SECURITY SYSTEMS

A Project

by

HET PATEL
2023
DIPLOMA [IT]
GOVERNMENT POLYTECHNIC AHMEDABAD

Submitted to the CSRBOX team
as the final project deliverable for
IBM SkillsBuild Data Analytics Internship

SkillsBuild

CSRBOX

Project Summary

Security and protection system, any of various means or devices designed to guard persons and property against a broad range of hazards, including crime, fire, accidents, espionage, sabotage, subversion, and attack. Most security and protection systems emphasize certain hazards more than others. In a retail store, for example, the principal security concerns are shoplifting and employee dishonesty (e.g., pilferage, embezzlement, and fraud). A typical set of categories to be protected includes the personal safety of people in the organization, such as employees, customers, or residents; tangible property, such as the plant, equipment, finished products, cash, and securities; and intangible property, such as highly classified national-security information or "proprietary" information (e.g., trade secrets) of private organizations. An important distinction between a security and protection system and public services such as police and fire departments is that the former employs means that emphasize passive and preventive measures. Security systems are found in a wide variety of organizations, ranging from government agencies and industrial plants to apartment buildings and schools. Sufficiently large organizations may have their own proprietary security systems or may purchase security services by contract from specialized security organizations. The objective of system security is the protection of information and property from theft, corruption and other types of damage, while allowing the information and property to remain accessible and productive. System security includes the development and implementation of security countermeasures. All home security systems work on the same basic principle of securing entry points, like doors and windows, as well as interior space containing valuables like art, computers, guns, and coin collections. Regardless of the size of your home, or the number of doors and windows or interior rooms a homeowner decides to protect, the only real difference is in the number of security components deployed throughout the home and monitored by the control panel.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

The study will be conducted to demonstrate the effective classification of SECURITY SYSTEMS. Objectives that state the desired level of protection are Protection Objectives. These objectives often define the target security level. Also, the means to achieve that level. Objectives that state what services need. It is to give to the business is Service Objectives. Service objectives may focus on availability and confidentiality. Also, integrity and reliability add other service attributes. A home security system offers protection for your loved ones and property, as well as peace of mind. While property crime has dropped more than 6% – the sixteenth year in a row it has declined, according to FBI Today's home security systems also can act as a hub for home automation systems, adding convenience and energy savings, which makes their cost more attractive. Gone are the days spent in worrying about home and any asset security. Now, with only a few smart IoT devices, you can ensure all-around home security. It's time to become intelligent citizens and adopt IoT. Not just home security, it's also a giant step towards home automation. working with a socio-technical view on information systems security is a challenge. Existing studies show that a great number of security incidents are caused by trusted personnel within organizations due to the tension between the design of information systems security policies, guidelines, rules and tools, and how they actually are used. This paper describes a framework for analysing users' compliance with the creator's intentions that underlie an information systems security design. This framework is anchored in the concept of rationality, and the result can be used, for example, to facilitate the task of analyzing security incidents, to verify existing information systems security approaches, and to match information systems security approaches with organizational requirements.

Topic Brief

Most security and protection systems emphasize certain hazards more than others. In a retail store, for example, the principal security concerns are shoplifting and employee dishonesty (e.g., pilferage, embezzlement, and fraud). A typical set of categories to be protected includes the personal safety of people in the organization, such as employees, customers, or residents; tangible property, such as the plant, equipment, finished products, cash, and securities; and intangible property, such as highly classified national-security information or "proprietary" information (e.g., trade secrets) of private organizations. An important distinction between a security and protection system and public services such as police and fire departments is that the former employs means that emphasize passive and preventive measures. Security systems are found in a wide variety of organizations, ranging from government agencies and industrial plants to apartment buildings and schools. Sufficiently large organizations may have their own proprietary security systems or may purchase security services by contract from specialized security organizations. The objective of system security is the protection of information and property from theft, corruption and other types of damage, while allowing the information and property to remain accessible and productive. System security includes the development and implementation of security countermeasures. All home security systems work on the same basic principle of securing entry points, like doors and windows, as well as interior space containing valuables like art, computers, guns, and coin collections. Regardless of the size of your home, or the number of doors and windows or interior rooms a homeowner decides to protect, the only real difference is in the number of security components deployed throughout the home and monitored by the control panel.

.

Purpose of the Study

- The security system's purpose is often misunderstood. Some seem to think that an alarm system must catch a criminal. Really, that's not its purpose. Sometimes they help lead to an arrest, but the main roles of a security system are as follows.
- We want a burglary to never occur. There is no larger deterrent a person can add to their home or business than a security system. Many studies have proved this. The most recent is the "Rutgers Study," where they tracked the location of every alarm system and burglary for more than 5 years in Newark, NJ. The study showed that alarm systems are not only extremely effective at being a deterrent to the home or business, but they even reduce crime in surrounding areas. The higher the concentration of alarm systems, the further out the deterrence extends.

- Most security systems have a high decibel siren. This not only lets the home or business owner know that something has happened, but it also lets the intruder know that something has triggered the alarm. This increases the level of fear of apprehension or arrest.

- Someone is going to know about what is going on. Usually it's a well-trained, sworn law enforcement official. If needed, someone will check on the home, business, or person where the alarm was triggered. This saves life every year. The easiest to document are the alarm systems that have a monitored heat detector.
- Occasionally intrusion alarms are silent, or without a siren. When that is the case, the capture rate increases. But this means that the first three functions of an alarm system are sacrificed. There is no deterring, warning, or loss prevention. It's better for home
- Motion sensor is used to detect the movment of any accidental activity and alerts user based on that activity.

Hypotheses

hypotheses

Criminal systems work with ***presumption of innocence***. The defendant is always innocent unless proven guilty. It is the job of the prosecutor to prove the defendant as 'guilty' by providing evidence. This helps us define our hypotheses, as follows.

Null hypothesis (H0)

The defendant is innocent of murder or theft charge.

Alternative hypothesis (H1)

The defendant is guilty of a murder or theft charge.

While making a quantitative statistical assessment, researchers assume the role of prosecutors. It may seem counterintuitive, but researchers often create null hypothesis in hopes of being able to reject it.

Significance level

Next step is to come up with a threshold at which we would reject our null hypothesis. This threshold is also known as a significance level. What does significance level exactly mean?

The end result of Hypothesis testing is, we either reject the null hypothesis or fail to reject it. (Note that we never claim that H1 is true, but more on that later). The decision of rejecting null hypothesis is based on the strength of evidences, with a degree of uncertainty of course. We acknowledge that there is always a likelihood of observing as strong as the evidences that we have, just out of pure chance. The question we need to ask here is, *What is the level of risk we are prepared to undertake while making this decision*?

Significance level is the threshold at which we cap our risk of falsely rejecting a null hypothesis.

Most common significance levels that researchers use are 0.1, 0.05 or 0.01 (or 10%, 5% and 1% respectively). In our case, let us suppose the judge fixes a significance level of 0.05. This means that the judge is prepared to take a risk of 5% in passing a judgement against the defendant, when he is actually innocent. If you've heard the phrase 'guilty beyond reasonable doubt', the judge is willing to have at least 95% confidence when he passes a judgement against the defendant.

Note: I am using arbitrary numbers to explain how quantitative assessments are performed with Statistical hypothesis testing. In reality, it is impossible to assign a fixed number to confidence levels for courtroom proceedings.

p-value

Let us examine the evidences presented by the prosecutor.

- DNA of defendant found in fingernails of victim, in spite of them never having crossed their paths before
- Criminal history of defendant — several petty crimes

- One serious conviction of residential burglary
- Homeless, mental health disorder and strong alcohol addiction

I do not have a degree in law, but to me it appears that the evidences presented are not strong enough to prove the defendant guilty. Even the presence of defendant's DNA on victim's body can have a logical alternative explanation (if that's unsettling to you, please go ahead and read this). If we have to assign a number, let's say the combined probability of having all these evidences out of pure chance is 0.12. This is known as p-value which is the specific probability of getting results as extreme as we have if the null hypothesis were true.

p-value is the specific probability of getting results as extreme as we have, if the null hypothesis were true.

The p-value in our case is way above the significance level of 0.05 decided beforehand and therefore, we fail to reject the null hypothesis. As a matter of semantics, we have not proved null hypothesis to be true. We are not claiming that the defendant is innocent but based on the evidences presented, we are not persuaded otherwise.

Significance of the Study

1.
I collected data of crimes done throughout years,I now analyze data on basis of years
-Analyze data which shows how much crimes per year is done how much murders,rape,robbery etc is done.
-Analyze sex of people out of total number of persons
-Analyze ages of peoples
-Analyze areas where this crimes happens.

2.

1. HOME SECURITY SYSTEMS ARE DESIGNED TO BE A DETERRENT.

- We want a burglary to never occur. There is no larger deterrent a person can add to their home or business than a security system. Many studies have proved this. The most recent is the "Rutgers Study," where they tracked the location of every alarm system and burglary for more than 5 years in Newark, NJ. The study showed that alarm systems are not only extremely effective at being a deterrent to the home or business, but they even reduce crime in surrounding areas. The higher the concentration of alarm systems, the further out the deterrence extends.

2. SECURITY SYSTEMS SUMMON HELP.

- Someone is going to know about what is going on. Usually it's a well-trained, sworn law enforcement official. If needed, someone will check on the home, business, or person where the alarm was triggered. This saves life every year. The easiest to document are the alarm systems that have a monitored heat detector.
- Occasionally intrusion alarms are silent, or without a siren. When that is the case, the capture rate increases. But this means that the first three functions of an alarm system are sacrificed. There is no deterring, warning, or loss prevention. It's better for home and business owners to use all four functions.

3.MOTION SENSOR

- Motion sensor is used to detect the movment of any accidental activity and alerts user based on that activity.

3.

- Protects valuables
- Deters crime
- Allows remote access to your home
- Lowers homeowner’s insurance
- Notifies you of fire or gas problems
- Helps keep tabs on kids
- Improves electricity management
- Makes room for peace of mind

Method of Procedure

- Data and analytics is especially important to modern businesses as it can improve decision outcomes for all types of decisions (macro, micro, real-time, cyclical, strategic, tactical and operational). At the same time, D&A can unearth new questions and innovative solutions to questions — and opportunities — that business leaders had not even considered.

- Progressive organizations use data in many ways and must often rely on data from outside their boundary of control for making smarter business decisions.

- Data and analytics is also a **catalyst for digital strategy** and transformation as it enables faster, more accurate and more relevant decisions in complex and fast–changing business contexts.

- Decisions are made by individuals (e.g., when a sales prospect is considering whether to buy a product or service) and by organizational teams (e.g., when determining how best to serve a client or citizen). Digital strategy is, therefore, as much about asking smarter questions via data to improve the outcome and impact of those decisions.

- Data-driven decision making means using data to work out how to improve decision making processes. This leads to the idea of a **decision model**, which can include **prescriptive** analytical techniques that generate outputs that are able to specify which actions to take. Other analytical models are **descriptive**, **diagnostic** or **predictive** (also see **"What are core analytics techniques?**") and these can help with other kinds of decisions.

- Notably, decisions drive action but may equally determine when not to act.

Collection of Data

- I researched about topic and gather information about it and searched the good website for data set.
- I found Kaggle.com so I have searched it and used it.

Treatment of Data

- 'Statistical treatment' is when you apply a statistical method to a data set to draw meaning from it. Statistical treatment can be either descriptive statistics, which describes the relationship between variables in a population, or inferential statistics, which tests a hypothesis by making inferences from the collected data.

- Statistical treatment of data is when you apply some form of statistical method to a data set to transform it from a group of meaningless numbers into meaningful output.
- Statistical treatment of data involves the use of statistical methods such as:
- mean,
- mode,
- median,
- regression,
- conditional probability,
- sampling,
- standard deviation and
- distribution range.

- These statistical methods allow us to investigate the statistical relationships between the data and identify possible errors in the study.
- In addition to being able to identify trends, statistical treatment also allows us to organise and process our data in the first place. This is because when carrying out statistical analysis of our data, it is generally more useful to draw several conclusions for each subgroup within our population than to draw a single, more general conclusion for the whole population. However, to do this, we need to be able to classify the population into different subgroups so that we can later break down our data in the same way before analysing it

- I also treated data and cleaned it.
- We use median to replace null values etc.
- Also applied categorial variable method

Data Source

- https://www.forbes.com/home-improvement/home-security/what-is-a-home-security-system/
- information-security-today.com
- www.usnews.com
- EXPLORING THE CONCEPTUAL STRUCTURE OF SECURITY RATIONALE (diva-portal.org)
- www.britannica.com
- Security and protection system - Physical security. | Britannica
- (safewise.com)
- (zionssecurity.com)
- https://www.safewise.com
- www.kaggle.com

Limitations

-It does not detects fire accurately

-Motion sensor detects only 180 degree picture not 360 degree.

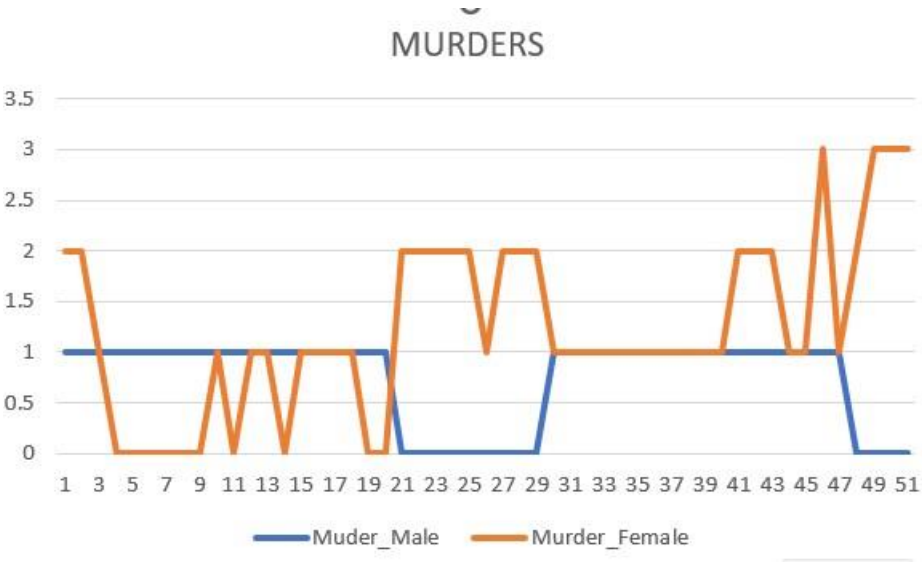
-It not detects all objects.

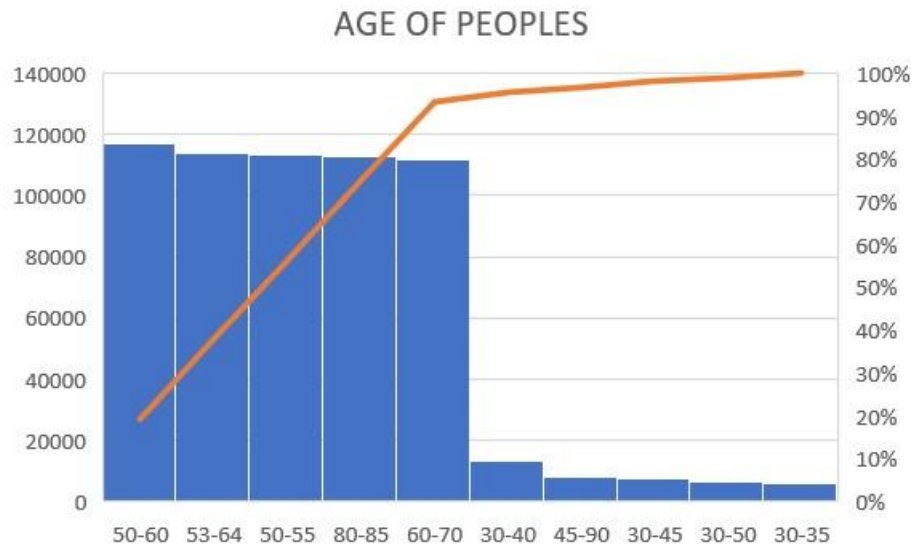
Assumptions

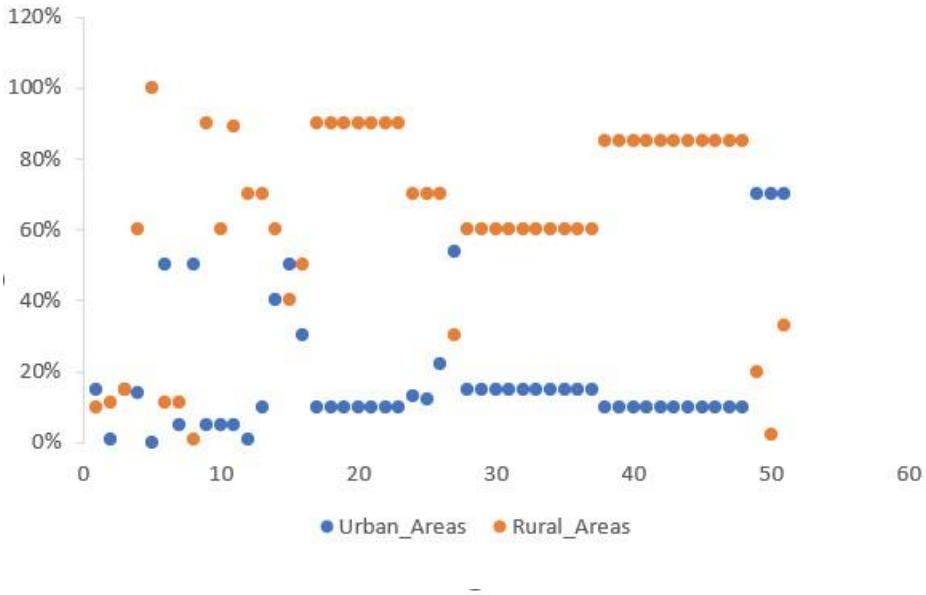
1. Protects valuables
2. Deters crime
3. Allows remote access to your home
4. Lowers homeowner's insurance
5. Notifies you of fire or gas problems
6. Helps keep tabs on kids
7. Improves electricity management
8. Makes room for peace of mind

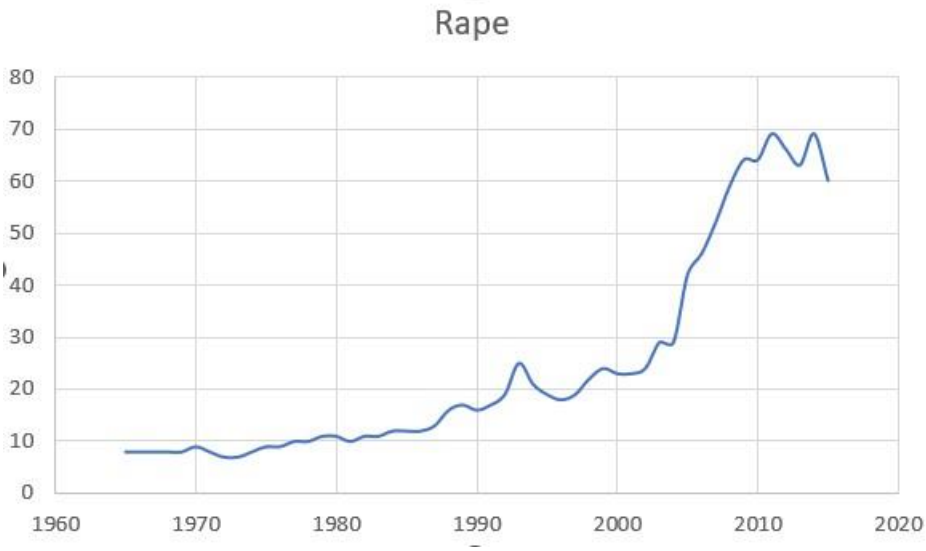
Chapter 2

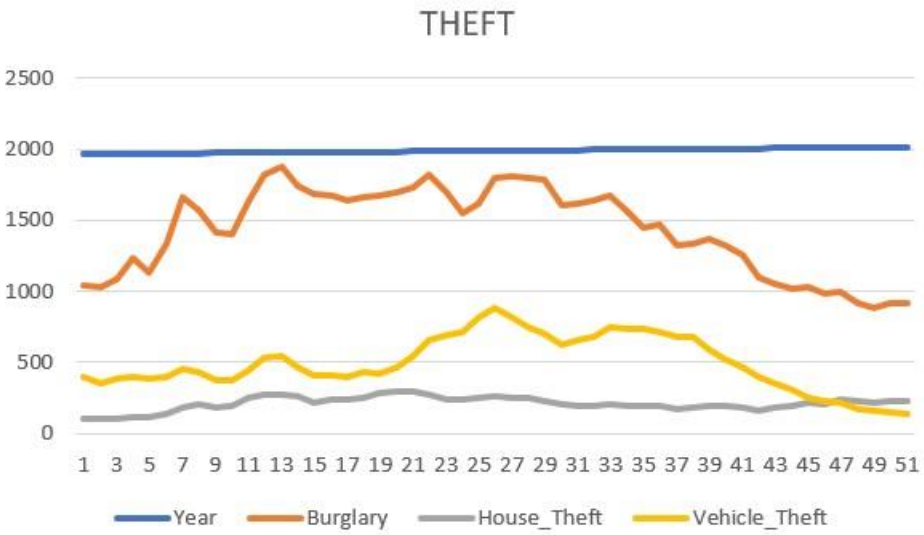
Analysis

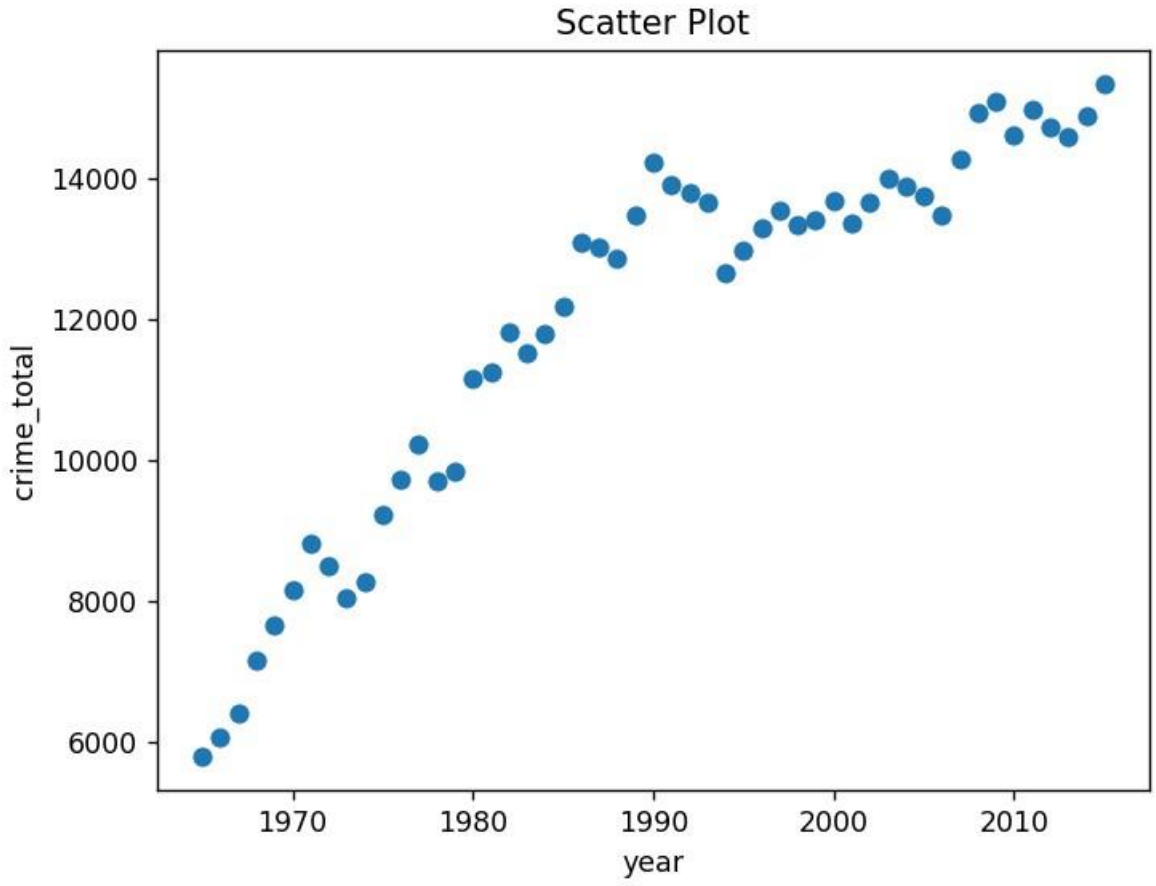


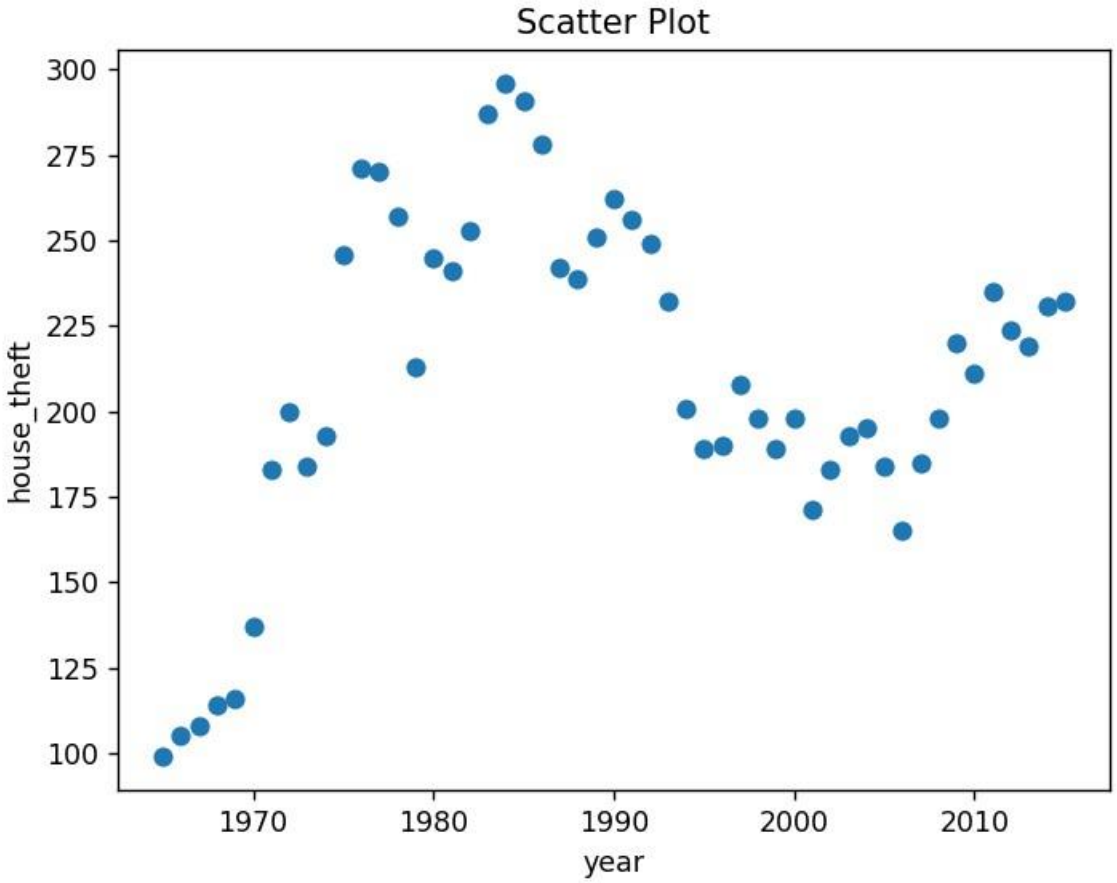


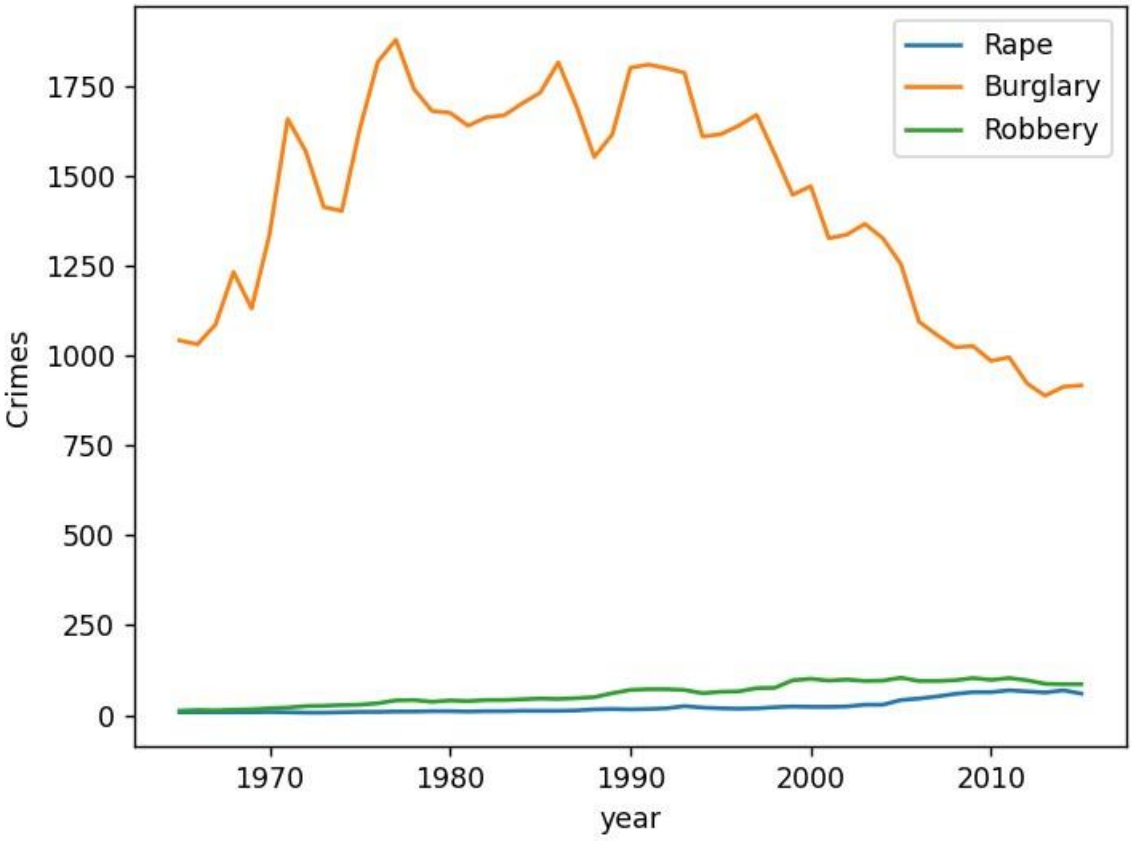

120%
100%
80%
60%
40%
20%
0%
0
10
20
30
40
50
60
Urban_Areas
Rural_Areas


Rape
80
70
60
50
40
30
20
10
0
1960
1970
1980
1990
2000
2010
2020


THEFT
2500
2000
1500
1000
500
0
1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51
Year
Burglary
House_Theft
Vehicle_Theft


Scatter Plot
crime_total
14000
12000
10000
8000
6000
1970
1980
1990
2000
2010
year


Scatter Plot
house_theft
year
300
275
250
225
200
175
150
125
100
1970
1980
1990
2000
2010


Rape
Burglary
Robbery
Crimes
1750
1500
1250
1000
750
500
250
0
1970
1980
1990
2000
2010
year

-There are a lot of elements to think about when it comes to security systems and that includes how the security system could benefit you and your family. Here are a few reasons how that is true. Installing, arming, disarming, paying monthly fees, and dealing with false alarms are all things that are tied to monitored security systems which may cause you to wonder if home security systems are worth the inherent hassle. This is a good question to ask as you consider how you can best protect your valuables and your loved ones. In this project we are preparing an IOT based system model of security, we are using so many devices and sensors like PIR sensor, light sensor etc. We are making a website using latest technologies for user to monitor and maintain their system (on hand service), anywhere & anytime. Security system is made of sensors which detects the activity and sends details and alert to system of user.

- Deters crime
- Allows remote access to your home
- Notifies you of fire or gas problems
- Helps keep tabs on kids
- Improves electricity management
- Makes room for peace of mind

3. SUMMARY OF THE STUDY AND THE FINDINGS, CONCLUSIONS, ESTIMATIONS, PREDICTIONS, FUTURE COURSE OF ACTION

REFERENCES

- https://www.forbes.com/home-improvement/home-security/what-is-a-home-security-system/
- information-security-today.com
- www.usnews.com
- EXPLORING THE CONCEPTUAL STRUCTURE OF SECURITY RATIONALE (diva-portal.org)
- www.britannica.com
- Security and protection system - Physical security. | Britannica
- (safewise.com)
- (zionssecurity.com)
- https://www.safewise.com
- www.kaggle.com

APPENDICES

Code-

Object detection model

```
import cv2
import numpy as np

# Load YOLO Algorithm
net = cv2.dnn.readNet("yolov3.weights", "yolov3.cfg")

# To load all objects that have to be detected
classes = []
with open("coco.names", "r") as f:
    read = f.readlines()
for i in range(len(read)):
    classes.append(read[i].strip("\n"))

# Defining layer names
layer_names = net.getLayerNames()
output_layers = []
for i in net.getUnconnectedOutLayers():
    output_layers.append(layer_names[i - 1])

# Loading the Image
img = cv2.imread("Road.jpg")

height, width, channels = img.shape

# Extracting features to detect objects
blob = cv2.dnn.blobFromImage(img, 0.00392, (416, 416), (0, 0, 0), True,
crop=False)
# Inverting blue with red
# bgr->rgb


# We need to pass the img_blob to the algorithm
net.setInput(blob)
outs = net.forward(output_layers)
# print(outs)
```

```
# Displaying informations on the screen
class_ids = []
confidences = []
boxes = []
for output in outs:
    for detection in output:
        # Detecting confidence in 3 steps
        scores = detection[5:]  # 1
        class_id = np.argmax(scores)  # 2
        confidence = scores[class_id]  # 3

        if confidence > 0.5:  # Means if the object is detected
            center_x = int(detection[0] * width)
            center_y = int(detection[1] * height)
            w = int(detection[2] * width)
            h = int(detection[3] * height)

            # Drawing a rectangle
            x = int(center_x - w / 2)  # top left value
            y = int(center_y - h / 2)  # top left value

            boxes.append([x, y, w, h])
            confidences.append(float(confidence))
            class_ids.append(class_id)
        # cv2.rectangle(img,(x,y),(x+w,y+h),(0,255,0),2)

# Removing Double Boxes
indexes = cv2.dnn.NMSBoxes(boxes, confidences, 0.3, 0.4)

for i in range(len(boxes)):
    if i in indexes:
        x, y, w, h = boxes[i]
        label = classes[class_ids[i]]  # name of the objects
        cv2.rectangle(img, (x, y), (x + w, y + h), (0, 255, 0), 2)
        cv2.putText(img, label, (x, y), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0,
255), 2)

cv2.imshow("Output", img)
cv2.waitKey(0)
cv2.destroyAllWindows()
```

```
[net]
# Testing
# batch=1
# subdivisions=1
# Training
batch=64
subdivisions=16
width=608
height=608
channels=3
momentum=0.9
decay=0.0005
angle=0
saturation = 1.5
```

```
exposure = 1.5
hue=.1

learning_rate=0.001
burn_in=1000
max_batches = 500200
policy=steps
steps=400000,450000
scales=.1,.1

[convolutional]
batch_normalize=1
filters=32
size=3
stride=1
pad=1
activation=leaky

# Downsample

[convolutional]
batch_normalize=1
filters=64
size=3
stride=2
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=32
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=64
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

# Downsample

[convolutional]
batch_normalize=1
filters=128
size=3
stride=2
pad=1
activation=leaky
```

```
[convolutional]
batch_normalize=1
filters=64
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=128
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=64
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=128
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

# Downsample

[convolutional]
batch_normalize=1
filters=256
size=3
stride=2
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
```

```
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=128
```

```
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear


[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear
```

```
[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

# Downsample

[convolutional]
batch_normalize=1
filters=512
size=3
stride=2
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
```

```
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear


[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear


[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear
```

```
[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear


[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=3
stride=1
pad=1
activation=leaky
```

```
[shortcut]
from=-3
activation=linear


[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

# Downsample

[convolutional]
batch_normalize=1
filters=1024
size=3
stride=2
pad=1
activation=leaky

[convolutional]
batch_normalize=1
```

```
filters=512
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=1024
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=512
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=1024
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

[convolutional]
batch_normalize=1
filters=512
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=1024
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear
```

```
[convolutional]
batch_normalize=1
filters=512
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
filters=1024
size=3
stride=1
pad=1
activation=leaky

[shortcut]
from=-3
activation=linear

######################

[convolutional]
batch_normalize=1
filters=512
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=1024
activation=leaky

[convolutional]
batch_normalize=1
filters=512
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=1024
activation=leaky

[convolutional]
batch_normalize=1
```

```
filters=512
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=1024
activation=leaky

[convolutional]
size=1
stride=1
pad=1
filters=255
activation=linear


[yolo]
mask = 6,7,8
anchors = 10,13,  16,30,  33,23,  30,61,  62,45,  59,119,  116,90,  156,198,
373,326
classes=80
num=9
jitter=.3
ignore_thresh = .7
truth_thresh = 1
random=1


[route]
layers = -4

[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[upsample]
stride=2

[route]
layers = -1, 61



[convolutional]
batch_normalize=1
filters=256
size=1
```

```
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=512
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=512
activation=leaky

[convolutional]
batch_normalize=1
filters=256
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=512
activation=leaky

[convolutional]
size=1
stride=1
pad=1
filters=255
activation=linear


[yolo]
mask = 3,4,5
anchors = 10,13,  16,30,  33,23,  30,61,  62,45,  59,119,  116,90,  156,198,
373,326
classes=80
```

```
num=9
jitter=.3
ignore_thresh = .7
truth_thresh = 1
random=1



[route]
layers = -4

[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[upsample]
stride=2

[route]
layers = -1, 36



[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=256
activation=leaky

[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=256
```

```
activation=leaky

[convolutional]
batch_normalize=1
filters=128
size=1
stride=1
pad=1
activation=leaky

[convolutional]
batch_normalize=1
size=3
stride=1
pad=1
filters=256
activation=leaky

[convolutional]
size=1
stride=1
pad=1
filters=255
activation=linear


[yolo]
mask = 0,1,2
anchors = 10,13,  16,30,  33,23,  30,61,  62,45,  59,119,  116,90,  156,198,
373,326
classes=80
num=9
jitter=.3
ignore_thresh = .7
truth_thresh = 1
random=1
```

Yolov3.cfg

```
person
bicycle
car
motorbike
aeroplane
bus
train
truck
boat
traffic light
fire hydrant
stop sign
parking meter
bench
bird
cat
```

```
dog
horse
sheep
cow
elephant
bear
zebra
giraffe
backpack
umbrella
handbag
tie
suitcase
frisbee
skis
snowboard
sports ball
kite
baseball bat
baseball glove
skateboard
surfboard
tennis racket
bottle
wine glass
cup
fork
knife
spoon
bowl
banana
apple
sandwich
orange
broccoli
carrot
hot dog
pizza
donut
cake
chair
sofa
pottedplant
bed
diningtable
toilet
tvmonitor
laptop
mouse
remote
keyboard
cell phone
microwave
oven
toaster
sink
refrigerator
```

```
book
clock
vase
scissors
teddy bear
hair drier
toothbrush
```

coco.names

```
import cv2

cap = cv2.VideoCapture(0)

ret1, frame1 = cap.read()
gray1 = cv2.cvtColor(frame1, cv2.COLOR_BGR2GRAY)
gray1 = cv2.GaussianBlur(gray1, (21, 21), 0)
cv2.imshow('window', frame1)

while (True):
    ret2, frame2 = cap.read()
    gray2 = cv2.cvtColor(frame2, cv2.COLOR_BGR2GRAY)
    gray2 = cv2.GaussianBlur(gray2, (21, 21), 0)

    deltaframe = cv2.absdiff(gray1, gray2)
    cv2.imshow('delta', deltaframe)
    threshold = cv2.threshold(deltaframe, 25, 255, cv2.THRESH_BINARY)[1]
    threshold = cv2.dilate(threshold, None)
    cv2.imshow('threshold', threshold)
    countour, heirarchy = cv2.findContours(threshold, cv2.RETR_EXTERNAL,
cv2.CHAIN_APPROX_SIMPLE)
    for i in countour:
        if cv2.contourArea(i) < 50:
            continue

        (x, y, w, h) = cv2.boundingRect(i)
        cv2.rectangle(frame2, (x, y), (x + w, y + h), (255, 0, 0), 2)

    cv2.imshow('window', frame2)

    if cv2.waitKey(20) == ord('q'):
        break
cap.release()
cv2.destroyAllWindows()
```

motion.py

PLACEMENT AND LABELING OF TABLES AND FIGURES

TABLE 1
Increasing number of thefts.

Burglary	House_Thef	Vehicle_Theft	Yea
1042	99	397	1965
1031	105	350	1966
1086	108	384	1967
1232	114	396	1968
1131	116	384	1969
1338	137	402	1970
1658	183	457	1971
1568	200	426	1972
1413	184	380	1973
1402	193	372	1974
1631	246	448	1975
1817	271	532	1976
1878	270	539	1977
1741	257	469	1978
1680	213	412	1979
1675	245	413	1980
1639	241	393	1981
1662	253	429	1982
1668	287	419	

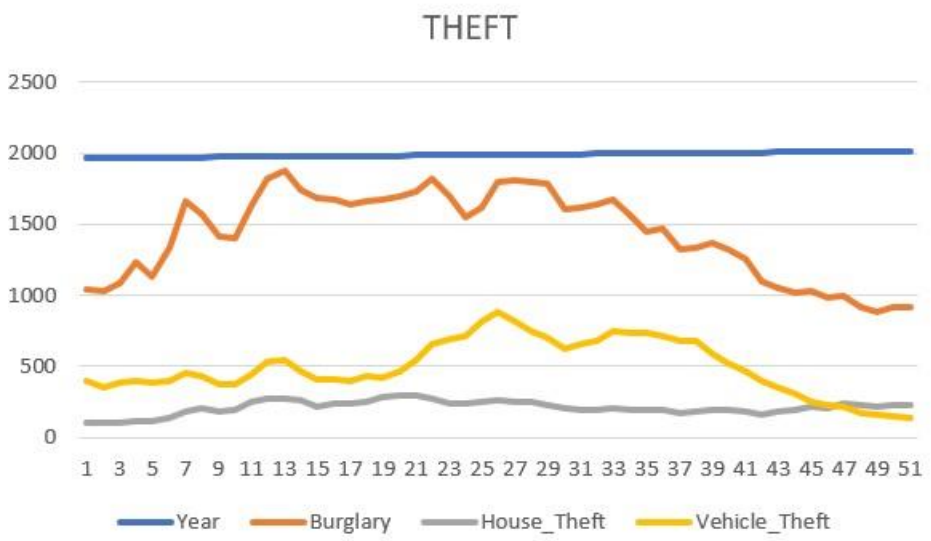


TABLE 2

Increasing number of murders.

Muder_Male	Murder_Female
1	2
1	2
1	1
1	0
1	0
1	0
1	0
1	0
1	0
1	1
1	0
1	1
1	1
1	0
1	1
1	1
1	1
1	1
1	0
1	0
0	2

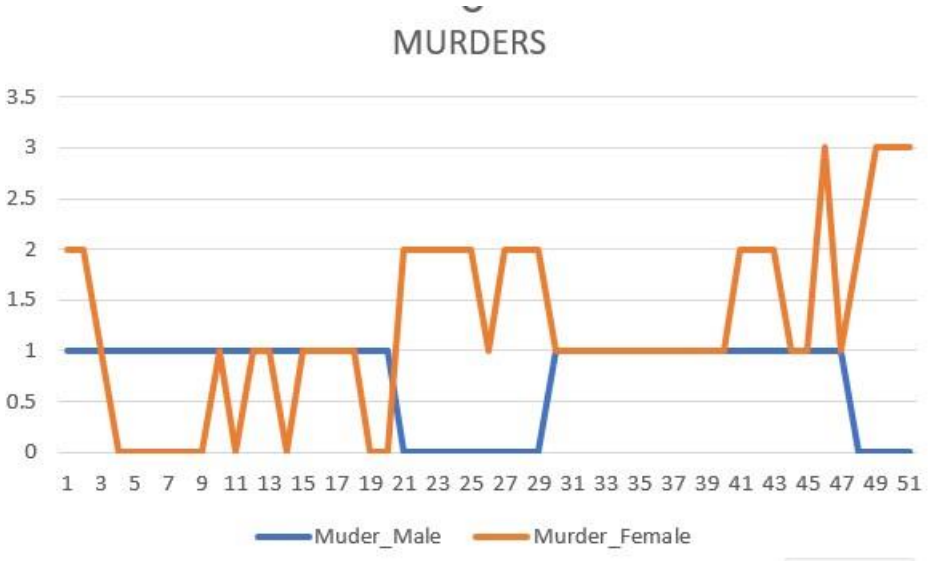


TABLE -3:
Crime areas.

Urban_Areas	Rural_Areas
15%	10%
1%	11%
15%	15%
14%	60%
0%	100%
50%	11%
5%	11%
50%	1%
5%	90%
5%	60%
5%	89%
1%	70%
10%	70%
40%	60%
50%	40%
30%	50%
10%	90%
10%	90%
10%	90%
10%	90%
10%	90%
10%	90%
10%	90%
13%	70%

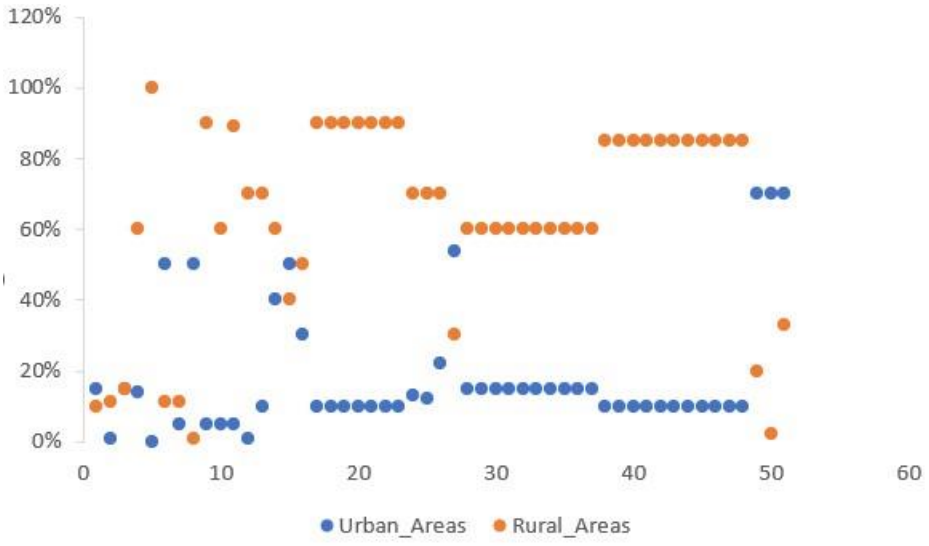
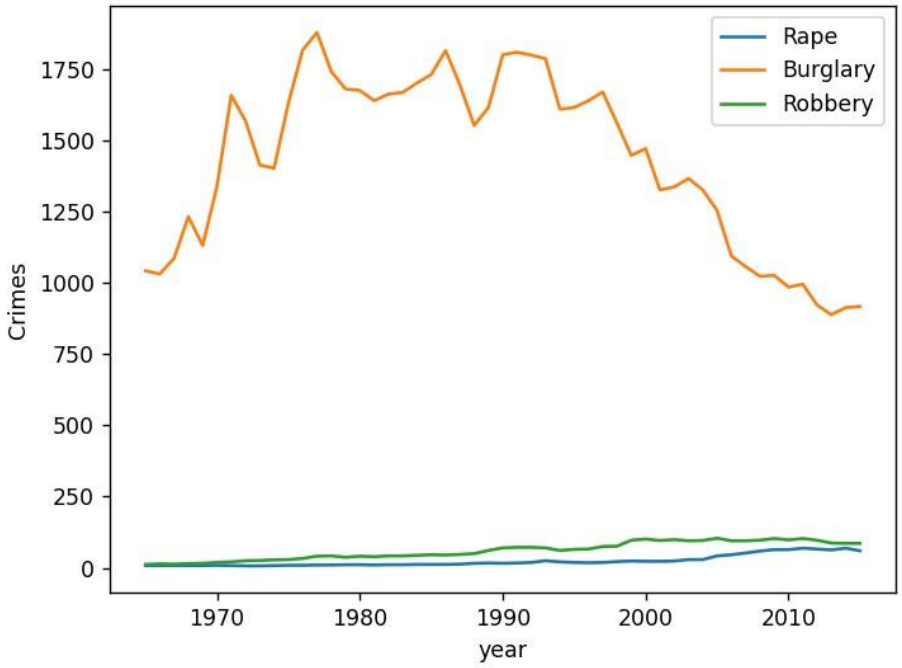


TABLE 4
Increasing number of rapes,bulgary,robbery.

Rape	Burglary	Robbery
8	1042	12
8	1031	14
8	1086	13
8	1232	15
8	1131	16
9	1338	19
8	1658	21
7	1568	25
7	1413	26
8	1402	28
9	1631	29
9	1817	33
10	1878	41
10	1741	42
11	1680	37
11	1675	41


Rape
Burglary
Robbery
Crimes
1750
1500
1250
1000
750
500
250
0
1970
1980
1990
2000
2010
year