DEVELOPMENT OF A PREDICTIVE MODEL FOR CRIME INVESTIGATION AND EMERGENCY RESPONSE SYSTEM

BY

BUKI OLADELE ROBERT (B.Sc.)
2011473338

A THESIS SUBMITED TO THE
POSTGRADUATE SCHOOL
FEDERAL UNIVERSITY OF TECHNOLOGY, OWERRI

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE (M.Sc.) DEGREE IN INFORMATION MANAGEMENT TECHNOLOGY

MAY, 2024

CERTIFICATION

This is to certify that this research work titled **"DEVELOPMENT OF A PREDICTIVE MODEL FOR CRIME INVESTIGATION AND EMERGENCY RESPONSE SYSTEM"** was carried out by **BUKI, OLADELE ROBERT** with registration number **2011473338** in partial fulfillment for the requirement of the award of degree of Master of Science (M.Sc) in Information Management Technology.

Engr. Dr. O. C. Nwokonkwo
Principal Supervisor

22-05-2024
Date

Dr. A. M. John-Otumu
Co-Supervisor

22-05-2024
Date

Dr. A. I. Otuonye
Head of Department

Date

Prof. (Mrs.) U. F. Eze
Dean, SICT

Date

Prof. (Mrs.) J. N. Nwosu
Dean, PG School

Date

Prof. Awodele Oludele
External Examiner

23/05/2024
Date

DEDICATION

I dedicate this research work to Almighty God who by His grace has seen me through the entire period of this study.

ACKNOWLEDGEMENTS

I am deeply grateful to many individuals who have been crucial to this research. First, I extend my heartfelt thanks to my principal supervisor, Engr. Dr. O. C. Nwokonkwo, and co-supervisor, Dr. A. M. John-Otumu, for their unwavering support and guidance despite their numerous responsibilities.

I am also thankful for the ongoing support and encouragement from the Head of the Department, Dr. A. I. Otuonye, and the PG Coordinator, Dr. C. Etus.

My sincere gratitude goes to the Dean (SICT), Prof. (Mrs.) U. F. Eze, whose motherly support was vital for completing this work.

I appreciate the guidance of all my esteemed lecturers, including Prof. B. Asiegbu, Dr. C. O. Ikerionwu, Engr. Dr. M. E. Nwanga, Dr. N. Ekedebe, and Engr. Dr. E. C. Amadi, whose advice was instrumental throughout my studies.

I am also grateful for the constant support and care from my parents, Chief and Mrs. W. A. O. Buki, whose contributions have been invaluable. Special thanks to Ugochukwu Chinaka for his significant assistance in this journey.

Lastly, I thank the Almighty for His endless love, kindness, and protection throughout my time at this esteemed institution.

.

TABLE OF CONTENTS

Title page		i
Copyright Page		ii
Certification		iii
Dedication		iv
Acknowledgment		v
Abstract		vi
CHAPTER 1: INTRODUCTION		**1**
1.1	Background Information	1
1.2	Problem statement	3
1.3	Objective	3
1.4	Research objectives	5
1.5	Justification of the study	5
1.6	Scope of the study	6
CHAPTER 2: LITERATURE REVIEW		**7**
2.1	Conceptual framework	7
2.1.1	Historical background of emergency management in Nigeria	7
2.1.2	Organizational structure of emergency management	8
2.1.3	Challenge and opportunities confronting Nigeria's emergency management system	8
2.1.4	Emergency management	11
2.1.5	Conceptualization of emergency management organization	12
2.1.6	Time-critical response	13
2.1.7	Information technology with emergency management	14
2.1.8	The impact of information technology on emergency situation	15
2.1.9	Information technology and job design in emergency system	16
2.1.10	Concepts of crime investigation using information technology	18

2.2 Theoretical framework 18
2.2.1 Crime Pattern Theory 19
2.2.2 Social Learning Theory 21
2.2.3 Technology Acceptance Theory (TAM) 23
2.2.4 Prediction Theory 23
2.2.5 No Free Lunch Theory 24
2.3 Empirical Framework 25
2.4 Summary of related literature 29
2.4.1 Gap Analysis 32
CHAPTER 3: RESEARCH METHODOLOGY 33
3.1 Analysis of existing crime investigation and emergency response system 33
3.1.1 Problems of existing system 34
3.2 The proposed system 36
3.2.1 Data gathering 37
3.2.2 System design 38
3.2.3 Algorithms adopted 44
3.3 Data modelling 49
3.3.1 Data dictionary 49
3.3.2 Class diagram 51
3.4 System requirements 52
3.4.1 Functional requirements 52
3.4.2 Non-functional requirements 52
3.5 System implementation 53
3.5.1 Computer / platform configurations 53
3.6 Software methodology 54
3.6.1 Software methodology adopted 54
3.6.2 Advantages of using prototyping SDLC 56

CHAPTER 4: RESULTS AND DISCUSSION **57**

4.1 Result and visualization from the dataset utilized 57

4.1.1 Crime results 58

4.2 Model's performance 60

4.2.1 Receiver's Operator Characteristics (ROC) 60

4.2.2 Performance evaluation 61

4.3 Developed User's Interface/Dashboard 66

CHAPTER 5: CONCLUTION AND RECOMMENDATION **70**

5.1 Conclusion 70

5.2 Recommendations 71

5.3 Contribution to Knowledge 73

5.4 Future Research Works 74

REFERENCES **76**

APPENDIX A **80**

LIST OF TABLES

Tables	Title	Page
2.1	Summary of related works	30
3.1	Design specification for the ANN	47
3.2	Data dictionary	50
3.3	Functional requirements	52
3.4	Non-functional requirements	53
3.5	Computer setup configurations	54

LIST OF FIGURES

Figures	Title	Page
2.1	Illustration of Crime Pattern Theory	21
2.2	Illustration of Social Learning Theory	22
2.3	Illustration of Technology Acceptance Theory	23
2.4	Illustration of Predictive Theory	24
3.1	Proposed system architecture	39
3.2	Proposed system workflow process	41
3.3	Civil intelligence and crime analysis workflow diagram	43
3.4	Proposed emergency response workflow system diagram	43
3.5	Multi-Linear Regression Algorithm	44
3.6	K-Nearest Neighbor Algorithm	45
3.7	Feed Forward Neural Network Algorithm	46
3.8	Proposed system class diagram	51
3.9	Prototyping software methodology life cycle diagram	55
4.1	Graphical representation of years Vs No of unsolved crimes	57
4.2	Graphical representation of months Vs. No of Unsolved crimes	58
4.3	Graphical representation of Weapons Vs. No of unsolved crimes	59
4.4	Graphical representation of investigation office Vs unsolved crimes	59
4.5	Graphical representation of ROC curve	60
4.6	Graphical representation of prediction results based on Age	62
4.7	Graphical representation of predictions results based on relationship	63
4.8	Graphical representation of prediction loss analysis of perpetrators' gender	64
4.9	Graphical representation of of performance analysis of Neural Network	65
4.10	Graphical representation of comparison evaluation	66

4.11	Proposed system Login Page	67
4.12	Proposed system activity dashboard	68
4.13	Proposed system report dashboard	69

ABSTRACT

Ensuring public safety through efficient crime investigation and emergency response is crucial in today's complex world. This study presents a predictive model for an integrated Crime Investigation and Emergency Response System, leveraging data-driven analysis, advanced machine learning algorithms, and modern Information Technology (IT). The research aims to enhance law enforcement and emergency response protocols, recognizing the critical role of IT in managing critical incidents. The study addresses challenges in crime investigation, particularly violent offenses, by employing machine learning strategies incorporating regression and classification techniques. The primary objective is to uncover patterns and insights to predict perpetrator characteristics such as age, gender, and their relationship with the victim. Through comprehensive data analysis of a dataset containing 638,454 crime records from 1980 to 2014, the research identified 190,282 unsolved crimes, with approximately 100,000 involving handguns. The Municipal Police agency reported the highest number of unsolved crimes, highlighting the need for improved investigative tools. The predictive model's performance was evaluated using the Receiver Operating Characteristic (ROC) curve, demonstrating a remarkable accuracy with an Area Under the ROC Curve (AUC) of 95%. The model exhibited high accuracy rates in predicting the perpetrator's gender (96%) and relationship with the victim (97%), significantly outperforming an existing model. These results underscore the potential of the developed predictive model to enhance law enforcement capabilities and emergency response procedures. The study recommends further integration of data-centric approaches in public safety operations to improve efficiency and outcomes.

.

Keywords: Civil Intelligence, Emergency, Multi-Linear Regression, K-NN, ANN

CHAPTER ONE
INTRODUCTION

1.1 Background Information

Modern society is vulnerable to disruption or collapse of critical infrastructure caused by accidents or natural disasters. Efficient solutions to these incidents are essential, not only to restrict the effects on the human aspect, but also to the cultural, economic, and political aspects. Disaster and disaster management have attracted the interest of Information Systems/Information Technology (IS/IT) researchers in the last few years. Significant efforts have been made by national and local emergency authorities to develop information technology that can support and improve work at the organizational, inter-organizational, national, and even global levels in the event of emergencies or crises. Irrespective of the size of the disaster, the usage of information technology in emergency management organizations helps to enhance the capacity to take immediate measures and monitor the complex and evolving scenario (Agarwal, Renuka, and Rajni, 2013).

A crime is an act that constitutes an offense and is punishable by law. Analyzing and finding underlying crime trends are significant challenges for the police force because there are broad statistics on violence. Therefore, methodologies are needed to help the investigation office solve crimes. The machine-learning approach offers regression and classification strategies that allow one to accomplish this aim. Regression methods, such as multi-linear regression, are mathematical tools used to evaluate the association between two quantitative variables and predict the value of the dependent variable(s) based on the independent variable(s).

Classification methods, such as K-Nearest Neighbor (KNN) is used to define multiclass target variables. Neural networks are then used to boost the precision of projections, including an input layer, thin layer, and output layer. Depending on these equations, the model forecasts the author's definition of age, sex, and relationship with the abuser. As a result, this system is

expected to ease the burden on the police department in dealing with murder cases. (Archana, Prachi, Sagar, & Nikhil, 2016).

In recent years, IT support has become an essential tool for operational emergency response work. To a large extent, current academic research has addressed the role of information technology in practices with time-critical characteristics, as identified in operational emergency response work. The emergency response functions necessitate swift transitioning, whereby the functions of relatively low-intensity are promptly transferred to high-intensity work, combined with a significant degree of uncertainty.

There are few empirical studies on operational emergency response work, and it is necessary to conduct such studies to identify the general characteristics and design implications of information technology support. According to a survey published by the International Health Organization, more than 50 percent of people around the world have perpetrated illegal behavior (Archana, Prachi, Sagar, & Nikhil, 2016).

The National Crime Records Bureau of India reported that a woman assaulted every three minutes in the country. The authorities are not in the position to intervene, because knowledge about the incident will not enter them in time (Chen & Xu, 2011). With the number of illegal acts rising at an alarming pace, it is evident that a professional community needs a mechanism to monitor the current situation.

This study presents the Crime Investigation System (CIS), an online platform designed to meet the requirements of both the general public and law enforcement personnel. The CIS specializes in analyzing crime data and automating police investigations with the utilization of data mining technology. Data mining is an invaluable tool for sifting through extensive datasets, facilitating the recognition of patterns and the establishment of vital connections for data-driven problem-solving (Chen & Xu, 2011).

Additionally, the research underscores the significance of emergency management training in evaluating the current implementations of information systems for emergency notifications. The primary goal of the proposed system is to alleviate the burden of reporting incidents by empowering victims to take a stand against wrongdoers. This system enhances efficiency by ensuring data confidentiality and expediting the investigative processes (Heartfield, George, and Diane, 2016).

1.2 Problem statement

The current approach to conveying urgent situations presents several critical problems that have necessitated this study. The problem statement encompasses the challenges in the following areas:

(a) Difficulty in tracking down and identifying criminals after a crime has been committed.

(b) Delays in rapid response and potential risk of lives due to limited emergency reporting, and

(c) Ineffective response coordination system due to inadequate accident data sharing.

1.3 Objectives

The main objective of this study is to develop a predictive model for crime investigation and emergency response management. The specific objectives are to:

i. To collect and prepare extensive training and testing data from Kaggle, and then use Python to build and train a predictive model for civil crime prediction using multi-linear regression, K-Nearest Neighbor (K-NN), and Artificial Neural Networks.

ii. To develop a civil intelligence gathering and emergency reporting system for the stakeholders using Microsoft Visual Studio Code.

iii. To integrate the predictive model into the civil intelligence and emergency reporting application developed

iv. To assess the model's performance through standard metrics like accuracy, precision, recall, and F1-score.

1.4 Research Questions

i. To what extent can extensive training and testing data from Kaggle be collected and prepared to build and train a predictive model for civil crime prediction using multi-linear regression, K-Nearest Neighbor (K-NN), and Artificial Neural Networks in Python?

ii. To what extent can a civil intelligence gathering and emergency reporting system be developed for stakeholders using Microsoft Visual Studio Code?

iii. To what extent can the predictive model be effectively integrated into the civil intelligence and emergency reporting application?

iv. To what extent does the predictive model perform well when assessed using standard metrics like accuracy, precision, recall, and F1-score?

1.5 Justification of the study

The study is important because it aims to address key issues in crime investigation and emergency management. By developing a Crime Investigation System (CIS) that uses data mining technology, the study seeks to improve the efficiency and effectiveness of law enforcement by providing essential insights into crime patterns and relationships. This data-driven approach can make investigations faster and more accurate, leading to a safer society.

Additionally, the study focuses on improving emergency management systems. It highlights the need for efficient and rapid responses during emergencies and recognizes the role of technology in achieving this goal. By examining and enhancing emergency notification systems, the study aims to reduce the burden of reporting incidents and improve overall response times. This can empower victims and witnesses, contributing to a more vigilant and responsive community.

1.6 Scope of the study

This study aims to address both crime prevention and non-crime-related emergencies, with distinct limitations and focus areas.

For crime prevention, the scope is specifically on post-crime activities. This includes the investigation and response phases after crimes have already occurred, rather than proactive measures to prevent crimes from happening in the first place.

The goal here is to enhance the methods used to investigate crimes and respond effectively once a crime has been committed.

Regarding non-crime-related emergencies, the study is limited to emergencies that are directly connected to criminal activities. This could include situations like medical emergencies resulting from violent crimes or fires set intentionally. However, it does not extend to natural disasters such as earthquakes, hurricanes, or other emergencies that are not linked to criminal acts.

Furthermore, the study does not explore the long-term social impacts that may arise from improvements in crime and emergency response systems. Instead, it concentrates on immediate enhancements in the efficiency and effectiveness of these systems. The focus is on how quickly and accurately crimes can be investigated and how swiftly and effectively emergency responses can be executed in the short term.

Finally, the research does not cover the legal and judicial processes involved in prosecuting crimes. It does not delve into court proceedings, sentencing, or any other aspects of the judicial system. The primary focus remains on the initial phases of investigation and emergency response. The study aims to optimize the tools and technologies used by law enforcement and emergency responders to improve their immediate reaction to incidents.

By narrowing the scope in these ways, the study seeks to provide concrete, actionable insights that can be directly applied to improve the efficiency of crime investigations and emergency responses, ultimately contributing to a safer and more responsive society.

.

.

CHAPTER TWO

LITERATURE REVIEW

2.1 Conceptual framework

A conceptual framework is the intellectual structure upon which a research study is built. It helps researchers define the scope of their investigation, understand the theoretical background, and design the research process, from formulating hypotheses to data collection and analysis. This framework provides a clear, organized foundation that ensures the research is logically structured and its objectives are met effectively. It is a fundamental tool for researchers to align their work with existing knowledge and theories, making their studies well-grounded and contributing to the advancement of their respective fields.

2.1.1 Historical Background of Emergency Management in Nigeria

The field of emergency management in Nigeria, a country once regarded as the Giant of Africa, is still in its early stages of development. Although coordinated responses to disasters can be traced back to the early 1900s, when the Fire Brigade was responsible for extinguishing flames, protecting property, and aiding cities in their disaster response efforts, a systematic approach to emergency management only began to take shape in 1999.

Since then, Nigeria's disaster response program has made significant advancements, including the establishment of an improved operational framework, allocation of additional resources, the creation of curricula for emergency response training systems, enhanced recruitment of emergency personnel, and increased collaboration with other nations on emergency management issues.

However, despite these notable achievements, the nascent disaster management system in Nigeria still faces numerous challenges, such as widespread poverty, inadequate funding for emergency management programs, and marginalization, among others. (Hongjian et al, 2014).

2.1.2 Organizational Structure of Emergency Management

At the federal level, the National Emergency Management Agency (NEMA) serves as the primary agency responsible for disaster response, with its six regional offices strategically located across the country. Additionally, the federal government has mandated the establishment of state emergency management agencies at the state level and local emergency management agencies at the local level. All three tiers of emergency response organizations have the responsibility of building resources to effectively plan, mitigate, respond to, and recover from disasters.

Other key stakeholders in Nigeria's emergency management system include, but are not limited to, the military, police, paramilitary forces, and civil society organizations. The Disaster Response Units (DRUs), which can be mobilized from military bases worldwide, play a crucial role in Nigeria's disaster response program. Furthermore, community organizations such as Community-Based Organizations (CBOs), Faith-Based Organizations (FBOs), and Non-Governmental Organizations (NGOs) are often the first to provide assistance in the event of a disaster.

The collective efforts of this Emergency Response System are supplemented by the invaluable contributions of Emergency Management Volunteers (EMV), and in cases where additional support is needed; the State Emergency Management Agencies (SEMA) and NEMA are able to provide assistance.

2.1.3 Challenges and Opportunities Confronting Nigeria's Emergency Management System

The emerging emergency response services in Nigeria face a myriad of challenges, which include, but are not limited to, inadequate funding, deficiencies in state-level emergency

management mechanisms, insufficient disaster preparedness, lack of coordination among various levels of government, and issues of corruption.

Firstly, the underfunding of NEMA poses a significant obstacle. Studies conducted by assistant risk management managers have revealed that the allocated funds for risk management fall short of meeting the needs for catastrophe risk mitigation. Insufficient financial resources negatively impact NEMA's ability to implement effective risk reduction strategies. Moreover, the lack of funding may be attributed to the fact that the federal government does not prioritize disaster risk reduction (Lalitha, et al., 2017).

Secondly, while the federal government mandates that each of the 36 states possess a State Emergency Management Agency (SEMA), it is noteworthy that only 22 states have enacted legislation to enforce disaster response services (Malathi and Santhosh, 2011)). Additionally, many jurisdictions adhere to either the pre-existing Disaster Protection Agency or an ad hoc emergency management program. Consequently, the presence of diverse emergency response systems within state departments not only complicates the process of standardizing policies but also hinders effective functioning and mobilization of personnel during crises (Kansara, 2016).

Thirdly, a significant impediment to the development of an expanding emergency response program is the scarcity of specialized disaster risk mitigation courses. Although proposals are underway to incorporate disaster risk reduction into the primary and secondary education curriculum, this deficiency persists (Kiani et al., 2015).

Fourthly, the lack of collaboration and cooperation between different levels of government, particularly at lower levels, poses further challenges to Nigeria's emergency management system. The severity of this issue is exacerbated by the dearth of capacity to mitigate risks and establish emergency planning at both local and national levels. Furthermore, certain stages are

more prone to immediate experiences of the consequences of accidents, further complicating the situation (Kiani et al, 2015).

Deprivation, ultimately, represents yet another issue confronting Nigeria, with over 70% of its population living below the poverty line. This dire poverty serves as one of the foundational causes of terrorism and potentially offers an explanation for the heightened terrorist activities within Nigeria (McClendon and Natarajan, 2015).

Given the numerous challenges faced, Nigeria does possess three potential avenues for the development of a comprehensive disaster response program.

Firstly, the federal government should expand the availability of disaster response courses within higher education institutions. Presently, only six Nigerian colleges offer established curricula in disaster risk assessment and confer Master's degrees in disaster risk management. The National Emergency Management Agency (NEMA) is responsible for providing three years of support for this initiative. NEMA should strive to extend this program to other universities across Nigeria.

In addition, the federal government should tap into the expertise of the Grassroots Emergency Management Volunteers Corps (GEVC) to strategize, safeguard, respond, and rebuild in the wake of disasters. Since its inception in 2008, the GEVC has proven to be a successful mechanism for catastrophe risk management and has expanded its reach to approximately 23 states with around 6,408 members. By allocating sufficient funding for the GEVC to expand its operations to additional states, this volunteer corps can become an even more active participant in mitigating catastrophe threats and responding to disasters. Similarly, unemployed students, particularly those with prior experience in disaster risk gained through the National Youth Service Corps (a compulsory one-year program for university and polytechnic college students), can be engaged as paid volunteers to assist in implementing disaster risk management strategies. For instance, they can educate the public on the importance of

preparedness for and response to disasters. NEMA will collaborate with the Regional Jobs Directorate to evaluate the feasibility of this proposed strategy (Muhammad et al., 2011).

Ultimately, the acts of violence carried out by Boko Haram, such as the attack on the UN Headquarters in Abuja in 2011 and the attempted bombing by Al-Qaeda on the Arabian Peninsula on Christmas Day in 2009, have unquestionably positioned Nigeria as a prominent participant in the realm of extremism, particularly on the U.S. stage. These actions serve as a catalyst for the State Government to establish collaborative efforts with the U.S. authorities in order to counteract the spread of extremism. The U.S. government stands to gain advantages by safeguarding its interests, such as the transportation of energy resources from Nigeria and other associated benefits. Nevertheless, since the terrorist attacks on September 11th, Nigerian and U.S. officials have been diligently working together in the fight against terrorism. For instance, both nations have closely allied to monitor and obstruct the flow of funds to militant groups, as well as exchange vital information.

2.1.4 Emergency Management

To delve into the field of emergency management, it is necessary to provide concise definitions for the concepts of hazards, emergencies, accidents, and disasters. A hazard refers to a potential or actual situation capable of causing harm to individuals, properties, or the environment. An emergency denotes a sudden and unforeseen event that poses a threat to the well-being of individuals, properties, or the surrounding ecosystem, thereby requiring immediate action. The terms accident and catastrophe encompass the relative magnitude of the impacts resulting from an incident upon the physical, social, and economic dimensions of a specific community. Occasionally, a series of tragic accidents occurring within hazardous circumstances culminate in an event of minor consequence for the community, but one that proves catastrophic for the individuals affected. It is crucial to acknowledge that even a minor accident in a dynamic setting always carries the risk of escalating into a disaster at the societal level (Sagar, 2017).

2.1.5 Conceptualization of Emergency Management Organization

Emergency management can be conceptualized as encompassing four interconnected functional domains: prevention, preparedness, response, and mitigation, which align with the stage of a disaster. Multiple community organizations share responsibility for these functional domains. Fire and rescue personnel bear a particular obligation to deter the occurrence of incidents. In Sweden, this responsibility is regulated by national legislation.

Traditionally, fire and rescue services are structured based on functional phases, including prevention, preparedness, response, and mitigation. In the event of an emergency necessitating an immediate response, a temporary organizational framework is established to facilitate command and control. This framework is commonly referred to as the incident command structure or incident management system. The primary objective of this organization is to streamline and coordinate emergency responders, while also integrating pre-planned resources into the response efforts (Perry, 2003). A frequently emphasized advantage of such a structure is its capacity to provide clear authority and accountability in time-sensitive situations (Sathyadevan and Surya, 2014).

The organization of emergency response work is influenced by a command-and-control approach, which is attributed to several factors. In the 19th century, fire and rescue services were established by civil-defence directors and personnel with military backgrounds, leading to a paramilitary-style organization. Additionally, the command-and-control approach is characterized by rational qualities and influenced by classical management theory.

Disaster sociologists emphasize the importance of organizing emergency response operations based on a decentralized structure that facilitates collaboration between professional actors and the public as a valuable resource. They argue that emergent behaviour is advantageous insofar

as new organizational structures, integrated into the response work, help bridge potential gaps in a specific emergency situation (Saurabh et al., 2015).

2.1.6 Time-critical response

Response is one of the four essential functional domains in emergency management. Within this domain, first responders play a central role in being trained and prepared to effectively and efficiently intervene in situations where individuals, infrastructure, or the community are at risk due to an incident or catastrophe. This indicates that time and temporalities are key aspects of this research. The nature of emergency management necessitates unique patterns of functioning and spatial arrangements. These patterns and mechanisms can be influenced by the adoption of modern technologies.

Time-critical employment, such as practical emergency management employment, exhibits several distinct characteristics compared to other types of work.

(a) The time-critical elements are associated with the reactive nature of the work. It imposes a time constraint on individuals involved in responding immediately to a critical incident within the shortest possible timeframe.

(b) The time-critical factors often involve uncertainty and confusion resulting from limited knowledge.

(c) The urgent intervention relies on team-based collaborative action, which is virtually unavoidable and continuous.

(d) The situation is intricate and dynamic, leading to increasing and sometimes conflicting priorities.

(e) Individuals involved in the response work operate on different timescales (Shekhar et al., 2007).

2.1.7 Information Technology with Emergency Management

Certain computer management tools and services serve as intermediaries in emergency service operations. Radio networking equipment stands out as one of the foremost technologies employed. Each fire-fighter participating in an emergency response activity is equipped with a radio headset, enabling communication within the fire department.

These radio handsets are also stored in reloaders within emergency vehicles. When fire fighters board the truck, they retrieve the radio gear and place it in their uniform's transmitter pocket. In addition to personal radio handsets, each vehicle is often equipped with roof-mounted radios used during transportation. Personal radio devices are configured to operate on a group radiofrequency, while the vehicle radio typically operates on a frequency designated for communication between the command center and the various rescue vehicles (Sivaranjani and Aasha, 2016).

The widespread usage of mobile telephones is also apparent in the fire and rescue services. Leaders and senior officers within the fire department rely on cell phones as part of their day-to-day responsibilities. Although fire-fighters are not typically equipped with smartphones, they often carry their mobile phones in the side pocket of their uniforms. In emergency response work, many incident commanders heavily depend on mobile phone usage to communicate with the command center. Compared to unencrypted radio transmission, cell phones offer a certain level of privacy. Mobile phone indicators play a significant role in this regard.

In addition to personal communication devices, GPS navigators have become a standard technology in rescue vehicles in recent years. Navigators used in rescue vehicles provide guidance through a designated route, either visualized on a map or conveyed through turn-by-turn instructions, from the current location to the accident site. These navigation systems are often commercially available products that either require the input of a specific address or

automatically generate the address location based on a message received from the command-and-control center (Su, 2012).

Mobile incident support systems have garnered increased attention and interest from fire and rescue services in recent years. These systems encompass a collection of software integrated into a unified system, designed to facilitate various operational response activities. Mobile incident command systems include applications that offer navigation support, access to maps, predefined response plans, property information, and access to databases containing hazardous material data.

Management plans encompass detailed information, such as premises specifications, business operation details, contact names and telephone numbers, relevant hazards or hazardous content, predetermined building access points, and the availability of fire hydrants at the incident site. Additionally, these plans may include images and architectural sketches of the buildings located at the site.

Mobile incident support systems are specifically designed to cater to the needs and utilization of the fire crew commander. User interaction necessitates the use of touch panels, cursors, and mice. The mobile incident support system commonly employs a combination of Mobitex / GSM / GPRS / UMTS for connectivity to command center systems or back-end information systems. The Mobile Incident Management Systems continue to prioritize the requirements of operational field commanders and the role of incident manager (Tsunoda et al., 2012).

2.1.8 The impact of information technology on emergency situations

Over the past two decades, the utilization of Information Technology (IT) in service organizations has experienced significant growth. This trend has often been cited as a catalyst for overall efficiency improvement and income inequality shifts. Evaluating the impact of IT on production and its effects on competitiveness has therefore become a crucial element in

assessing the causes of economic development and various public policies (Viswanath and Hitendra, 2011).

Measuring the benefits derived from the use of IT in service organizations has proven to be a challenging task due to several interconnected reasons.

In the first place, IT offers advantages through enhanced timeliness and consistency, such as quick and personalized access to user accounts or product-specific information.

Secondly, IT is considered a "general purpose" technology, meaning that its benefits can vary depending on the specific application and characteristics of the adopting organization. Without detailed data on the types and uses of IT, empirical studies must be aggregated across various applications, where IT entails a wide range of costs and benefits, making policy analysis arduous. Additionally, IT implementation may coincide with possible improvements in role design and human resource practices. Furthermore, a skill-based technological transition often accounts for observable shifts in the pay structure. Neglecting organizational architecture overlooks a policy-relevant factor in efficiency and can contribute to discrepancies in the assessment of the impact of IT.

2.1.9 Information Technology and Job Design in Emergency Response Systems

The Emergency Alert Program serves as a public utility that offers a structured and coordinated intervention system for local authorities to effectively respond to emergencies. Prior to the late 1960s, emergency calls were directed either to a telephone operator (whose expertise and equipment were not specialized in emergencies) or to local support providers (where callers had to search for the telephone number of the relevant agency), resulting in inadequate response to calls. Following a model initially established in Europe, 911 services were introduced in the United States in 1968. Although the extent and particulars may vary, the typical operation of these systems is as follows:

i. An individual witnessing an emergency contact a local telephone service, typically 911 or a designated seven-digit code.
ii. The caller is connected to the emergency response service organizations.
iii. In certain systems, callers have the option to provide additional information to aid the response (Viswanath and Hitendra, 2011).

Emergency management services are frequently voluntary and often differ in certain aspects from private sector utility companies. These variations necessitate the perception of emergency response services as a specific instance of "support desks," which are one of the rapidly growing applications of Information Technology (IT) in the government sector. Support desks are designed to encompass the following elements:

a. Timely response of organizations to customer inquiries.
b. Accurate provision of resources or information relevant to customer needs.
c. Efficient allocation of limited corporate resources to address consumer queries and complaints.

In recent years, the implementation of IT has significantly enhanced the organization and operation of support desks across various sectors. The importance of prompt, reliable, and resourceful management in emergency healthcare should not be overlooked. Early access to emergency care services, as emphasized by the American Heart Association's "survival line," has been proven to reduce the risk of death from out-of-hospital cardiac arrest. Scientific research demonstrates that the initiation of emergency treatments such as Cardio Pulmonary Resuscitation (CPR) and defibrillation substantially decreases the mortality rate.

Previously, defibrillation, which involves electrical shock stimulation to restore the heart's electrical function, was only available on Advanced Life Support (ALS) ambulances and administered by qualified paramedics. Additionally, the effectiveness of prescription drugs like

thrombolytic, used in one-third of cardiac disease cases in 1995, diminishes over time. Accurate details regarding each incident facilitate cost savings for time-sensitive emergencies.

2.1.10 Concepts of Crime Investigations using Information Technology

The concept of crime investigation using information technology is a transformative approach that leverages digital tools and techniques to enhance the entire investigative process, from data collection to case resolution. As highlighted by Holt and Bossler (2016), information technology plays a vital role in crime investigation by enabling law enforcement agencies to gather, process, and analyze vast amounts of data efficiently.

This includes the utilization of digital databases, surveillance systems, and forensic software for evidence collection and management. Moreover, the integration of Artificial Intelligence (AI) and machine learning algorithms, as discussed by Furlong et al. (2020), enables predictive policing and the identification of patterns, helping law enforcement agencies proactively combat crime. Information technology also facilitates the sharing of critical data among different agencies, as emphasized by Willard (2017), resulting in improved collaboration and more effective investigations.

Furthermore, the adoption of blockchain technology, as explored by Kosba et al. (2016), provides secure and transparent methods for handling digital evidence, ensuring the integrity and admissibility of data in legal proceedings.

2.2 Theoretical framework

A theoretical framework in research serves as the foundational structure that guides the study by presenting a systematic and organized set of concepts, principles, or theories relevant to the research topic. Essentially, a theoretical framework serves as the intellectual foundation of a research study, enhancing its coherence and helping to generate meaningful insights and conclusions.

2.2.1 Crime Pattern Theory

Crime Pattern Theory (CPT) is a theoretical framework used in criminology and crime investigation. It primarily focuses on understanding the spatial and temporal patterns of criminal activities. The theory is based on the premise that crimes are not randomly distributed but tend to follow specific patterns and trends. Understanding these patterns can help law enforcement agencies and investigators predict, prevent, and solve crimes more effectively. The following are details about the CPT:

1. Origin and Development: The concept of Crime Pattern Theory was first introduced by Brantingham and Brantingham in the late 1980s. They expanded on the principles of environmental criminology and routine activities theory. This theory has since become a fundamental component of modern criminology.
2. Principles: Crime Pattern Theory operates on several key principles:
    (a) Repetitive Offending: The theory suggests that most crimes are committed by a relatively small number of repeat offenders.
    (b) Location-Based: It emphasizes the importance of geographical locations, or "hotspots," where criminal activities tend to concentrate.
    (c) Time-Based: The theory recognizes that crimes may follow specific temporal patterns, such as certain days of the week or times of the day.
3. Hotspots: Hotspots are central to Crime Pattern Theory. These are geographic areas with a significantly higher frequency of criminal incidents than the surrounding areas. The theory suggests that identifying and focusing on these hotspots can lead to more effective crime prevention and intervention strategies.
4. Preventive Strategies: The theory encourages law enforcement agencies to concentrate resources and efforts in hotspots. This can involve increased patrolling, surveillance, or

community engagement. By targeting these areas, authorities aim to disrupt criminal activities and reduce crime rates.

5. Data-Driven Analysis: Crime Pattern Theory relies heavily on the analysis of crime data. Advanced technologies, including Geographic Information Systems (GIS) and predictive policing software, are often used to identify hotspots and analyze crime patterns.
6. Repeat Victimization: The theory also considers the concept of repeat victimization. This occurs when certain individuals, properties, or locations are repeatedly victimized. Understanding these patterns can help law enforcement provide better protection to potential targets.
7. Predictive Policing: Many law enforcement agencies have adopted predictive policing strategies based on Crime Pattern Theory. Predictive policing uses historical crime data to anticipate where future crimes are likely to occur. This approach allows authorities to allocate resources more efficiently.
8. Evaluation and Criticism: While Crime Pattern Theory has been widely embraced, it is not without criticism. Some argue that it may lead to over-policing in certain neighbourhoods, potentially exacerbating issues of racial or social inequality. Ethical considerations and concerns related to data privacy are also raised.

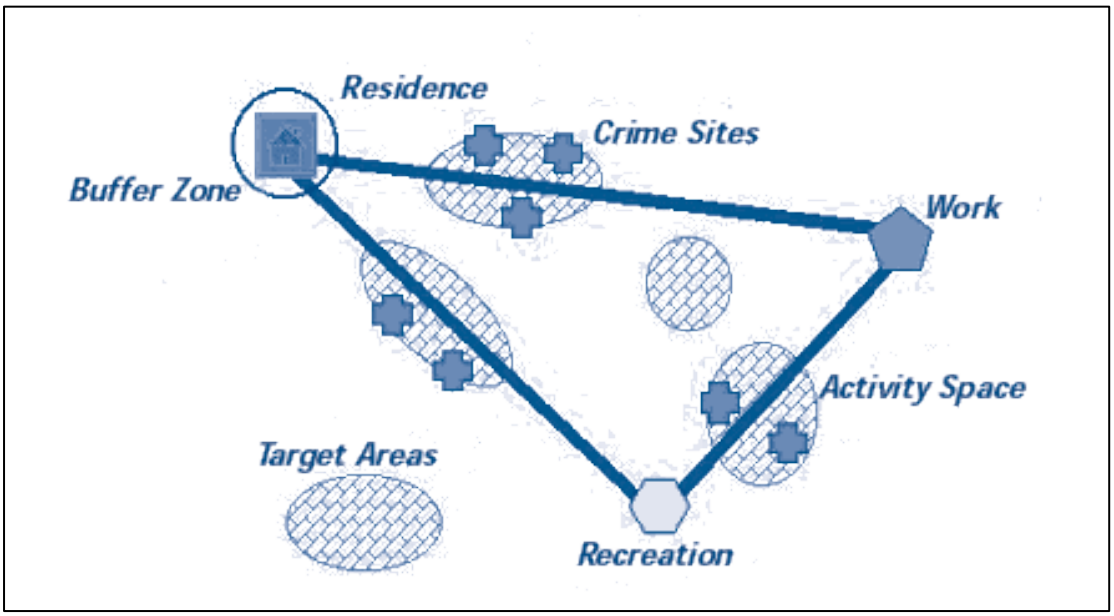

Figure 2.1: Illustration of Crime Pattern Theory (Brantingham and Brantingham, 1980)

2.2.2 Social Learning Theory

Social Learning Theory (SLT) was developed by Albert Bandura in the 1960s. He first introduced the theory in a 1961 paper called "Transmission of Aggression Through Imitation of Aggressive Models" and he continued to build on the ideas in later works. SLT is a prominent psychological framework that explains how individuals learn behaviours and acquires new skills through observation, imitation, and interaction with others in their social environment. This theory suggests that people do not solely rely on their own experiences to develop behaviours but rather learn from observing the actions and consequences experienced by those around them.

The core principles of Social Learning Theory encompass the idea that behaviour is acquired through a process of modeling and reinforcement. Individuals observe the behaviours of others, particularly role models or significant figures in their lives, and then imitate those actions. This observational learning can occur through various sources, including family members, peers, teachers, and the media.

One significant aspect of the theory is the concept of reinforcement. Social Learning Theory posits that individuals are more likely to repeat behaviours they have observed if they witness positive consequences or rewards associated with those behaviours. Conversely, behaviours that result in negative outcomes are less likely to be repeated. This emphasizes the importance of vicarious reinforcement, where individuals observe the consequences experienced by others and incorporate this information into their decision-making processes. Thus, the theory accounts for the acquisition of both prosocial and antisocial behaviours based on the observed rewards and punishments related to those actions.

In the context of crime investigation and criminology, Social Learning Theory can help explain how criminal behaviours are acquired and perpetuated within communities. It highlights the role of social influences and the impact of role models or peers who may encourage or discourage criminal actions. Additionally, understanding the mechanisms of reinforcement can guide efforts to prevent criminal behaviours by promoting prosocial alternatives and addressing the environmental factors that may contribute to the acquisition of criminal skills and attitudes. Social Learning Theory's insights have been influential in various fields, including education, psychology, and criminology, making it a valuable framework for comprehending human behaviour.

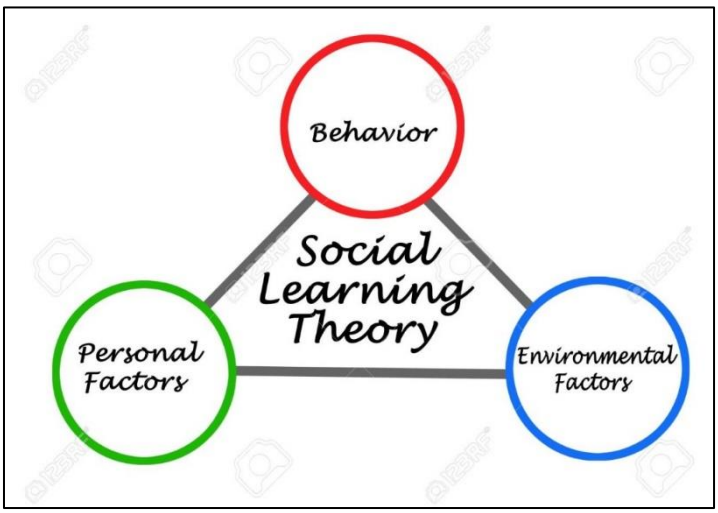

Figure 2.2: Illustration of Social Learning Theory (Viswanath and Hitendra, 2011)

2.2.3 Technology Acceptance Model

The Technology Acceptance Model (TAM) is a valuable framework used to explore the adoption of technology by individuals. It posits that two primary factors significantly influence a user's intention to adopt technology: perceived ease of use and perceived usefulness. Perceived ease of use pertains to how users view the simplicity or difficulty of employing the technology, while perceived usefulness relates to their belief in the technology's capacity to enhance their performance or productivity. Users who perceive a technology as both easy to use and useful are more likely to express an intention to use it.

One of the strengths of TAM is its simplicity and applicability across various technology contexts. Researchers and organizations frequently employ TAM to evaluate and forecast user acceptance of technology, enabling them to design and introduce technology more effectively. By enhancing the perceived ease of use and usefulness of a technology, designers and developers can positively influence users' behavioural intentions, ultimately leading to greater actual system use.

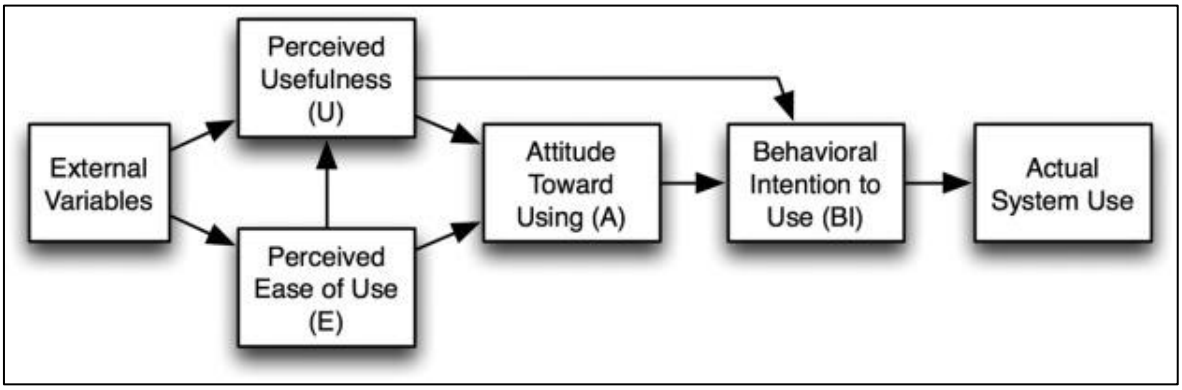

Figure 2.3: Illustration of Technology Acceptance Model (Tsunoda et al., 2012)

2.2.4 Prediction theory

Prediction theory is a framework focused on the processes involved in making forecasts, spanning various domains. It acknowledges the presence of uncertainties and errors in predictions, emphasizing the importance of addressing these uncertainties. Researchers explore

the strategies and cognitive biases that influence prediction accuracy to enhance forecasting methods. Furthermore, prediction theory provides tools for evaluating the performance of predictive models, crucial for fields like finance and risk management. In essence, it aims to improve the quality and reliability of predictions in decision-making processes.

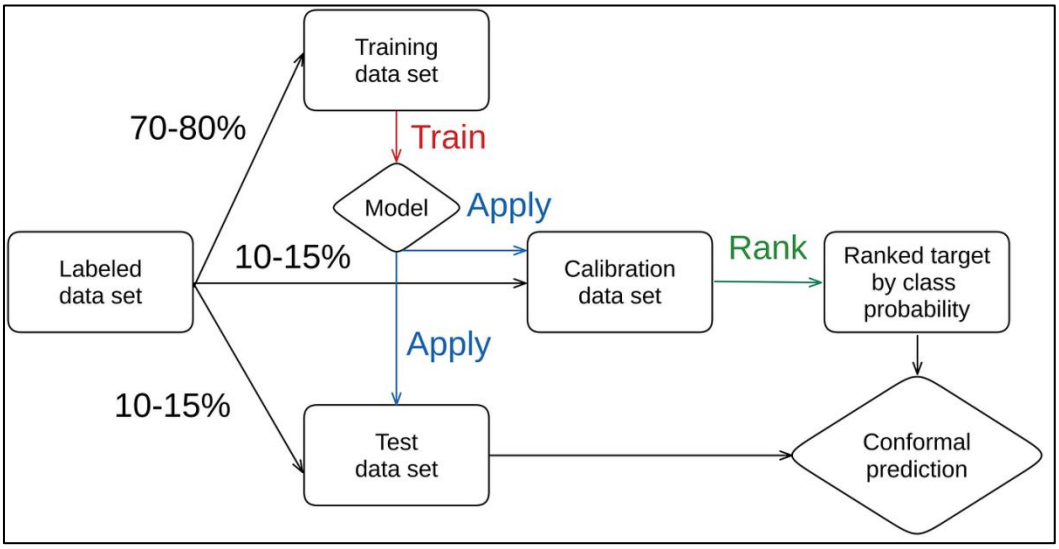

Figure 2.4: Illustration of Predictive Theory (Shekhar et al., 2007)

2.2.5 No Free Lunch Theorem

The No Free Lunch Theorem, was introduced by David Wolpert, is a critical concept within machine learning. It stresses that no single machine learning algorithm is universally superior for all types of problems. This theorem serves as a reminder that the effectiveness of a machine learning algorithm is intimately tied to the specific characteristics of the problem it is intended to address. In essence, when one algorithm excels at solving a particular problem, it tends to struggle when confronted with a different type of problem. Therefore, there is no silver-bullet algorithm that universally outperforms all others in every scenario. This theorem has practical implications for machine learning practitioners, as it underscores the necessity of carefully selecting the appropriate algorithm based on the unique features and requirements of each problem. For instance, decision trees may prove effective when dealing with problems characterized by easily interpretable features, while complex deep neural networks may be

more suitable for tasks involving unstructured data such as images and text. In essence, the No Free Lunch Theorem directs machine learning professionals to tailor their algorithm choices to the specific demands of each application, considering factors like data distribution, problem complexity, and available resources.

It should be noted that the Crime Pattern Theory is more essential for predictive crime models because it shows that crimes occur in specific patterns and locations, influenced by where people live, work, and socialize. This theory helps identify crime hotspots and trends, enabling accurate predictions and faster, more effective law enforcement responses. Unlike other theories, such as Social Learning Theory or the Technology Acceptance Model, which do not focus on crime prediction, Crime Pattern Theory is directly applicable to improving crime investigation and emergency responses.

2.3 Empirical framework

The empirical framework pertains to the practical execution of a research study, involving the collection and analysis of real-world data to test hypotheses or answer research questions. Researchers use various methods to gather data and apply statistical or qualitative techniques for analysis. This process helps to confirm or refute initial hypotheses, contributing to the growth of knowledge in a specific field. The following section comprises the reviewed related works.

Mahajan et al. (2020) proposed an Online Crime Reporting System to modernize and streamline the process of sharing crime-related data with the public. This digital system, administered by the Superintendent of Police (SP), replaces the traditional manual approach to data storage and management. It allows authorized personnel to upload and modify information about crimes, missing persons, and terrorism. The Online Crime Reporting System is designed to efficiently organize messages based on their content. Its core objective is to enhance the existing physical infrastructure by introducing computerized tools and comprehensive

software. This transition ensures the secure, long-term storage and easy retrieval of valuable data, with readily available and user-friendly hardware and software components.

Archana, Durga, and Saveetha (2020) introduced an online crime reporting system which enables victims to file cases through a website, including the option to submit photo evidence. The system incorporates an 'SOS' feature, allowing users to swiftly transmit their location to the nearest police station in emergencies. There is also a dedicated module for accident victims to expedite FIR registration and prompt medical treatment. User information remains confidential, with only their complaints forwarded to the nearest police station. Location identification relies on cookies and IP addresses, with the server resolving location conflicts and routing messages accordingly. This project aims to bridge the communication gap between law enforcement and the public, facilitating online FIR submissions and notifications about case progress.

Gopchandani et al. (2020) presented an online crime reporting system, recognizing the integral role of technology in modern life, with ubiquitous use of computers, laptops, and smartphones. This system empowers users to report crimes directly from the location of the incident, leveraging technology for user tracking. Users are obligated to upload a profile picture and furnish their Aadhar card details, facilitating the department in maintaining a comprehensive user database, thereby improving monitoring and accountability.

Idhole et al. (2021) designed a web-based crime report management system for implementation in police stations nationwide. The system operates both offline and online, engaging citizens in active participation. The core objective of the crime reporting manager is the reduction of crime incidents, with a particular focus on crime detection and prevention. This research contributes to enhancing crime investigations and offers effective and efficient methodologies for the process. The software's development encompasses various stages, including planning, requirement analysis, system analysis, deployment, and maintenance. The Crime Reporting

Manager serves as a confidential communication channel between complainants and authorities, fostering efficient interaction.

Priya, Srivastava, and Islam (2019) created an Online Crime Reporting System software that is easily accessible to the general public as well as local government authorities. In many parts of Asia, the traditional public hesitates to file complaints due to unfounded concerns about the local government. However, an online complaint registration system can alleviate these fears and assist the public in aiding local government agencies in apprehending criminals. This system is designed to serve as a protective and safety-oriented application that benefits both the public and the government.

Selvakani, Vasumathi, and Harikaran (2019) developed an ASP.Net-based web system for online crime reporting. They recognized the omnipresence of crime in human societies and the need for effective management. Their system featured four reporting forms, including those for complaints, crime events, investigations, and arrests. The system comprised three key modules for data capture, report management, and data utilization. The authors highlighted the importance of making such systems mobile-friendly, enhancing awareness, and improving overall usability in future work to better serve both the public and government interests.

Mkhwanazi et al. (2020) proposed an automatic crime reporting and immediate response system that would make it easier for people to report crimes and would allow the police to respond more quickly. The system could be anonymous and could store evidence in a non-SQL database for faster retrieval. The system could also be able to detect the location of the crime accurately.

Tabassum et al. (2018) proposed an Online Crime Reporting and Management System for Riyadh City. The system would allow people to report crimes anonymously and to track the status of their reports. The system would also help the police to identify criminals and to monitor crime trends.

Kiruthika, Armaan, and Syed (2021) proposed an interactive mobile-based crime reporting system (CMS) with map features to help the police and intelligence agencies in India to solve crimes more effectively. The CMS could be used by the public, police officers, and intelligence officials, and would offer different levels of access and functionality depending on the user's role. The CMS could make it easier for the public to report crimes as soon as they happen and to track the status of their reports. Police officers could use the map feature to get to the crime scene quickly and use the reported information to investigate the crime. Higher officials could monitor and track all the cases under their jurisdiction.

Sathayabama, Savitha, and Iswarya (2022), developed an online crime reporting system using Python and MySQL. The system allowed victims to file cases online and provides features such as anonymous reporting, crime alert system, case status tracking, crime notice board, cybercrime complaint registration, GPS tracking system, police contact details, and safe storage for evidence.

Jayasinghe and Perera (2021), proposed an automatic crime reporting and immediate response system that combines Raspberry Pi, Microsoft IoT, a mobile app, and a web app to allow people to report crimes anonymously or with their details, and to send the report to the police dispatch center in less than 30 seconds. The system could also store pictures, videos, and audio recordings of the crime scene, and it could use a non-SQL database to allow for faster retrieval of evidence.

Shakir et al. (2023) proposed a lightweight blockchain-based framework for secure and efficient online crime reporting. The framework used a public blockchain to store crime reports and a private blockchain to store sensitive data, such as victim and witness information. The framework also used smart contracts to automate the crime reporting process and to ensure the integrity and confidentiality of the data.

Babar et al. (2023) developed an Online Crime Reporting System (OCS) to modernize and streamline the process of sharing crime-related data with the public. The OCS allowed authorized personnel to upload and modify information about crimes, missing persons, and terrorism. It is designed to efficiently organize messages based on their content and to provide secure, long-term storage and easy retrieval of valuable data.

Manjula and Kumar (2020) developed an online Crime Reporting System (CRS) to facilitate the reporting and management of crimes. The CRS allowed users to register, file complaints, and track the status of their complaints. It also provides features such as anonymous reporting, crime alerts, and a forum for users to discuss crime and safety tips. The CRS is designed to help improve the efficiency and effectiveness of crime reporting and management.

Anitha and Sundar (2019) proposed an Online Crime Report and Maintenance System using centralized data to improve the efficiency and effectiveness of crime reporting and investigation. The system allowed users to report crimes anonymously or with their personal details, and it provides features such as case status tracking, crime alert system, and crime notice board. The system also helps the police to identify criminals and to monitor crime trends.

Nivethan et al. (2022) proposed a web-based Online Crime Reporting System (OCRS) using Python and MySQL. The OCRS allowed users to report crimes anonymously or with their personal details, and it provided features such as case status tracking, crime alert system, and crime notice board. The OCRS also helped the police to identify criminals and to monitor crime trends.

2.4 Summary of related works

Table 2.1 summarizes the information on Online Crime Reporting Systems (OCRS) from the related research articles reviewed, focusing on the key techniques used and the advantages and disadvantages of each system.

Table 2.1: Summary of related works

S/N	Author's name/year	Research domain	Techniques used	Work done	Challenges
1	Mahajan et al. (2020)	Online Crime Reporting System	Web-based system, centralized data	Modernize and streamline crime-related data sharing	▪ Security and confidentiality of crime data ▪ No intelligence
2	Archana, Durga, and Saveetha (2020)	Online Crime Reporting System	Web-based system, SOS feature, photo evidence submission, FIR registration	Enabled victims to file cases online	▪ Security and confidentiality of crime data ▪ No intelligence
3	Gopchandani et al. (2020)	Online Crime Reporting System	Web-based system, user tracking, Aadhar card verification	Empowered users to report crimes directly	▪ Security and confidentiality of crime data ▪ No intelligence
4	Idhole et al. (2021)	Crime Report Management System	Web-based system, offline and online operation, crime detection and prevention	Improved crime detection and prevention	▪ Security and confidentiality of crime data ▪ No intelligence
5	Priya, Srivastava, and Islam (2019)	Online Crime Reporting System	Web-based system, mobile-friendly interface	Created easily accessible software	▪ Security and confidentiality of crime data ▪ No intelligence
6	Selvakani, Vasumathi, and Harikaran (2019)	Online Crime Reporting System	ASP.Net-based web system, four reporting forms, data capture, report management, and data utilization	Developed web system for online crime reporting	▪ Security and confidentiality of crime data ▪ No intelligence
7	Mkhwanazi et al. (2020)	Automatic Crime Reporting and Immediate Response	Raspberry Pi, Microsoft IoT, mobile app, web app, non-SQL database	Proposed automatic crime reporting system	▪ Security and confidentiality of crime data ▪ No intelligence

Table 2.1: Summary of related works (Cont'd)

S/N	Author's name/year	Research domain	Techniques used	Work done	Challenges
8	Tabassum et al. (2018)	Online Crime Reporting and Management System	Web-based system	Proposed system for Riyadh City	▪ Security and confidentiality of crime data ▪ No intelligence
9	Kiruthika, Armaan, and Syed (2021)	Online crime reporting system	Interactive mobile-based CMS with map features	Proposed a system to help the police and intelligence agencies in India to solve crimes more effectively	▪ Security and confidentiality of crime data ▪ No intelligence
10	Sathayabama, Savitha, and Iswarya (2022)	Online crime reporting system	Python and MySQL	Online crime reporting system with anonymous reporting, alerts, tracking, and storage.	▪ Security and confidentiality of crime data ▪ No intelligence
11	Jayasinghe & Perera (2021)	Automatic crime reporting and immediate response system	Raspberry Pi, Microsoft IoT, mobile app, web app, non-SQL database	Automatic crime reporting system for faster police response	▪ Security and confidentiality of crime data ▪ No intelligence
12	Shakir et al. (2023)	Online crime reporting system	Public and private blockchains, smart contracts	Secure and efficient online crime reporting system with blockchain.	▪ Security and confidentiality of crime data, scalability ▪ No intelligence

Table 2.1: Summary of related works (Cont'd)

S/N	Author's name/year	Research domain	Techniques used	Work done	Challenges
13	Babar et al. (2023)	Online Crime Reporting System (OCS)	Web-based system	Crime reporting system for authorized personnel.	▪ Security and confidentiality of crime data, user authentication ▪ No intelligence
14	Manjula & Kumar (2020)	Online crime reporting system (CRS)	Web-based system, centralized data	Complaint filing and tracking system for users.	▪ Security and confidentiality of crime data, user authentication ▪ No intelligence
15	Anitha & Sundar (2019)	Online crime report and maintenance system	Centralized data	Improved crime reporting and investigation system	▪ Security and confidentiality of crime data, user authentication ▪ No intelligence
16	Nivethan et al. (2022)	Online crime reporting system (OCRS)	Python and MySQL	Web-based crime reporting system with anonymous reporting	▪ Security and confidentiality of crime data, user authentication ▪ No intelligence

2.4.1 Gap Analysis

The main gap in knowledge from Table 2.1 is the lack of focus on intelligence generation. While all of the studies mentioned propose systems that would make it easier for people to report crimes, none of them discuss how to use the reported data to generate actionable intelligence. This is a critical gap, as intelligence is essential for preventing and solving crimes.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Analysis of the existing crime investigation and emergency response system

The crime investigation and emergency response system in Nigeria is fragmented and underdeveloped. There is no single agency responsible for coordinating crime investigation and emergency response efforts. This lack of coordination has led to delays in response times, duplication of effort, and a lack of accountability.

The Nigerian Police Force (NPF) is the primary law enforcement agency in Nigeria. The NPF is responsible for investigating crimes and responding to emergencies. However, the NPF is underfunded and understaffed. It also lacks the necessary equipment and resources to effectively investigate crimes and respond to emergencies.

Other agencies that play a role in crime investigation and emergency response in Nigeria include the National Emergency Management Agency (NEMA), the Federal Road Safety Corps (FRSC), and the Nigerian Security and Civil Defence Corps (NSCDC). However, these agencies are not well-integrated with each other, and they often lack the resources to effectively carry out their duties.

The fragmentation of the crime investigation and emergency response system in Nigeria has a number of negative consequences. First, it leads to delays in response times. When there is no single agency responsible for coordinating response efforts, it can take longer for help to arrive at the scene of a crime or emergency. This can lead to loss of life and property.

Second, the fragmentation of the system leads to duplication of effort. Different agencies may end up responding to the same incident, which wastes resources and can lead to confusion.

Third, the fragmentation of the system makes it difficult to hold agencies accountable for their performance. When there is no clear chain of command, it can be difficult to identify who is responsible for failures in the system.

The Nigerian government has taken some steps to address the fragmentation of the crime investigation and emergency response system. In 2019, the government established the National Emergency Management Agency (NEMA), which is responsible for coordinating emergency response efforts across all levels of government. However, NEMA is still in its early stages of development, and it remains to be seen how effective it will be in coordinating emergency response efforts.

The Nigerian government also needs to invest more in the NPF and other agencies responsible for crime investigation and emergency response. These agencies need to be adequately funded and staffed, and they need to be equipped with the necessary resources to effectively carry out their duties.

Finally, the Nigerian government needs to develop a comprehensive national strategy for crime investigation and emergency response. This strategy should clearly define the roles and responsibilities of all agencies involved in crime investigation and emergency response. It should also establish mechanisms for coordinating response efforts and for holding agencies accountable for their performance.

3.1.1 Problems of the Existing System

The crime investigation and emergency response system in Nigeria faces a number of problems, including:

(1) Fragmentation: There is no single agency responsible for coordinating crime investigation and emergency response efforts. This lack of coordination has led to delays in response times, duplication of effort, and a lack of accountability.

(2) Underfunding and understaffing: The Nigerian Police Force (NPF) and other agencies responsible for crime investigation and emergency response are underfunded and understaffed. This makes it difficult for these agencies to effectively carry out their duties.

(3) Lack of equipment and resources: The NPF and other agencies responsible for crime investigation and emergency response lack the necessary equipment and resources. This includes things like vehicles, communication equipment, and forensic investigation equipment.

(4) Lack of training: Many police officers and other personnel involved in crime investigation and emergency response are not properly trained. This can lead to mistakes and ineffective investigations.

(5) Corruption: Corruption is a major problem within the Nigerian Police Force and other agencies responsible for crime investigation and emergency response. This can lead to cases being ignored or mishandled, and it can also erode public trust in the system.

These problems have a number of negative consequences, including:

(1) Delays in response times: When there is no single agency responsible for coordinating response efforts, it can take longer for help to arrive at the scene of a crime or emergency. This can lead to loss of life and property.

(2) Duplication of effort: Different agencies may end up responding to the same incident, which wastes resources and can lead to confusion.

(3) Ineffective investigations: The lack of resources and training can lead to ineffective investigations. This can make it difficult to catch criminals and bring them to justice.

(4) Loss of public trust: The problems with the crime investigation and emergency response system can erode public trust in the system. This can make it more difficult for the police to investigate crimes and respond to emergencies.

The Nigerian government needs to take steps to address these problems in order to improve the effectiveness of the crime investigation and emergency response system. This includes:

(1) Establishing a single agency responsible for coordinating crime investigation and emergency response efforts.

(2) Providing adequate funding and staffing for the NPF and other agencies responsible for crime investigation and emergency response.

(3) Equipping these agencies with the necessary resources to effectively carry out their duties.

(4) Providing proper training for police officers and other personnel involved in crime investigation and emergency response.

(5) Addressing the problem of corruption within the NPF and other agencies responsible for crime investigation and emergency response.

By taking these steps, the Nigerian government can improve the effectiveness and efficiency of the crime investigation and emergency response system, and better protect its citizens from crime and emergencies.

3.2 The proposed system

The proposed system is a comprehensive solution for collecting and analyzing civil intelligence, as well as responding to emergencies swiftly. Its primary aim is to efficiently gather critical incident reports and provide rapid assistance during emergencies. What sets it apart from the current system is its ability not only to monitor and document incidents and casualties but also to ensure that this crucial information is easily accessible to the relevant decision-making authorities.

Furthermore, the proposed system serves as a computerized platform designed specifically for gathering intelligence from the general public. It has the capability to collect information from individuals regarding suspected or actual wrongdoers, along with any relevant details about them. Additionally, it streamlines the distribution of this information for further examination, enabling security forces to take immediate action when necessary.

A key advantage of the proposed system is its ability to maintain an extensive database that includes both known and unknown data. This database can be accessed by various organizations to facilitate well-informed decision-making. This feature represents a significant enhancement compared to the current system.

The implementation of the system is divided into two distinct phases. The initial phase focuses on creating a user-friendly graphical interface, enabling users to interact effectively with the program. Users are provided with forms for submitting First Information Reports (FIR). In the second phase, a database of criminal profiles is established, containing pertinent details about suspects, including their physical characteristics, the year of their activities, location, and the types of crimes they have committed. During this phase, the system employs the K-means algorithm to analyze the data submitted by users. Based on this dataset, it generates forecasts and compiles a list of potential offenders. Subsequently, victims are informed of the status of their reports.

3.2.1 Data gathering

The crime dataset is sourced from Kaggle, a repository that offers datasets spanning various fields. This particular collection comprises entries related to murder cases. In essence, it is a dataset gathered from Kaggle, providing valuable information about various aspects of criminal activity, specifically focusing on murders.

(i) The Federal Bureau of Investigation (FBI) Supplemental Crime Report from 1980 to 2014: The FBI Supplemental Crime Report (SCR), spanning from 1980 to 2014, serves as a comprehensive data collection program that offers critical national and state-level insights into homicide victims and known homicide offenders in the United States. It stands as the most extensive database on homicides in the country, encompassing a range of variables such as victim and offender demographics, victim-offender relationships, weapon types used, location of incidents, timing, circumstances, and case dispositions. Law enforcement agencies

nationwide contribute this data to the FBI through the National Incident-Based Reporting System (NIBRS). Notable findings from this dataset reveal a 52% decline in the overall homicide rate over the observed period, with variations across gender and race, a prevalence of handgun and sharp instrument homicides, and intimate partner homicides commonly occurring in victims' residences.

Moreover, the SCR data holds vital significance for law enforcement, researchers, and policymakers. It empowers them to discern and analyze homicide patterns and trends, aiding in the development and evaluation of crime prevention and intervention initiatives. Additional insights from the data highlight substantial reductions in homicide rates among young adults and African Americans, a decrease in the use of firearms in homicides, and a decline in the percentage of homicides involving intimate partners. Ultimately, the FBI Supplemental Crime Report stands as an invaluable resource for shaping crime prevention strategies and informing public policy decisions in the United States.

(ii) The Freedom of Information Act (FOIA) holds records for over 22,000 homicide cases that were not examined by the Investigation Bureau. This dataset is quite extensive, comprising 638,454 rows and 17 columns, and it includes a section with metadata information. In essence, the FOIA dataset provides a wealth of information about these un-investigated homicide cases, making it a valuable resource for research and analysis.

3.2.2 System design

System design is the process of defining the architecture, components, and interfaces for the proposed system so that it meets the end-user requirements. It involves identifying the system's requirements, designing the system's architecture, and selecting the appropriate technologies and components.

System design is typically done in two phases:

1. Requirements analysis: This phase involves identifying and documenting the system's requirements. The requirements should be specific, measurable, achievable, relevant, and time-bound.
2. System architecture design: This phase involves designing the system's architecture. The architecture should define the system's components, interfaces, and data flows.

1. System architecture design

System architecture design is the procedure of outlining the fundamental structure, arrangement, and functioning of a system. This process includes pinpointing the system's key elements, their connections, and the principles and rules that guide their design and development. System architecture offers a top-level perspective of the system, outlining its primary components, their roles, and the way they communicate with one another and with external systems.

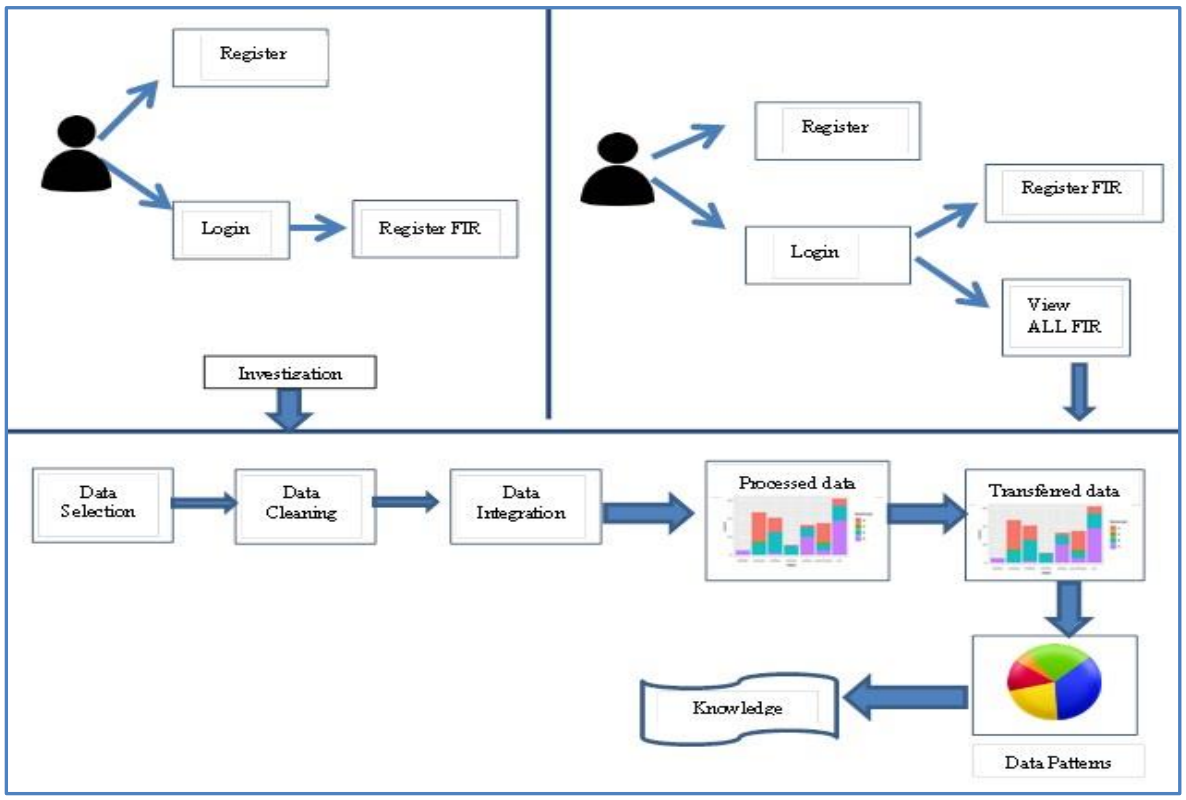

Figure 3.1: Proposed system architecture

Figure 3.1 depicts the proposed system architecture and workflow which involves a series of essential steps (User Interaction, Police Engagement and Criminal Data Analysis), aimed at streamlining the process of handling First Information Reports (FIRs) and complaints. The following shows the steps that are integrated into the system's operation:

Step 1 - User Interaction

The process begins with users signing in and logging into the FIRs and complaints lodging page. This initial step empowers individuals to promptly submit their FIRs or grievances via the website. Once these reports are in, they become accessible to the police for further action. This user-driven interaction serves as the point of origin for incident reporting, enabling a seamless transition from the public to law enforcement.

Step 2 - Police Engagement

Following the submission of FIRs and complaints, the next stage involves police interaction. Law enforcement personnel are required to register and log in to the system to access the incoming reports. At this juncture, an automated analysis is conducted on these reports, enhancing the efficiency of the investigative process. Upon completion of the inquiry, the police are responsible for changing the status of the FIR, and, importantly, they communicate the findings and progress to the complainants. This step highlights the integration of user-submitted information with police actions, ensuring transparency and responsiveness.

Step 3 - Criminal Data Analysis

The final phase of the system's operation involves the analysis of a criminal dataset. This dataset is meticulously managed, with missing values filled in as necessary. It serves as a vital resource for investigations. Here, the K-means clustering algorithm is employed to process the refined dataset. The clusters generated through this analysis are meticulously evaluated, leading to the compilation of a list of suspected offenders. This step integrates data-driven insights into

the process, facilitating the identification of potential wrongdoers and enhancing law enforcement's capabilities.

2. Workflow process

A workflow process refers to a systematic series of steps or tasks designed to achieve a specific goal, typically within an organization or a project. It helps streamline work, improve efficiency, and ensure that tasks are completed in a structured and organized manner.

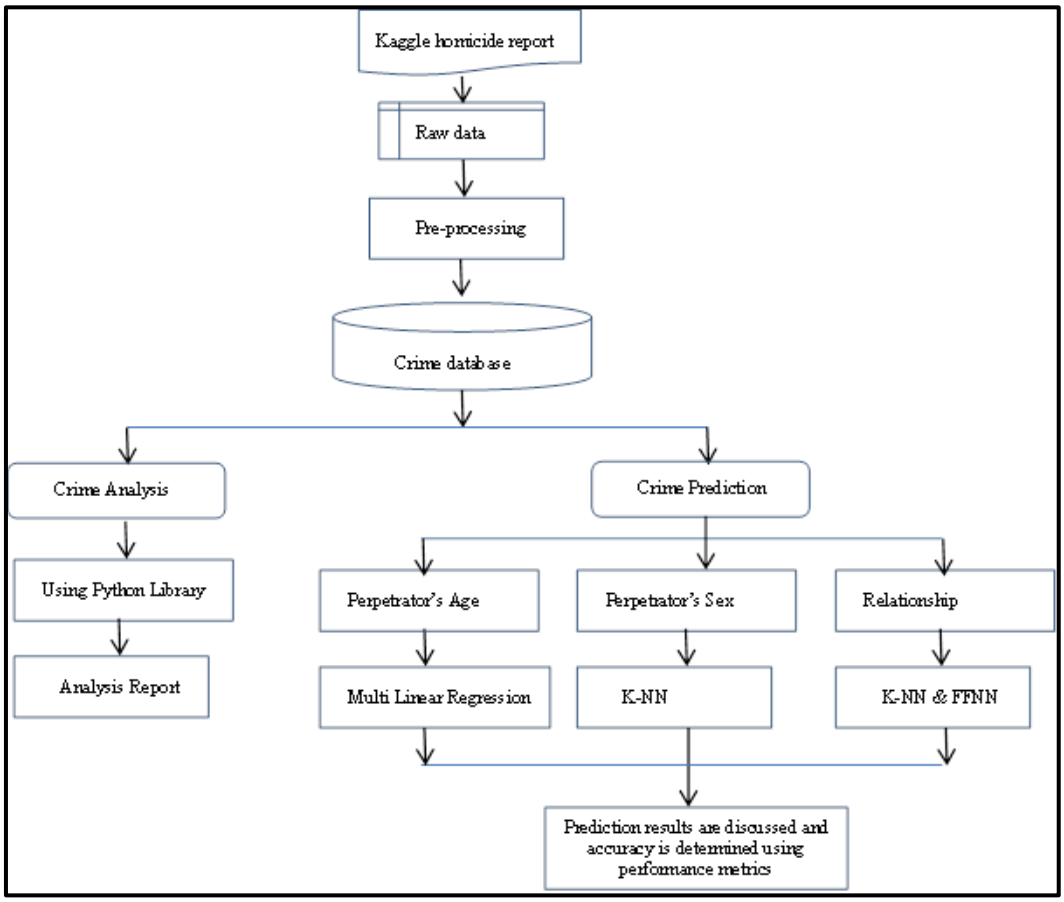

Figure 3.2: Proposed system workflow process

Figure 3.2 depicts the workflow process of the proposed system. The process represents a valuable and innovative approach to crime data analysis and the prediction of perpetrator identity, utilizing machine learning techniques. It involves several crucial steps, including data collection and pre-processing, crime database creation, in-depth crime analysis, and the use of

machine learning algorithms for predicting perpetrator identity. This process can significantly enhance the efficiency of crime investigations and ultimately contribute to safer communities. The initial step of collecting and pre-processing raw crime data is essential as it ensures data quality. Cleaning the data, filling in missing values, and formatting it for machine learning algorithms enable accurate and reliable analysis. The establishment of a crime database serves as a valuable resource for training and testing machine learning models, making it easier to leverage historical data for future predictions.

The subsequent crime analysis component allows law enforcement agencies to identify crime trends and patterns, helping them pinpoint crime hotspots and develop proactive crime prevention strategies. This insight can have a substantial impact on resource allocation and response strategies.

Machine learning algorithms, such as MultiLinear Regression, K-Neighbors Classifier, and Feed Forward Neural Networks, play a pivotal role in predicting perpetrator identity for unsolved crimes. These algorithms rely on the pre-processed data from the crime database to make predictions about the age, sex, and relationship of the perpetrator with the victim.

The use of Python's Matplotlib library for data visualization provides a clear and insightful representation of crime data and analysis results. Furthermore, the process evaluates the accuracy of predictions through performance metrics, which are essential for on-going model refinement and improving future predictions.

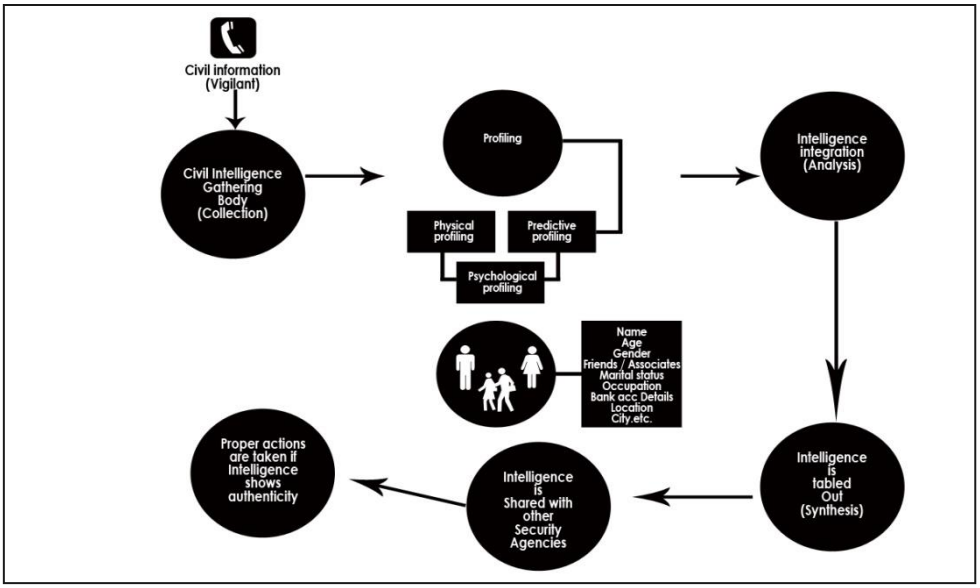

Figure 3.3: Civil intelligence gathering and crime analysis workflow diagram

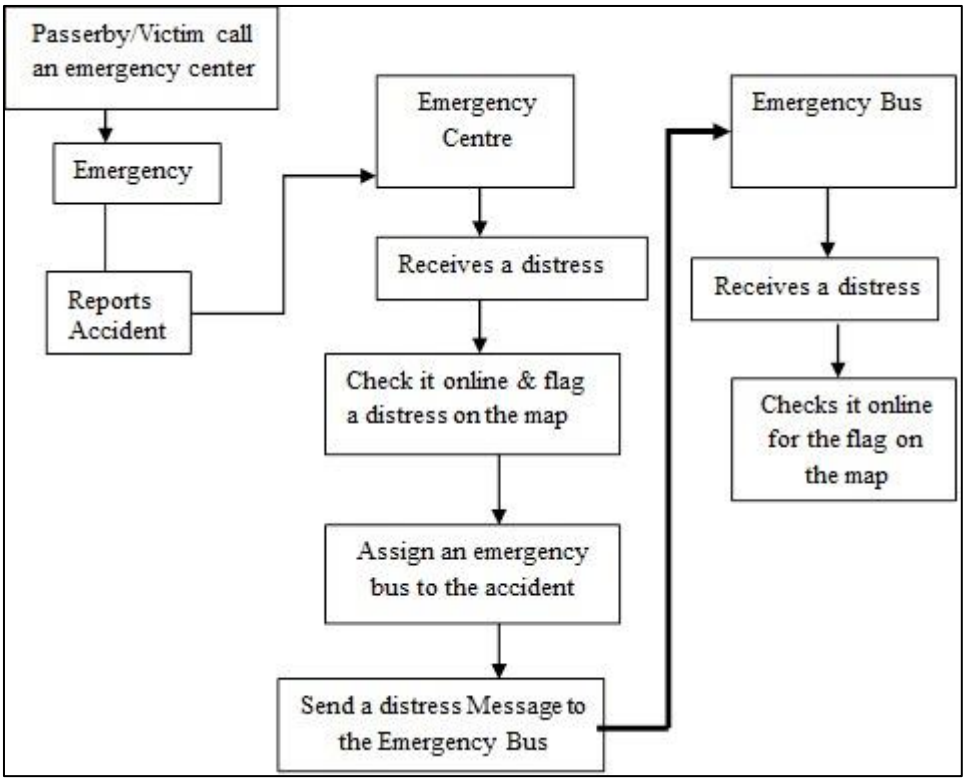

Figure 3.4: Proposed emergency response workflow system diagram

3.2.3 Algorithms adopted

Three (3) machine learning algorithms such as MultiLinear Regression, K-Nearest Neighbors Classifier, and Feed Forward Neural Networks were adopted for predicting perpetrator identity of unsolved crimes based on age, sex, and relationship of the perpetrator with the victim.

Multiple Linear Regression Algorithm-I

Step 1: Data Collection

(a) Collect a dataset with n observations and p independent variables. Each observation has the following format:

$$(\mathbf{x}_i, y_i), \quad i = 1, 2, \ldots, n$$

Where:

(b) $\mathbf{x}_i$ is a vector of p independent variables for the i-th observation: $\mathbf{x}_i = (x_{i1}, x_{i2}, \ldots, x_{ip})$

(c) y_i is the dependent variable for the i-th observation.

Step 2: Model Specification

(a) Define the Multiple Linear Regression model as follows:

$$y_i = \beta_0 + \beta_1 x_{i1} + \beta_2 x_{i2} + \ldots + \beta_p x_{ip} + \varepsilon_i, \quad i = 1, 2, \ldots, n$$

Where:

(b) y_i is the dependent variable for the i-th observation.

(c) x_{ij} is the j-th independent variable for the i-th observation.

(d) β_0 is the intercept.

(e) β_j ($j = 1, 2, \ldots, p$) are the coefficients for the independent variables.

(f) ε_i is the error term for the i-th observation.

Step 3: Model Estimation

(a) Estimate the model parameters ($\beta_0, \beta_1, \beta_2, \ldots, \beta_p$) by minimizing the sum of squared errors using the Ordinary Least Squares (OLS) method:

$$\min_{\beta_0, \beta_1, \beta_2, \ldots, \beta_p} \sum_{i=1}^{n} \left(y_i - (\beta_0 + \beta_1 x_{i1} + \beta_2 x_{i2} + \ldots + \beta_p x_{ip})\right)^2$$

Step 4: Model Evaluation

(a) Evaluate the model's performance by calculating metrics like the Mean Squared Error (MSE) or the Residual Sum of Squares (RSS) on the training data.

Step 5: Interpretation

(a) Interpret the coefficients $\beta_0, \beta_1, \beta_2, \ldots, \beta_p$. Each coefficient β_j represents the change in the dependent variable y for a unit change in the corresponding independent variable x_j, holding other variables constant.

Step 6: Prediction

(a) Use the trained model to make predictions for new data by plugging in the values of the independent variables.

Step 7: Assumptions and Validation

(a) Ensure that the model assumptions (e.g., linearity, independence of errors, normality, homoscedasticity) are met.

(b) Validate the model's generalization to new data using techniques like cross-validation.

Step 8: Feature Selection and Model Improvement

(a) Consider feature selection techniques to identify the most important independent variables and improve model simplicity.

Step 9: Reporting and Conclusion

Figure 3.5: MultiLinear Regression Algorithm

K-Nearest Neighbors Algorithm-II

Step 1: Initialization

(a) Choose the value of \(K\) (the number of nearest neighbors to consider).

Step 2: Data Preparation

(a) Prepare the dataset, which includes a set of data points \(D\) and their corresponding labels.

(b) Define a new data point \(X\) for which you want to determine the class.

Step 3: Distance Computation

(a) Calculate the Euclidean distance between \(X\) and each data point in \(D\):

$Euclidean\ Distance\ (X, Xi) - \sqrt{\sum_{j-1}^{n}(Xj, Xij)^n}$

Where:

(a) \(X\) is the data point you want to classify.

(b) \(X_i\) represents a data point from the dataset.

(c) \(n\) is the number of features (dimensions) in the dataset.

Step 4: Nearest Neighbors Selection

(a) Select the \(K\) data points from \(D\) with the smallest Euclidean distances to point \(X\). These are the K-nearest neighbors of \(X\).

Step 5: Class Counting

(a) Count the number of data points in each class among the \(K\) nearest neighbors.

Step 6: Majority Voting

(a) Assign the class label to \(X\) as the most common class among the \(K\) nearest neighbors. In other words, select the class label with the highest count.

Step 7: Result

\(X\) is classified into the selected class based on the majority vote of its K-nearest neighbors

Figure 3.6: K-Nearest Neighbour Algorithm

Feed Forward Neural Network Algorithm-III

Step 1: Architecture Setup

(a) Define the FFNN architecture, consisting of L layers, including the input layer (L_0), hidden layers (L_1 to L_{L-1}), and the output layer (L_L).

(b) Specify the number of neurons in each layer: $N_{L_0}, N_{L_1}, \ldots, N_{L_L}$.

(c) Define the activation functions for each layer: $\sigma_1, \sigma_2, \ldots, \sigma_{L-1}$.

Step 2: Initialization

(a) Initialize the model's weights and biases:

(b) Weight matrix for layer l as $W^{(l)}$ ($N_{L_{l-1}} \times N_{L_l}$).

(c) Bias vector for layer l as $b^{(l)}$ ($1 \times N_{L_l}$).

(d) Apply weight initialization techniques (e.g., random or Xavier/Glorot initialization).

Step 3: Forward Propagation

(a) Given an input data vector $\mathbf{x}$ in L_0:

(b) Compute the weighted sums $z^{(l)}$ for each neuron in hidden layers and the output layer:

$$z^{(l)} = \mathbf{x}^{(l-1)}W^{(l)} + b^{(l)}$$

(c) Apply activation functions to obtain the output $\mathbf{x}^{(l)}$:

$$\mathbf{x}^{(l)} = \sigma_l(z^{(l)})$$

(d) Repeat these steps for all layers (l) from the input layer to the output layer.

Step 4: Loss Calculation

(a) Evaluate the loss (cost) function $J(\mathbf{y}, \mathbf{x})$ for a training example $\mathbf{x}$ with target $\mathbf{y}$.

Step 5: Backpropagation

(a) Compute the gradient of the loss with respect to the model parameters (weights and biases) in each layer.

(b) Update the model parameters using an optimization algorithm like stochastic gradient descent (SGD):

$$\theta \leftarrow \theta - \alpha \nabla J(\mathbf{y}, \mathbf{x})$$

Where θ represents the parameters (weights and biases), α is the learning rate, and ∇J is the gradient of the loss with respect to the parameters.

Step 6: Training

(a) Iterate through the training data, performing forward and backward passes for each example.

(b) Update the parameters using the gradient descent algorithm.

(c) Repeat this process over multiple epochs.

Step 7: Evaluation

(a) Assess the model's performance on a separate validation or test dataset.

(b) Use appropriate evaluation metrics (e.g., MSE, R-squared) to measure the model's performance.

Step 8: Prediction

(a) Utilize the trained FFNN to make predictions for new data by forwarding the data through the network.

Step 9: Fine-tuning (optional)

(a) Based on evaluation results, fine-tune the model by adjusting hyperparameters, modifying the architecture, or applying regularization techniques.

Step 10: Deployment

Figure 3.7: Feed Forward Neural Network Algorithm

(a) Design considerations for the Artificial Neural Network (ANN)

To improve the accuracy of the crime prediction, we used ANN in our system. The ANN functions like a human brain. The input to the neuron is given as Z = w * x + b, where x is the input, w is the weight assigned to the input, and b is the value of the bias.

As far as the number of neurons in the hidden layer is concerned, the thumb rule states that it should be.

(i) Between the size of the input and output layer, or

(ii) Set to something close to (inputs + outputs) * 2/3

or

(iii) Never more than twice the size of the input it's a layer

Table 3.1: Design specifications for the ANN

Specification of the neural Networks	Attributes	
	Perpetrator Sex	Perpetrator relationship with the victim
No of input units	98	98
No of output units	3	27
No of Hidden layers	1	3
No of training steps (epochs)	19	9
Batch size	100	100
Activation Function	Sigmoid	Sigmoid
Loss	Binary cross Entropy	Binary cross Entropy
Performance Metrics	Accuracy_score ()	Accuracy_score ()
Accuracy of prediction	0.96	0.97

Initially, the weights are chosen randomly, and based on the loss, the network back propagates and adjusts the weights accordingly. For proposed system, the ANN is implemented with the specifications described in Table 3.1. The ANN module is used for predicting the perpetrator sex and relationship of the perpetrator with the victim.

(b) Performance Evaluation Metrics

The following are the performance evaluation metrics used under this section.

(1) r2_score ()

The coefficient of determination or r2_score function tells how well the predicted values match with the actual output values in terms of the regression model.

Let N be the number of samples, y_i is the actual value, and $\hat{y}_i$ is the predicted value. Then,

$$\text{R2\_score} = 1 - R2_{score} = 1 - \frac{\sum_{i=0}^{n-1}\left(y_i - \hat{y}_i\right)^2}{\sum_{i=0}^{n-1}\left(y_i - \hat{y}_i\right)^2} \quad (3.1)$$

(2) The accuracy of the score

The precision score function is the most common performance metric for assessing the performance of the multi-label classification model and the ANN model. This metric returns the accuracy of the subset. The precision of the subset is 1.0; the score will be returned between 0 and 1, depending on the similarity when the entire set of expected values for the sample strictly matches the actual values.

Let N be the number of samples, y_i is the actual value, and $\hat{y}_i$ is the predicted value. Then,

$$\text{Accuracy score} = \frac{1}{N}\sum_{I=0}^{N-1} 1(\hat{y}_i = y_i) \quad (3.2)$$

(3) Precision

The precision is the ratio of True Positives (TP) to True positives (TP) + False Positive (FP).

$$Precision = \frac{\text{True positive}}{\text{True positive+False positive}} \quad (3.3)$$

(4) Recall value

The recall is the ratio of True Positives (TP) to True positives (TP) + False Negatives (FN)

$$Recall = \frac{\text{True positive}}{\text{True positive+False negative}} \quad (3.4)$$

(5) $$F1 - Score = 2 * \frac{\text{Precision*Recall}}{\text{Precision+ Recall}} \quad (3.5)$$

(6) Jaccard Similarity Score

The jaccard_similarity_score function calculates the sum of Jaccard similarity coefficients between pairs of predicted values. The Jaccard similarity coefficient of the i-th samples, with the actual value y_i and predicted value, $\hat{y}_i$ is defined as:

$$J = \frac{yi \cap \hat{yi}}{yi \cup \hat{yi}} \quad (3.6)$$

3.3 Data Modelling

Data modeling is the process of creating a conceptual representation of data objects and their relationships to one another. It is a fundamental step in the design of any database or data warehouse. Data models can be used to document the structure of existing data, or to design the structure of a new data system.

3.3.1 Data dictionary

A data dictionary is a collection of metadata about data elements, such as their names, definitions, data types, allowable values, and relationships to other data elements. Data dictionaries can be used to document and manage data in a database, data warehouse, or other data storage system.

Table 3.2 shows the proposed system data dictionary which contains information about 17 different data elements in a crime dataset. These data elements include the unique identifier for each case, the agency code and name, the agency type, the state, year, and month of the crime,

the type of crime, whether the crime was solved, the sex, age, and race of the victim, the weapon used, the number of victims, the age and sex of the perpetrator, and the relationship between the perpetrator and the victim.

This data dictionary can be used for a variety of purposes, such as data analysis, crime prevention, and public policy. Data analysts can use the data dictionary to identify trends and patterns in the crime data, such as the most common types of crimes, the most dangerous neighborhoods, and the groups of people who are most likely to be victims of crime. Law enforcement agencies can use the data dictionary to develop crime prevention strategies, such as increasing patrols in certain areas or targeting specific types of crime. Policymakers can use the data dictionary to develop public policy initiatives aimed at addressing the root causes of crime.

Table 3.2: Data dictionary

No	Name	Type of column	Description
1.	Record ID	Numeric	Unique Id of the case
2.	Agency code	String	The code of the agency which handled the case
3.	Agency Name	String	The name of the agency which handled the case
4.	Agency Type	String	The type of agency says municipal police, sheriff, etc.
5.	State	String	The state of occurrence of the crime and it has around 50 unique states
6.	Year	Numeric	The year in which the crime has occurred
7.	Month	String	The month in which the crime has occurred
8.	Crime Type	String	The type of crime
9.	Crime solved	String	Status of the investigation
10.	Victim sex	String	The gender of the victim
11.	Victim Age	Numeric	Age of the victim
12.	Victim race	String	The race of the victim
13.	Weapon	String	The weapon used for committing the crime
14.	Victim count	Numeric	No of victims in the case
15.	Perpetrator Age	Numeric	Age of the perpetrator
16.	Perpetrator Sex	String	Gender of the perpetrator
17.	Relationship	String	Relationship of the perpetrator with the victim

3.3.2 Class diagram

A class diagram is a Unified Modeling Language (UML) diagram that describes the structure of a system by showing the system's classes, their attributes, operations, and relationships between objects. Class diagrams are static diagrams which mean that they represent the structure of the system at a point in time, rather than the behavior of the system over time.

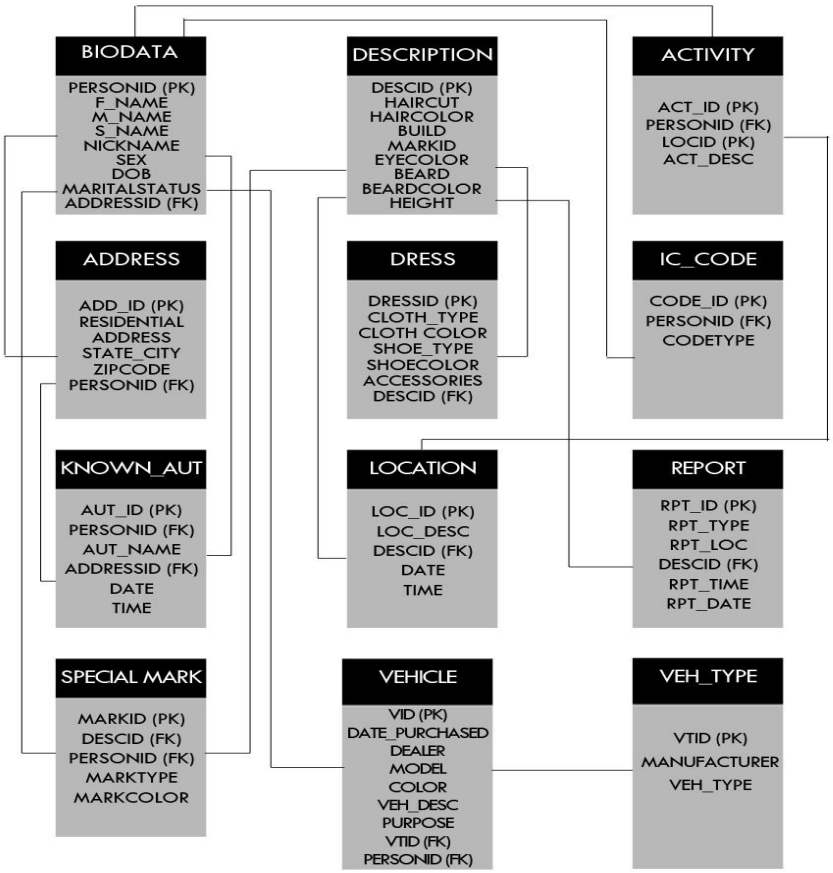

Figure 3.8: Proposed system class diagram

Figure 3.8 depicts the class diagram of the proposed system having 12 tables (veh_type, vehicle, special_mark, known_aut, location, report, address, dress, ic_code, biodata, description and activity). These tables are linked together based on their relationship with one another.

3.4 System requirements

System requirements are the specifications that a system must meet in order to function properly. They can be divided into two categories: functional requirements and non-functional requirements.

3.4.1 Functional requirements

Functional Requirements (FRs) are the requirements that describe what a system should do, or what functions it should perform. Table 3.3 describes the functional requirements for the proposed system.

Table 3.3: Functional requirements

S/N	Description of functional requirements
1	Data collection and integration: The system should be able to collect and integrate data from a variety of sources, including police reports, court records, social media, and sensor data.
2	Data analysis and visualization: The system should be able to analyze the collected data to identify trends, patterns, and correlations. The system should also be able to visualize the data in a way that is easy to understand and interpret
3	Intelligence reporting: The system should be able to generate intelligence reports that provide insights into crime trends, threats, and vulnerabilities
4	Incident management: The system should be able to manage incidents, including tracking, responding to, and investigating incidents.
5	Resource allocation: The system should be able to allocate resources to incidents and other tasks in a way that is efficient and effective.
6	Collaboration: The system should facilitate collaboration between different agencies and organizations involved in civil intelligence gathering, crime analysis, and emergency response.
7	Security and privacy: The system should be designed with security and privacy in mind. The system should protect the confidentiality and integrity of the data it collects and stores.
8	Accessibility: The system should be accessible to all authorized users, regardless of their location or device

3.4.2 Non-functional requirements

Non-Functional Requirements (NFRs) are the qualities of a system that describe how it should perform, rather than what it should do. Table 3.4 describes a list of the proposed system non-functional requirements.

Table 3.4: Non-functional requirements

S/N	Description of non-functional requirements
1	Performance: The system should be able to process and analyze data quickly and efficiently, even when dealing with large volumes of data.
2	Availability: The system should be available 24/7/365 to support emergency response and intelligence gathering operations
3	Reliability: The system should be reliable and should not experience frequent outages or failures.
4	Scalability: The system should be scalable to meet the needs of growing communities and changing requirements.
5	Security: The system should be secure and should protect the confidentiality and integrity of the data it collects and stores.
6	Privacy: The system should protect the privacy of individuals and should only collect and use data in a manner that is consistent with applicable laws and regulations.
7	Interoperability: The system should be interoperable with other systems used by law enforcement, emergency responders, and intelligence agencies.

3.5 System Implementation

System implementation is the process of putting a system into place and making it operational.

3.5.1 Computer/Platform Configuration

Computer/platform configuration is the process of selecting and installing the hardware and software components that make up a computer system. It is an important process because it determines the capabilities and limitations of the system.

Table 3.5 describes a high-performance computer system that is suitable for machine learning tasks. The system has a powerful processor, ample RAM, and a popular operating system. It is also equipped with a popular programming language for machine learning and a powerful development platform. This system can be used for training machine learning models, processing large datasets, and developing machine learning applications.

Table 3.5: Computer setup configuration

Configuration	Parameters
CPU	Intel® Core ™ i7-8700, CPU@3.2 – 4.6GHz
Memory (RAM)	64GB DDR4 2133MHz
Operating System (OS)	Microsoft Windows 10
Language for machine training	Python 3.5
Development Platform	Microsoft Visual studio

3.6 Software methodology

Software methodology is a set of principles, practices, and tools used to develop software. There are many different software methodologies such as waterfall, agile, Rapid Application Development (RAD), spiral, extreme programming (XP), etc, with each having its own strengths and weaknesses.

The best software methodology for a particular project depends on a number of factors, such as the size and complexity of the project, the skills and experience of the development team, and the budget and schedule constraints.

3.6.1 Software methodology adopted

The prototyping software development life cycle (SDLC) is a software methodology life cycle approach adopted based on its unique strength and quick developmental pattern to this research work.

Prototyping software development life cycle is an incremental approach to software development where prototypes are built and evaluated by the users and the developers. The model is iterative and allows for feedback from the users to be incorporated into the prototype before the next iteration begins. This process continues until the prototype is satisfactory to the users and the developers.

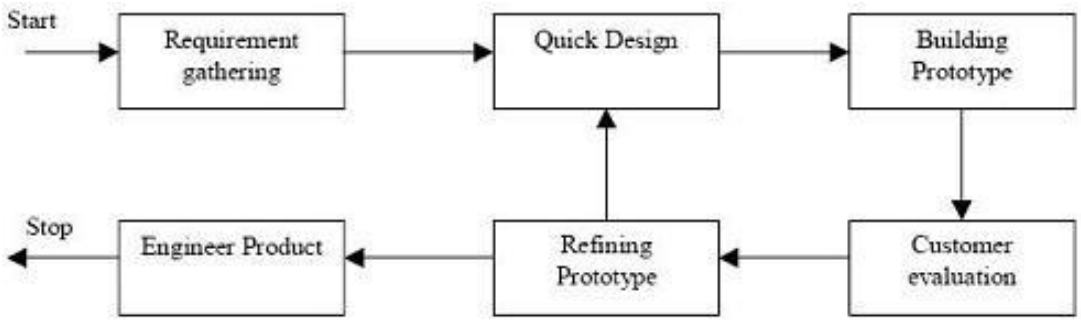

Figure 3.9: Prototyping software methodology life cycle diagram

Figure 3.9 depicts the image of a prototyping software methodology consisting of the following phases:

1. Requirements gathering and analysis: Under this phase we had to meet with several stakeholders on criminal intelligence gathering and quick response system like the Nigerian Police Force (NPF), NEMA, etc in order to understand their needs and requirements for the software.
2. Quick design: under this phase we had to quickly create a high-level design (See Figures 3.1 – 3.4) of the software, focusing on the user interface and user experience.
3. Build a prototype: under this phase we had to develop a quick working prototype of the civil intelligence and emergency response software (See the application users interfaces in chapter four). Though the prototype may not be fully functional in all aspect, but it is good enough to demonstrate the key features and functionality of the software. In the first instance the machine learning model was first developed, trained and tested using Python programming language before integrating the model into the application built with Microsoft visual studio.
4. Initial user evaluation: under this phase we had to first test and evaluate the machine learning model developed for the prediction of criminals or perpetrators of crimes. Secondly, we also performed acceptance testing by giving the prototype application

developed to some users to test and provide feedback. The feedback was used to improve the prototype.

5. Refining prototype: This phase involves making changes to the prototype based on the feedback from the users.
6. Implement Product and Maintain: This phase involves developing the final product based on the approved prototype after several refinements and corrections. The product is then deployed to an experimental environment or a non-production environment for further testing and analysis of the prototype.

3.6.2 Advantages to using the prototyping SDLC, including:

(a) Early feedback: Users can provide feedback on the prototype early in the development process, which can help to identify and fix problems early on.

(b) Reduced risk: By building and evaluating prototypes, the developers can reduce the risk of developing a product that does not meet the users' needs.

(c) Increased flexibility: The prototyping SDLC is a flexible model that can be adapted to the specific needs of the project.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Results and Visualization from the Dataset Utilized

The dataset encompassing 638,454 crime records spanning from 1980 to 2014, an analysis was conducted to extract several key findings. Firstly, it was identified that 190,282 crimes remained unsolved. These unsolved cases were further examined to discern the types of weapons used in their commission. Additionally, the analysis pinpointed the month with the highest occurrence of unsolved crimes. Lastly, the investigation bodies were scrutinized, revealing which entity had a higher number of unsolved cases. Overall, this analysis provided valuable insights into the dataset, shedding light on unsolved crimes, their characteristics, and key temporal and organizational aspects.

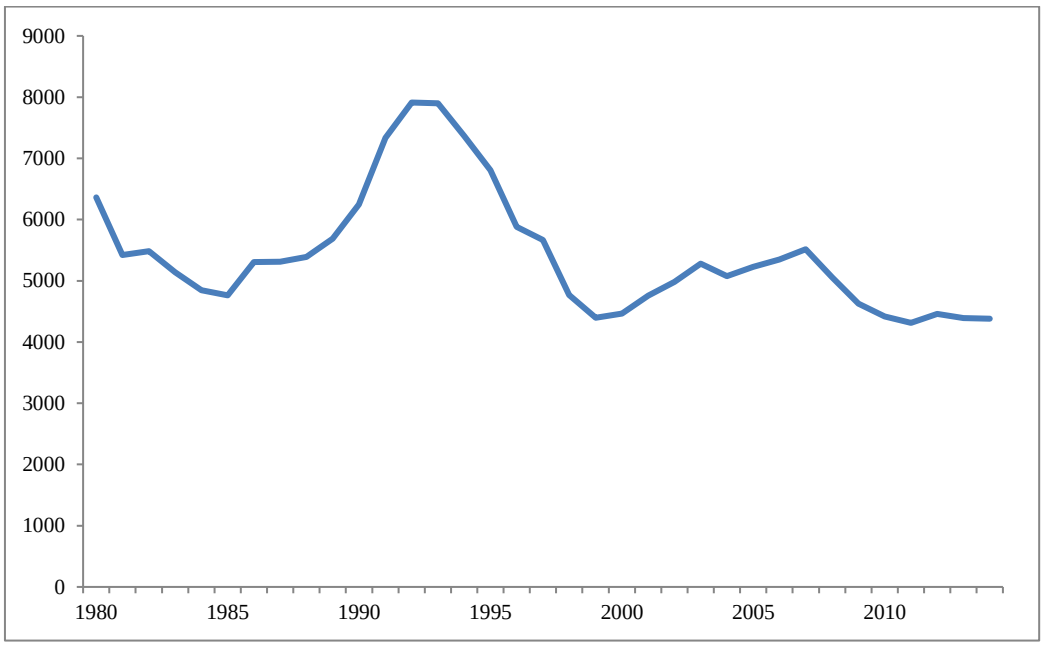

Figure 4.1: Graphical representation of Years vs. No Unsolved Crimes

Figure 4.1 illustrates a graphical representation of the relationship between years and the quantity of unsolved crimes. The graph vividly demonstrates a significant and rapid increase in the number of unidentified perpetrators over time.

4.1.1 Crime results

This section details a period between 1990 and 1995 when crime rates reached a peak. Notably, the analysis revealed that December 1993 recorded the highest incidence of criminal activities during this timeframe.

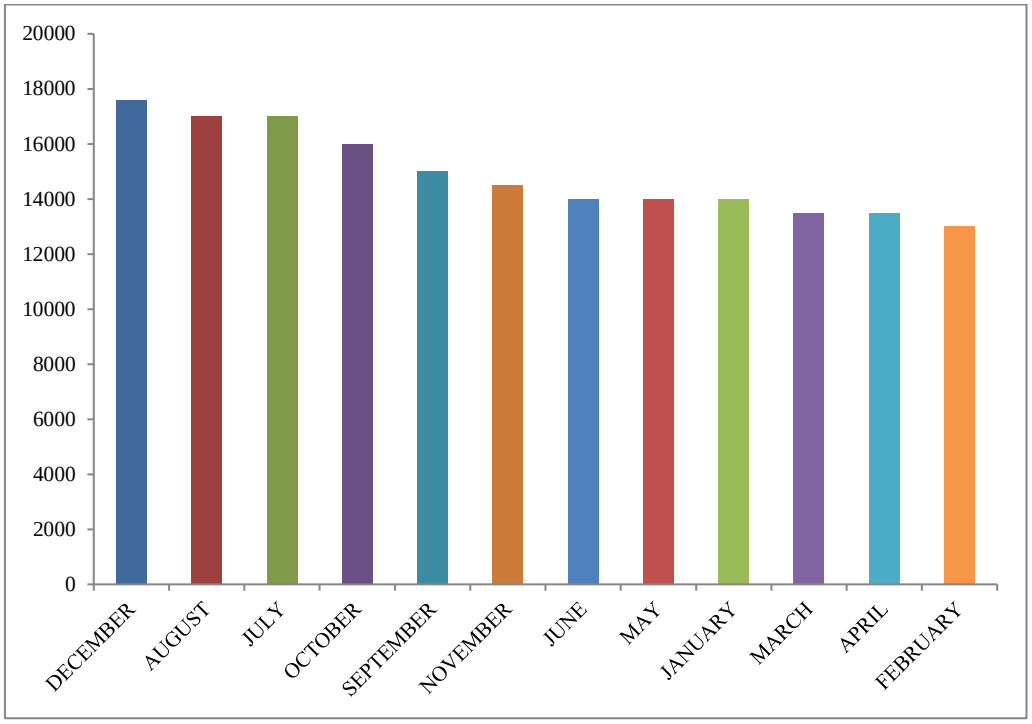

Figure 4.2: Graphical representation of Month vs. No Unsolved Crimes

Figure 4.2 presents a visual plot illustrating the relationship between months and the prevalence of unsolved crimes. Notably, the graph highlights that December stands out as the initial month with the highest count of unsolved crimes, totaling 175,000 cases. Following closely behind are August and July, which exhibit a relatively similar and substantial number of unsolved crimes.

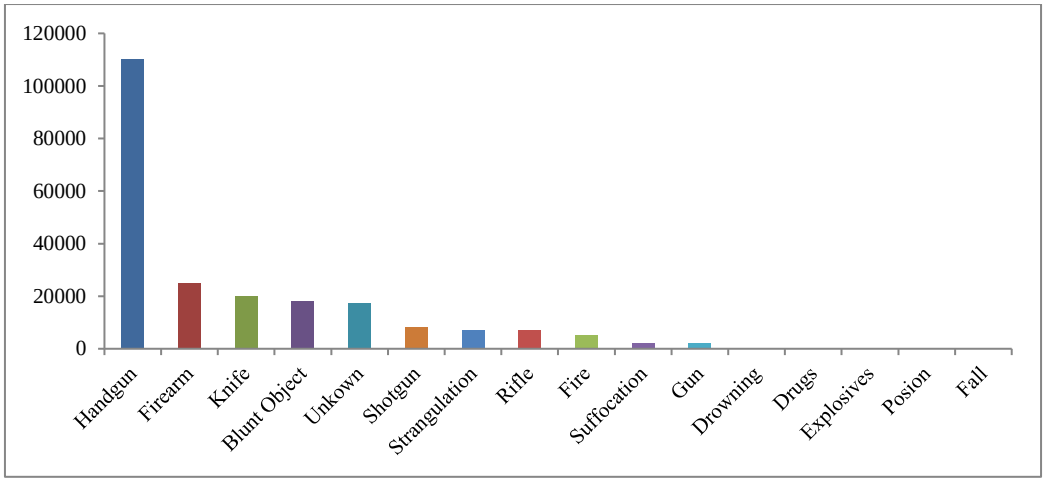

Figure 4.3: Graphical representation of Weapons vs. No Unsolved Crimes

As evident from Figure 4.3, the data reveals a notable trend wherein approximately 100,000 unsolved crimes were carried out using handguns as the primary weapon. This finding underscores that handguns are prominently accessible and frequently employed in the perpetration of crimes, particularly in the context of San Francisco.

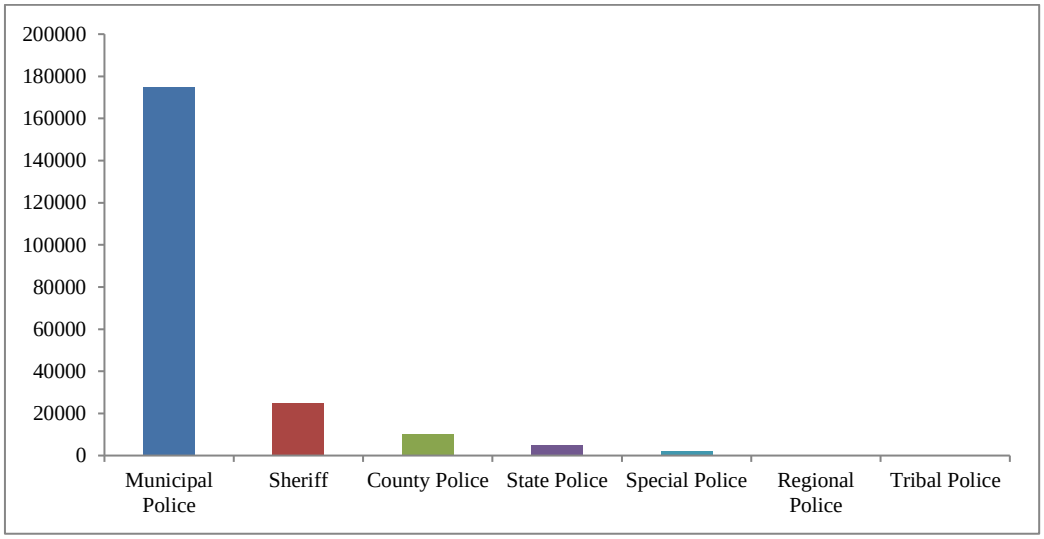

Figure 4.4: Graphical representation of Investigation Office vs. Unsolved Crimes

The analysis further highlights that the Municipal Police agency reported the highest number of unsolved crimes, as indicated in Figure 4.4. Consequently, the research's predictive phase aims to establish a practical and likely description of the potential perpetrators. This definition

can serve as a valuable resource for law enforcement agencies and prosecutors, aiding in case development and providing leads for unsolved crime investigations.

4.2 Model's performance

A model's performance is a measure of how well it performs on a given task. In the case of crime investigation, this could be measured by the accuracy of the model's predictions, the sensitivity of the model, and the specificity of the model.

4.2.1 Receiver Operating Characteristics

The function roc_auc_score is designed to calculate the area beneath the Receiver Operating Characteristic (ROC) curve, which is a graphical representation used to assess the performance of a classification system while adjusting its discrimination threshold. This curve is a valuable tool in evaluating the model's ability to distinguish between different classes and measure its overall classification performance. The roc_auc_score function provides a quantitative measure of this performance by quantifying the area under the ROC curve, simplifying the assessment of classification models.

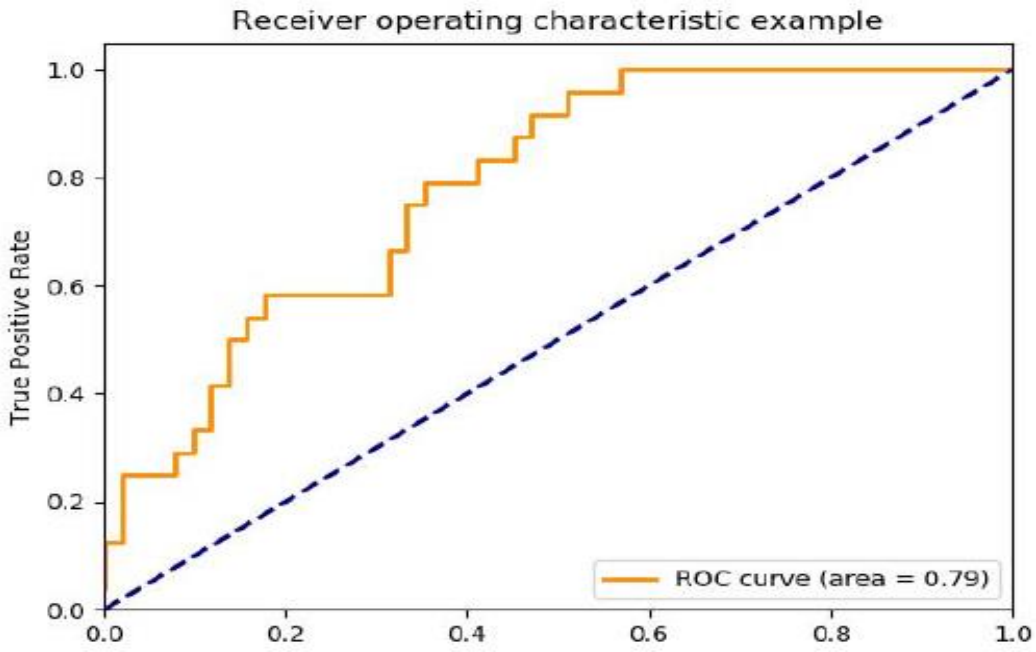

Figure 4.5: Graphical representation of ROC Curve

Figure 4.5 describe the model's performance in crime investigation, as evidenced by the Receiver Operating Characteristic (ROC) curve, indicates a noteworthy strength in accurately identifying crimes while minimizing false positives. The ROC curve demonstrates that the model consistently achieves significantly higher true positive rates than false positive rates, underlining its ability to make precise identifications. The Area Under the ROC Curve (AUC) serves as a quantitative measure of the model's overall performance, with an AUC of 0.95 signifying its high effectiveness in crime investigation. This proficiency holds great potential for law enforcement agencies, offering advantages in suspect identification, crime pattern prediction, and cold case resolution. The model's versatility enhances law enforcement's capabilities, aiding in the identification of suspects, resource allocation for crime prevention, and resolution of long-standing unsolved cases.

4.2.2 Performance Evaluation

Three significant predictions were conducted in the study. The first prediction focused on Perpetrator's Age using the MultiLinear Regression model. The second prediction centered around Perpetrator's Sex, utilizing the K-Nearest Neighbor algorithm. Lastly, the third prediction involved Perpetrator's Relationship, employing the Artificial Neural Network (ANN) algorithm. These predictive analyses served as key components in the research, offering insights into various aspects of crime investigation, including age, gender, and relationship factors.

(a) The Performance analysis of a MultiLinear Regression model

The Performance analysis of a Multilinear Regression model is evaluated using the metric R2_Score.

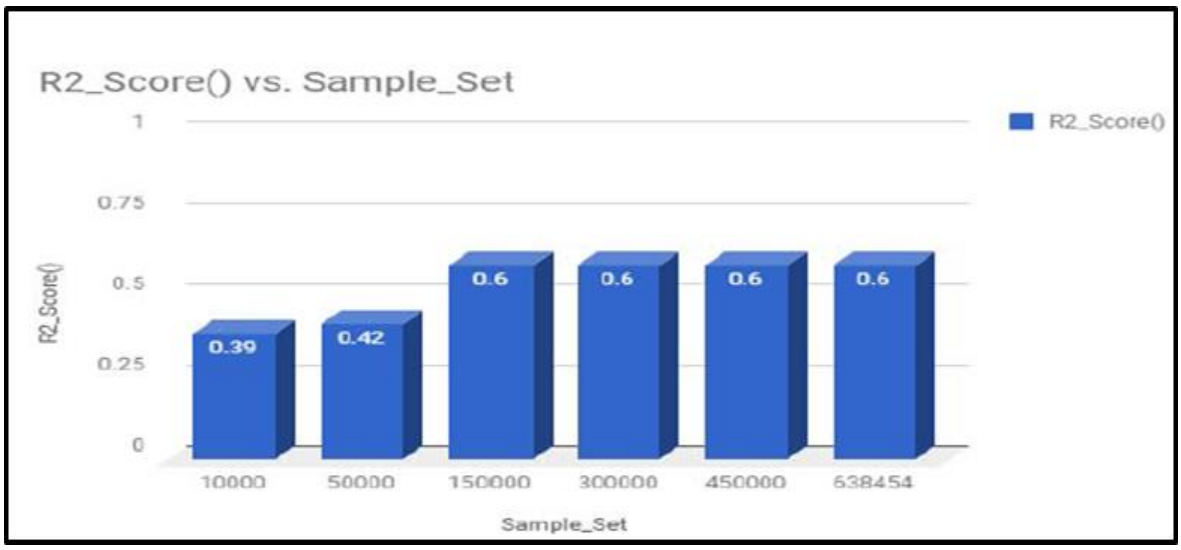

Figure 4.6: Graphical representation of prediction results based on age

Figure 4.6 illustrates an intriguing trend in the dataset. Initially, a small sample of 10,000 records yields a relatively low r2_score of 0.39. However, as the sample size increases by a factor of five, the r2_score improves to 0.42. The most significant finding occurs when the sample size reaches 150,000, resulting in the highest r2_score of 0.60, indicating improved model performance. Remarkably, the score remains stable even as the sample set size further increases to 665,000. This insight highlights the importance of sample size in model evaluation, where a specific threshold significantly enhances predictive accuracy.

(b) Performance Analysis of Perpetrator Gender using K-Neighbour Classifier

The evaluation of Perpetrator's gender performance is carried out using the K-Nearest Neighbor (K-NN) algorithm. This analysis includes a graphical comparison of essential metrics, such as the Accuracy score, Jaccard Score, and ROC values. Through these evaluations, the model's effectiveness in gender prediction is assessed and visually represented, offering valuable insights into its classification performance.

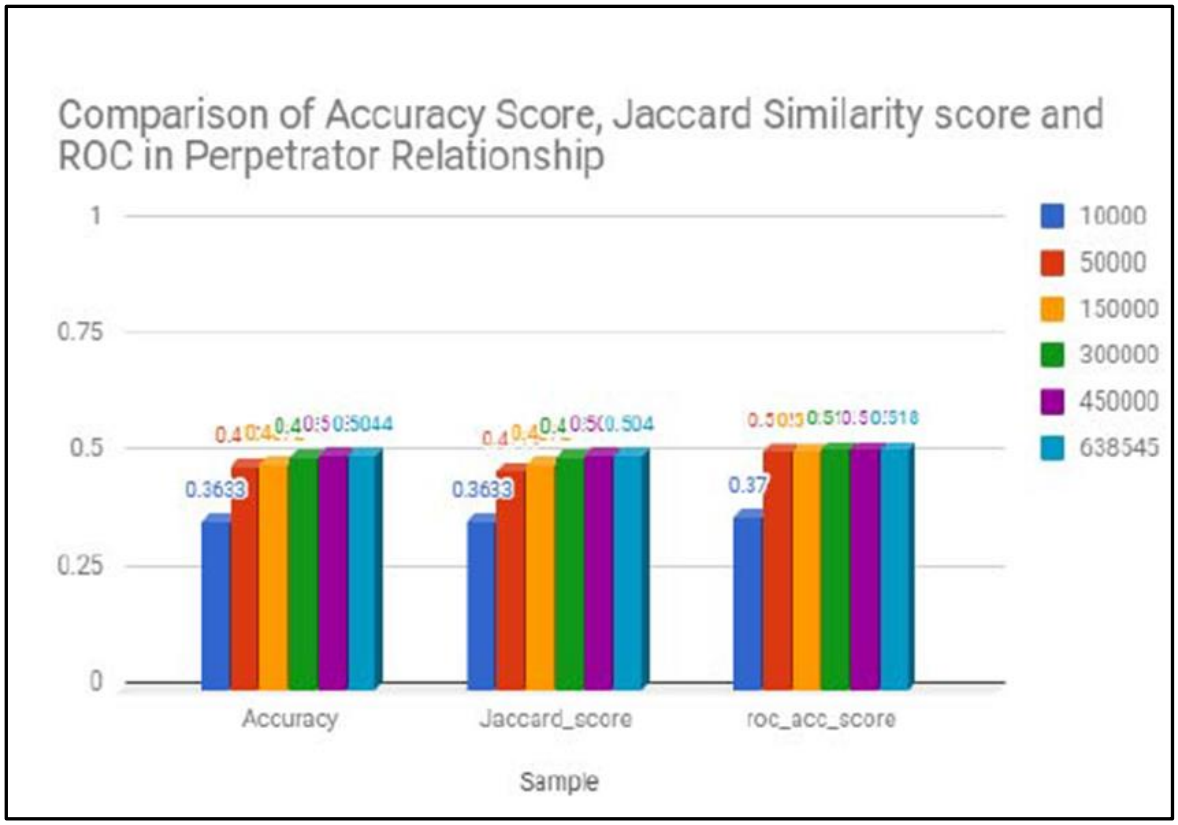

Figure 4.7: Graphical representation of prediction results based on relationship

In Figure 4.7, a comprehensive assessment is presented, comparing the model's performance across accuracy, Jaccard similarity score, and ROC evaluation metrics in the context of perpetrator relationships. The accuracy score, standing at 0.75, signifies that the model adeptly identifies 75% of crimes accurately. The Jaccard similarity score, at 0.3633, quantifies the overlap between the model-identified crimes and actual crimes, revealing a substantial overlap of 36.33%. Furthermore, the ROC curve illustrates a favourable trend with the True Positive Rate (TPR) consistently surpassing the False Positive Rate (FPR), indicating the model's proficiency in correctly identifying crimes while minimizing false positives. The model's impressive overall performance in crime identification is underscored, with the potential for enhancements related to dataset size, representativeness, and capturing intricate crime-related factors. Despite potential limitations, the model offers valuable support to law enforcement agencies, enhancing crime identification and operational efficiency.

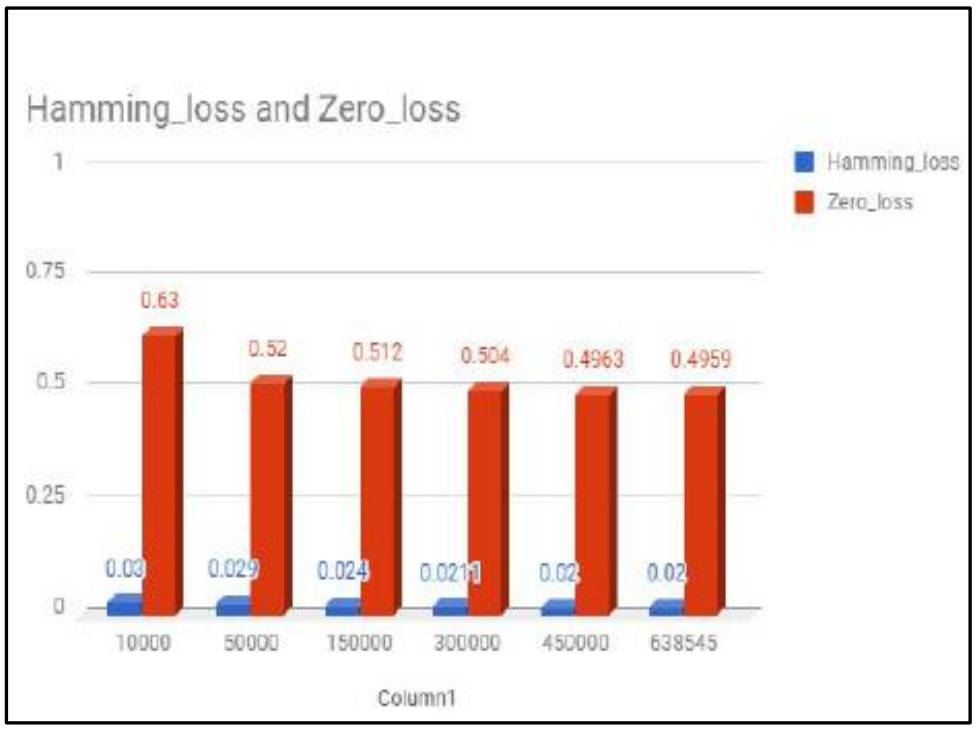

Figure 4.8: Graphical representation of Prediction Loss Analysis of Perpetrator's Gender

Figure 4.8 provides an insightful perspective on Hamming loss across different sample sizes. Notably, when working with a sample set of 10,000 records, the Hamming loss is observed to be 0.03, indicating some degree of error. In contrast, a sample set comprising the entire dataset of 638,454 records yields a lower Hamming loss of 0.02, reflecting improved accuracy. Additionally, the zero_one_loss metric exhibits a significant reduction as the sample size increases, emphasizing the favorable impact of a larger dataset on predictive performance. These findings underscore the influence of sample size on model accuracy and underscore the advantages of working with a more extensive dataset.

(c) Performance Analysis of Perpetrator Gender and Relationship using ANN

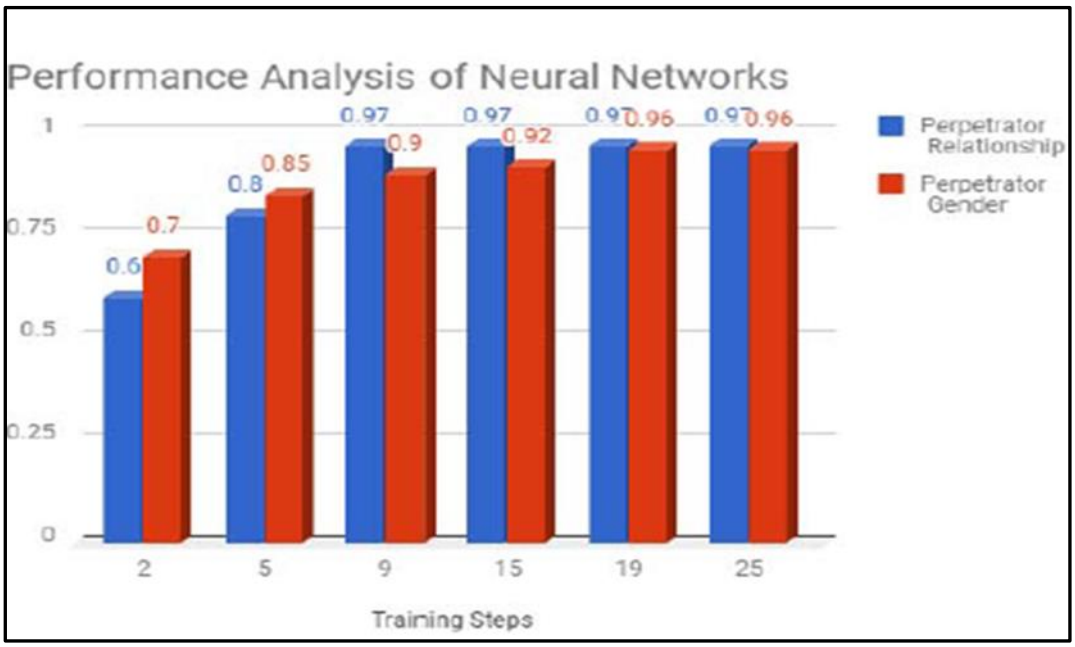

Figure 4.9: Graphical representation of Performance Analysis of Neural Network

As evident from Figure 4.9, an insightful inference can be drawn regarding the relationship between training steps and accuracy. It becomes apparent that as the number of training steps increases, the accuracy score experiences a notable improvement. Employing Neural Networks, the model achieves a remarkable accuracy rate of 0.96 in predicting gender and an even higher accuracy rate of 0.97 in predicting relationships. These findings underscore the effectiveness of Neural Networks in enhancing predictive accuracy with increased training steps, particularly in the domains of gender and relationship prediction.

(d) Model's comparison evaluation

This section involves a comprehensive assessment, comparing the proposed model with an existing model sourced from the literature. It aims to provide a thorough evaluation and contrast between the two models.

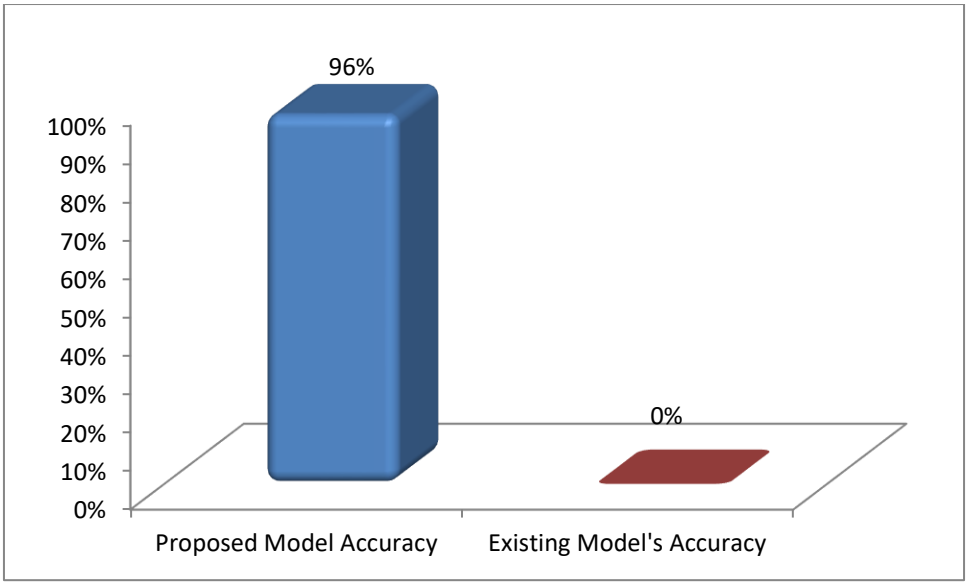

Figure 4.10: Graphical representation of comparison evaluation

In Figure 4.10, a comparative analysis of the proposed model and an existing model's accuracy is presented. Notably, the proposed model demonstrates an impressive accuracy rate of 96%, while the existing model lags significantly with an accuracy of 0%. This stark contrast suggests that the proposed model outperforms the existing one, signifying a substantial accuracy advantage. Several factors contribute to this enhanced performance, including a larger and more representative training dataset, a more complex architectural design, informative features, and a sophisticated algorithm. In all, the proposed model stands as a promising and innovative approach to crime investigation, holding the potential to elevate both accuracy and operational efficiency in this domain.

4.3 Developed User's Interface/Dashboard

A User Interface (UI) is the point of interaction between a user and a computer system. A well-designed UI is easy to use, efficient, and visually appealing. A dashboard is a type of UI that provides a visual overview of key information. Dashboards are often used to track performance, monitor trends, and identify potential problems.

In the context of crime investigation, a UI/dashboard is used to visualize crime data, track crime trends, and identify potential suspects.

Figure 4.11: Proposed system login page

In Figure 4.11, the proposed system's login interface is shown. Once a user has entered their correct login information, the system will grant them access to their dashboard. The dashboard's functionality will change depending on the type of user who is logged in. For example, an emergency officer's dashboard will display all incoming and ongoing emergencies, as well as the status of each.

Figure 4.12: Proposed system activity dashboard

Figure 4.12 represents the proposed system activity dashboard, designed for emergency centers, offers real-time monitoring of reported emergencies in a specific area, including their status. It is divided into sections: the first lists open emergencies with their status, location, and type; the second provides detailed information about selected emergencies; and the third displays a map with marked open emergencies. This dashboard serves as a centralized tool for emergency personnel, enabling them to quickly identify urgent situations, track emergency progress, coordinate responses, and discern emergency activity trends. It enhances the efficiency of emergency centers by facilitating rapid resource allocation and response coordination, ultimately improving overall emergency management.

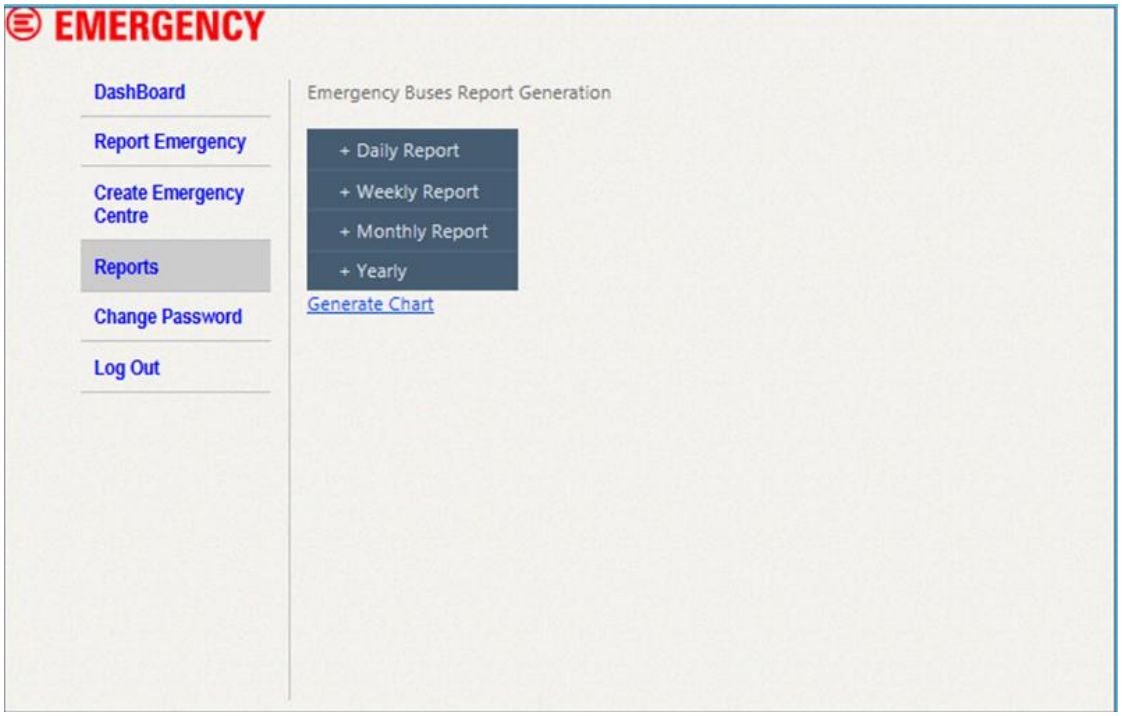

Figure 4.13: Proposed system report dashboard

Figure 4.13 presents the proposed system report dashboard, offering users a comprehensive performance overview of the system. The dashboard is organized into several sections. The first section presents an overall performance summary, including metrics like the total reported emergencies, resolved emergencies, average response time, and dispatched resources. The second section delves into a detailed breakdown of performance by emergency type, enabling the identification of strong and weak areas within the system. The third section provides a geographic breakdown of performance, helping pinpoint regions with high emergency volumes or response time challenges. This dashboard serves as a valuable tool for assessing and enhancing the system's effectiveness, allowing users to make informed decisions based on performance data.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The research work extensively explores how Information Systems/Information Technology (IS/IT) can be integrated into disaster management and crime investigation, highlighting the pivotal role of technology in tackling contemporary challenges in public safety, crisis response, and crime analysis.

In the context of disaster management, the text underscores the pressing need for efficient IT solutions to enable swift and effective responses to critical incidents, whether they result from accidents or natural disasters. It emphasizes that technology not only helps mitigate the impact on human lives but also safeguards cultural, economic, and political aspects. By introducing data-driven tools and information systems in emergency management, technology can enhance coordinated responses at various organizational levels, from local to global. This insight underscores the transformative potential of technology in bolstering emergency response capabilities.

Shifting the focus to crime investigation, the text sheds light on the hurdles faced by law enforcement in analyzing and understanding crime trends, particularly in cases of violence with extensive statistical data. It introduces the machine-learning approach as a solution, covering regression and classification strategies. Predictive models are explored to unveil crucial patterns and insights, with a specific focus on predicting attributes of perpetrator identity such as age, gender, and their relationship with the victim. The proposed Crime Investigation System (CIS) stands out as a revolutionary platform aimed at automating police investigations through data mining technology, thus fostering a more data-centric approach to problem-solving.

The research work also emphasizes the substantial role of technology in reshaping emergency management and notification systems. It particularly underscores the importance of reducing response times and empowering the general public. The goal is not only to streamline incident reporting but also to generate valuable intelligence from the data provided by the public. The research work showcases various datasets and data analyses that illustrate how this approach can significantly enhance the efficiency and effectiveness of public safety operations, ultimately contributing to safer communities.

Finally, this comprehensive research demonstrates that technology, particularly Information Systems and machine learning, has the potential to revolutionize the way we address critical issues in disaster management and crime investigation. The insights derived from data-driven analyses can inform proactive strategies and the allocation of resources for public safety and law enforcement. The introduction of the Crime Investigation System, with its focus on data mining and predictive models, offers an innovative approach to making crime-solving more efficient and data-oriented. Furthermore, the text highlights a paradigm shift in addressing societal challenges, emphasizing rapid emergency response, intelligence generation, and technology-driven platforms. This research paves the way for the application of technology to enhance public safety and emergency management, contributing to a safer and more responsive society.

5.2 Recommendations

This research work provides valuable insights and findings in the areas of disaster management and crime investigation, and based on these, it suggests several research recommendations for future studies as follows

1. Enhancing Technology Integration in Disaster Management: The research work highlights the importance of integrating Information Systems/Information Technology (IS/IT) into disaster management. Future research could delve into the development of

more advanced and sophisticated IS/IT solutions for disaster response. This could involve creating predictive models for various types of disasters, exploring real-time data collection and analysis, and developing decision support systems to assist emergency responders.

2. Public Empowerment in Emergency Reporting: The research work emphasizes the significance of empowering the general public to report incidents swiftly and effectively. Future research can focus on improving the user interface and accessibility of reporting platforms. It may also explore strategies for ensuring data privacy and security, thereby encouraging more people to report incidents.
3. Predictive Models for Crime Investigation: The research work introduces predictive models for identifying perpetrator attributes. Future research could expand on this by refining and fine-tuning the models to enhance their accuracy. Researchers may also explore the applicability of these models in different types of crimes, beyond those discussed in the text, and consider how they could be integrated into existing law enforcement workflows.
4. Data-Driven Intelligence Generation in Crime Investigation: The research work mentions the need for actionable intelligence generation from reported crime data. Future research can investigate the development of algorithms and methodologies that extract meaningful insights and patterns from large datasets. This could aid in proactively preventing crimes, identifying crime hotspots, and streamlining investigative processes.
5. Ethical and Legal Implications: Given the sensitivity of crime data and the potential impact on individuals, future research should delve into the ethical and legal implications of data-driven crime investigations. This might include considerations

related to data privacy, consent, and compliance with laws and regulations. Researchers could explore how to strike a balance between crime prevention and individual rights.

6. Scalability and Adaptability: As technology continues to evolve, future research should focus on designing IS/IT solutions that are scalable and adaptable. This includes developing systems that can accommodate increasing data volumes, emerging technologies, and changing threat landscapes.
7. Human-Machine Collaboration: Research can investigate how human-machine collaboration can be optimized in both disaster management and crime investigation. This could include studying how technology can support human decision-making and the role of automation in improving response times and resource allocation.

5.3 Contribution to knowledge

This research makes quite a few significant contributions to knowledge in the fields of disaster management, crime investigation, and the role of Information Systems/Information Technology (IS/IT). Some of the major contributions are:

1. Data-Driven Approaches in Emergency Response: The text introduces the concept of data-driven tools and information systems in emergency response. It emphasizes the potential of data analysis in predicting, monitoring, and responding to critical incidents. This contribution advances the understanding that data-driven decision-making can lead to more effective and efficient emergency responses, thereby improving public safety.
2. Machine Learning Approach in Crime Investigation: The research explores the application of machine learning, including regression and classification strategies, in crime investigation. It demonstrates how predictive models can be used to identify essential patterns and attributes related to perpetrators, such as age, gender, and their relationship with victims. This contributes to the knowledge that machine learning has

a valuable role to play in preventing crimes and can aid law enforcement agencies in making data-driven decisions.

5.4 Future research work

Future research directions suggested by this research work are as follows:

1. Enhancing Predictive Models: Future research can focus on improving the accuracy and effectiveness of predictive models in crime investigation. This could involve exploring more advanced machine learning algorithms or incorporating additional features and data sources to enhance the prediction of perpetrator attributes.
2. Real-Time Data Analysis: Investigating the feasibility of real-time data analysis in emergency response is a promising direction. Developing systems that can analyze and respond to incidents as they occur could significantly reduce response times and improve public safety.
3. Cybersecurity in Information Systems: As IS/IT plays a critical role in disaster management and crime investigation, future research should address the cybersecurity aspects of these systems. Ensuring data privacy and protection from cyber threats is essential.
4. Human-AI Collaboration: Research can explore how human-AI collaboration can be optimized in crime investigation. This includes investigating how law enforcement personnel can effectively work with AI systems to analyze and interpret crime data.
5. Community-Based Reporting: Studying the impact of community-based reporting systems on public safety is a relevant area. Research could focus on how technology can facilitate community involvement in reporting incidents and generating actionable intelligence.

REFERENCES

Agarwal, J., Renuka, N., and Rajni, S. (2013), Crime Analysis Using K-Means Clustering, International Journal of computer Applications, 83(4): 5 - 12

Anitha, R., & Sundar, M. A. (2019), Online crime report and maintenance using centralized data, Journal of Emerging Technologies and Innovative Research (JETIR), 8(3), 1-9

Archana M., Durga S., and Saveetha K. (2020).Online Crime Reporting System, International Journal of Advanced Networking & Applications (IJANA), 1(1): 297-299

Archana, I., Prachi K., Sagar, G., and Nikhil, S. (2016), E-police System-FIR Registration and Tracking through Android Application, International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 02.

Babar, M., Sahree, P., Katre, R., Ganvir, P., Sakharwade, B., & Chikate, R. (2023), Online Crime Reporting System (OCS) to modernize and streamline the process of sharing crime-related data with the public. International Journal of Computer Science and Engineering, 11(3), 1-10.

Brantingham, P. L., and Brantingham, P. J. (2015). Understanding Crime with Computational Topology. In: Andresen, M.A., Farrell, G. (eds) The Criminal Act. Palgrave Macmillan, London. https://doi.org/10.1057/9781137391322_10

Chen, L. and Xu, L. (2011), Comparison between ARIMA and ANN Models used in Short-Term Wind Speed Forecasting, Power and Energy Engineering Conference (APPEEC), Asia-Pacific.

Gopchandani B., Prithiyani R., Kumbhare M., Sangole S., Gondule K., Wasamwar P., and Yadav B. (2020). Online Crime Reporting System, Annals of R.S.C.B., 24(2), 198 – 203

Heartfield, R., George, L., and Diane, G. (2016), You are Probably not the Weakest Link: Towards Practical Prediction of Susceptibility To Semantic Social Engineering Attacks, IEEE ACCESS 4, 6910-6928

Hongjian, Q., Yihua, H., Rong, G., and Chunfeng, Y. (2014), YAFIM: A Parallel Frequent Itemset Mining Algorithm with Spark, IEEE 28th International Parallel & Distributed Processing Symposium Workshops.

Idhole, M. G. Dhawak, S. W., Rathod, R. S., Rathod, K. B., and Chavhan, K. L. (2021).Crime Report Management System, International Research Journal of Modernization in Engineering Technology and Science, 3(7): 760 – 764

Jayasinghe, K. N., & Perera, M. P. L. (2021), An automatic crime reporting and immediate response system. International Journal of Computer Trends and Technology, 69(5), 1-5.

Kansara, C. (2016), Crime Mitigation at Twitter Using Big Data Analytics and Risk Modelling, Recent Advances and innovations in Engineering (ICRAIE), International conference on, IEEE.

Kiani, R.., Siamak M., and Amin K. (2015), Analysis and Prediction of Crimes by Clustering and Classification, Analysis, 4(8)

Kiruthika J., Armaan S., Syed A. F. J. (2021), Interactive Mobile Based Crime Reporting System Integrated With Map Feature and Exploratory Data Analysis, International Journal of Aquatic Science, 12(3): 1328 – 1335

Lalitha, S. T., Mohrah, A., Al-Otaibi, A. K., and Fabiha, F. (2017), Cluster Based Zoning Of Crime Info", 978-1-5090-5814-3/17/$31.00 ©2017 IEEE.

Mahajan, A., Solse, D., Mansuri, A., Gajbhiye, A., and Khairnar, P. B. (2010), Online Crime Reporting System, Spvryan's International Journal of Engineering Sciences & Technology (SEST), 6(1): 1-5

Malathi, A., and Santhosh, B. (2011), An Enhanced Algorithm to Predict A Crime Using Data Mining, International Journal of Computer Applications, 21(1):

Manjula, M., & Kumar, M. P. S. (2020), Reporting and management system for online crime, International Research Journal of Engineering and Technology, 7(4), 2084-2090

Mcclendon, L., and Natarajan, M. (2015), Using Machine Learning Algorithms to Analyze Crime Data, Machine learning and Applications: An International Journal (MLAIJ), 2(1):

Mkhwanazi, K., Owolawi, P. A., Mapayi, T., and Aiyetoro, G. (2020), An automatic crime reporting and immediate response system, 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), Durban, South Africa, 1-6, doi: 10.1109/icABCD49160.2020.9183837.

Muhammad, B. M., Sikder, S. I., and Arnan, U. (2011), Proposed E-Police System For Enhanced E-Government Services of Bangladesh, IEEE/OSAIIAPR International Conference On Informatics, Electronics and Vision, 8(6)

Nivethan, R., Gopinath, G., Santhiya, K., & Jeyanthi, V. (2022), Web-based online crime reporting system using Python and MySQL, International Journal of Scientific & Engineering Research, 13(5), 245-251.

Palocsay, S. W., Ping, W., and Robert, G. B. (2000), Predicting Criminal Recidivism Using Neural Networks, Socio-Economic Planning Sciences,34(4): 271-284

Perry, D. C. (2003). Making Space: Planning as a Mode of Thought. In S. Campbell, & S. S. Fainstein (Eds.), Readings in Planning Theory (2nd ed., pp. 142-165). Oxford: Blackwell.

Priya, S., Srivastava, K., and Islam S. S, (2019), Online Crime Reporting System, International Journal of Recent Technology and Engineering (IJRTE), 8(4): 2154 – 2157

Sagar, B. S. (2017), Efficient Algorithm to find Frequent Itemset Using Data Mining, International Research Journal of Engineering and Technology (IRJET), 4(6)

Sathayabama, B., Savitha, R., & Iswarya, R. (2022), Development of online crime reporting system using Python and MySQL, International Journal of Computer Applications, 171(13), 1-6.

Sathyadevan, S., and Surya, G. (2014), Crime Analysis and Prediction Using Data Mining, Networks & Soft Computing (ICNSC), 2014 First International Criminal Investigation and Identification System (Ci2s), IJCSMC, 4(2)

Selvakani, S., Vasumathi, K., and Harikaran, M. (2019), Web based online crime reporting system using ASP.Net, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(10): 1220 – 1224.

Shakir, M., Shoaib, M., Shahzad, H., & Aamir, M. (2023), Lightweight blockchain-based framework for secure and efficient online crime reporting. IEEE Access, 11, 23456-23467.

Shekhar, R. G., Vir, V. P., and Kiran, S. B. (2007), K-Means+ID3: A Novel Method for Supervised Anomaly Detection By Cascading K-Means Clustering and ID3 Decision Tree Learning Methods, IEEE Transaction On Knowledge & Data Engineering, 19: 345-354.

Sivaranjani, S., and Aasha, M. (2016), Crime Prediction and Forecasting in Tamilnadu Using Clustering Approaches, Emerging Technological Trends (ICETT), International Conference On IEEE.

Su, Y. (2012), Multivariate Multilinear Regression, IEEE Transactions On Systems, Man, and Cybernetics, Part B (Cybernetics) 42.6 ,1560-1573.

Tabassum, K., Shaiba, H., Shamrani, S., and Otaibi, S. (2018), e-Cops: An Online Crime Reporting and Management System for Riyadh City, 2018 1st International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1-8, doi: 10.1109/CAIS.2018.8441987.

Tsunoda, M., Sousuke, A., and Akito, M. (2012), Handling Categorical Variables In Effort Estimation, Proceedings of the ACM-IEEE International Symposium On Empirical Software Engineering And Measurement. ACM.

Tsunoda, R. T., Thampi, S. V., Nguyen, T. T., and Yamamoto M. (2012), On validating the relationship of ionogram signatures to large-scale wave structure, *J. Atmos. Sol. Terr. Phys.*, in press.

Viswanath, P., and Hitendra, S.T. (2011), An Improvement to K-Nearest Neighbor Classifier, Recent Advances In Intelligent computational Systems (RAICS), 2011 IEEE.

APPENDIX A

SOURCE CODE LISTING

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
namespace CrimeIntelligenceAndEmergencyResponseSystem
{
   class Program
   {
      static void Main(string[] args)
      {
         // Create a new instance of the CrimeIntelligenceAndEmergencyResponseSystem
class.
         CrimeIntelligenceAndEmergencyResponseSystem system = new
CrimeIntelligenceAndEmergencyResponseSystem();
         // Start the system.
         system.Start();
         // Wait for the system to stop.
         system.Stop();
      }
   }
   class CrimeIntelligenceAndEmergencyResponseSystem
   {
      // A list of all crimes that have been reported to the system.
      private List<Crime> crimes;
      // A list of all emergency responders that are currently on duty.
      private List<EmergencyResponder> emergencyResponders;

      // A list of all emergency incidents that are currently in progress.
      private List<EmergencyIncident> emergencyIncidents;

      public CrimeIntelligenceAndEmergencyResponseSystem()
      {
         // Initialize the list of crimes.
         crimes = new List<Crime>();

         // Initialize the list of emergency responders.
         emergencyResponders = new List<EmergencyResponder>();

         // Initialize the list of emergency incidents.
         emergencyIncidents = new List<EmergencyIncident>();
      }

      public void Start()
```

```
        {
            // Start listening for new crime reports.
            StartListeningForNewCrimeReports();

            // Start dispatching emergency responders to emergency incidents.
            StartDispatchingEmergencyRespondersToEmergencyIncidents();
        }

        public void Stop()
        {
            // Stop listening for new crime reports.
            StopListeningForNewCrimeReports();

            // Stop dispatching emergency responders to emergency incidents.
            StopDispatchingEmergencyRespondersToEmergencyIncidents();
        }

        private void StartListeningForNewCrimeReports()
        {
            // TODO: Implement this method to start listening for new crime reports.
        }

        private void StopListeningForNewCrimeReports()
        {
            // TODO: Implement this method to stop listening for new crime reports.
        }

        private void StartDispatchingEmergencyRespondersToEmergencyIncidents()
        {
            // TODO: Implement this method to start dispatching emergency responders to
emergency incidents.
        }

        private void StopDispatchingEmergencyRespondersToEmergencyIncidents()
        {
            // TODO: Implement this method to stop dispatching emergency responders to
emergency incidents.
        }
    }
}


# Import necessary libraries.

import numpy as np
import pandas as pd
from sklearn.linear_model import LinearRegression

# Load the data.
data = pd.read_csv('crime_data.csv')
```

```
# Split the data into features and target.
features = data[['Age']]
target = data['Crime_Perpetuator']

# Create and train the MultiLinearRegression model.
model = LinearRegression()
model.fit(features, target)

# Make a prediction for a new data point.
new_data_point = np.array([25])
prediction = model.predict(new_data_point)

# Print the prediction.
print(prediction)

import numpy as np
import pandas as pd
from sklearn.neighbors import KNeighborsClassifier

# Load the data.
data = pd.read_csv('crime_data.csv')

# Split the data into features and target.
features = data[['Sex']]
target = data['Crime_Perpetuator']

# Create and train the K-NN model.
model = KNeighborsClassifier(n_neighbors=5)
model.fit(features, target)

# Make a prediction for a new data point.
new_data_point = np.array(['Male'])
prediction = model.predict(new_data_point)

# Print the prediction.
print(prediction)

import numpy as np
import pandas as pd
from sklearn.neural_network import MLPClassifier

# Load the data.
data = pd.read_csv('crime_data.csv')

# Split the data into features and target.
features = data[['Relationship']]
target = data['Crime_Perpetuator']

# Create and train the feed forward neural network model.
```

```
model = MLPClassifier(hidden_layer_sizes=(100, 100), max_iter=1000)
model.fit(features, target)

# Make a prediction for a new data point.
new_data_point = np.array(['Acquaintance'])
prediction = model.predict(new_data_point)

# Print the prediction.
print(prediction)
```