a digital offence could appear to be a variant of spam, and so classified within the content-related offences.

Cyber Laundering:

The Internet provides multiple ways for money-laundering, thanks to its characteristics that attract criminals. For instance, an associate degree wrongdoer will hide his identity to be some other person, whereas money transactions are unit depersonalized as no face-to-face contact is critical, and funds are often speedily transferred throughout the planet with very little or no expense. Another nice advantage for offenders is that the undeniable fact that many jurisdictions and legal systems are unit sometimes concerned within the case of cyber-laundering offences, as they're usually cross-border activities. As a result of the growing demand for micro-payments and also the problematic use of credit cards, virtual currencies were developed within the last twenty years, providing the chance for net users to have interaction in criminal activity. One among the foremost widespread actualizations of cyber washing is thru virtual currencies, like Bitcoin that uses peer-to-peer technology.

Cyber-warfare:

Cyber-warfare conjointly noted as action, cyberwar, or data war, is employed to explain the usage of knowledge technologies in conducting warfare through the net, having tremendous benefits like the flexibility to require down an associate degree enemy while not obtaining concerned in a very fight. Additionally, attacks victimization ICT are unit typically cheaper and quicker than standard military attacks, and may even be conducted by little states. This act excluding street riots, LED to coordinated pc connected attacks originating from multiple countries. Russia was suspect because of the instigator of the attack, any analysis although, disclosed the participation of computers set in 178 countries. These attacks targeted in the main government and personal sector official websites and on-line services, inflicting major economic instability.

Identifying Cybercrime Features and Elements:

Type A offences pertain to criminal activity that involves the requisite targeting of knowledge and communication technologies. What are often highlighted is that the actual target is sort of continually non-ICT-related, because the offender's objective is to eventually gain profit, harm morality or social values. It's obligatory although that the

initial target is ICT either of people or entities, or as a part of an associate degree infrastructure network for the attack to be thought of crime. Moreover, as indicated in schema, the damage obligatory has 2 levels of impact. The primary immediate level consists of individual damage, like instant loss of property and substantial harm, and direct general damage that is any damage with instant massive scale consequences like motility down of essential infrastructure and failure of a government perform. Later, as time passes, mass and generalized individual damage arise, e.g., within the variety of civil disturbance and social disorder. It's conjointly potential that potential incipient damage is caused, as for instance information illicitly non-heritable are often used at a later stage, resulting in individual.

4. RESULTS AND DISCUSSIONS

The multiple interpretations of what crime entails beside non-systematic classification of the corresponding offences and lack of steered actions do not appear to be motivative toward managing and orchestrating effective directives, policies, and legislative initiatives at native, national, or international level and result in ineffective handling of crime incidents.

This paper aims to contribute toward higher understanding crime by proposing a schema-based crime incident description that: 1) identifies the choices of against the law incident and their potential parts and 2) provides a two-level offence arrangement supported specific criteria.

The projected schema is also extended with an inventory of steered actions, corresponding measures and effective policies that counteract the offence kind and after the particular incident. This matching will alter higher observance, handling, and palliative the various crime offences and their incarnation at intervals the type of specific incidents.

BENEFITS

The final feature that the authors counsel is not directly joined with the define of the incident itself but ties it to: 1) immediate actions to handle it; 2) specific measures to forestall similar offences; and 3) elaborate policies that counsel formal action toward a selected category of crime. The authors believe that it's a necessity to properly assign crime

incidents to criminal offences utilizing a scientific approach and collectively apportion specific actions, measures and policies so as that an incident is properly addressed in all levels— from immediate actions to national policies. Especially, for crime offences with high frequency of occurrences this might prove quite helpful as a guide. However, this last feature needs any investigation and it is not analyzed any throughout this paper.

6.CONCLUSION & FUTURE WORK

The authors known crime incidents, a organization for connected offences and a schema that binds on the various parts and examines their interrelations to higher counsel corresponding actions, measures and policies. the strategy involved revision of reports conducted by authorities, academia and agencies related to knowledge security.

The identification of crime choices permits for added comprehensive description of individual incidents that finishes up in higher understanding, handling and management of their occurrences. the quality feature-based approach toward description of incidents permits for further choices to be enclosed at intervals the long run.

Co-jointly the enlargement or consolidation of their many parts can also be achieved betting on specific views. This paper collectively planned a comprehensive two-level organization of crime offences supported European Union's initial compartmentalization and a lot of analysis taking account of this standing and up thus far forms of crime.

The system encompasses the foremost common forms of portable computer connected offences and should prove useful for social control agencies. what's a lot of, the planned system is enclosed as a neighborhood of the feature-based description to classify a criminal offense incident at a lower place a corresponding criminal offence.

FUTURE WORK

The authors area unit presently in operation in automating the planned approach victimization the XML-based Structured Threat knowledge Expression; a structured language for describing cyber threat knowledge so it's shared, stored, and a lot of analyzed.

A future extension would possibly take into thought the frequency of occurrences therefore on propose custom actions, measures and policies, associate degreed eventually incorporate the created schema in an automatic incident management system with customary operating procedures and protocols.

The operational efficiency of such system would provide machine-driven identification of incidents and emergency response protocols. what's a lot of, all knowledge handled by the system would be recorded at intervals the fashion of associate degree somebody to provide analytics, statistics and visualizations for gaining insights and future bobbing up with, leading to improvement of handling transgression incidents by the relevant agencies.

REFERENCES

- [1] D. L. Shinder and M. Cross, *Scene of the Cybercrime*. Burlington, MA,USA: Syngress, 2008.
- [2] FBI and NW3C. (May 22, 2015). *2014 Internet Crime Report*. Accessed on May 17, 2016. [Online]. Available: https://pdf.ic3.gov/2014_IC3Report.pdf
- [3] "IFCC 2002 Internet fraud report," FBI, Washington, DC, USA, and NW3C, Glen Allen, VA, USA, Tech. Rep. NCJ 194344, 2003.
- [4] PricewaterhouseCoopers. (Sep. 30, 2014). *The Global State of Information Security_ Survey 2015—Managing Cyber Risks in an Interconnected World*. Accessed on May 19, 2016. [Online]. Available: http://www.pwccn.com/webmedia/doc/635527689739110925_rcs_info_security_2015.pdf
- [5] Federal Criminal Police Office. (2009). *Police Crime Statistics 2008*. Accessed on May 18, 2016. [Online]. Available: [http://www.bka.de/nn_194638/sid_73974E4F691258D85603C3F55F3BCC72/SharedDocs/Downloads/EN/Publications/Police meStatistics/2002Bis2013/pks2008__englisch.html?__nnn=true](http://www.bka.de/nn_194638/sid_73974E4F691258D85603C3F55F3BCC72/SharedDocs/Downloads/EN/Publications/Police%20meStatistics/2002Bis2013/pks2008__englisch.html?__nnn=true)
- [6] *2015 US State of Cybercrime Survey*, PwC, London, U.K., Jul. 2015, accessed on May 18, 2016. [Online]. Available: <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/uscybercrime-survey-2015.html>

[7] R. Anderson *et al.*, “Measuring the cost of cybercrime,” in *The Economics of Information Security and Privacy*. Berlin, Germany: Springer, 2013, pp. 265–300.

[8] L. D. Roberts, *Cyber-Victimisation in Australia: Extent, Impact on Individuals and Responses*. Hobart, TAS, Australia: Tasmanian Inst. Law Enforcement Stud., 2008.

[9] K. M. Finklea and C. A. Theohary, *Cybercrime: Conceptual Issues for Congress and U.S. Law*

Enforcement. Washington, DC, USA: Congressional Res. Service, 2012.

[10] Council of Europe. (Nov. 23, 2001). *Convention on Cybercrime*. Accessed on Apr. 27, 2016. [Online]. Available: <http://www.coe.int/el/web/conventions/full-list/-/conventions/treaty/185>

