Cybercrime Monitoring System for Online Security Expert

Latifat Olubusayo BELLO
LUC/PG/000895

Being a MSc Thesis Submitted to the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo State, Nigeria.

In Partial Fulfillment of Requirements for the Award of Master of Science Degree(MSc) in computer Science

2022

Certification

This is to certify that Latifat Olubusayo BELLO with Matriculation Number LCU/PG/000895 carried out this research work titled 'Cybercrime Monitoring System for Forensic Expert' in the Department of Computer Science, Faculty of Natural and Applied Science, Lead City University, Ibadan, Oyo State, for the award of Master Degree (MSc) in Computer Science and that this has not been previously submitted.

……. …….
Dr. Wilson SAKPERE Date
Supervisor

……. …….
Dr. Wilson SAKPERE Date
Head of Department

Dedication

This project work is dedicated to Almighty Allah, the author and finisher of my faith who in His infinity mercy has kept me thus far.

Acknowledgement

My appreciation goes to the management and staff of Lead City University, Ibadan in general and the department of Computer Science in particular. I thank both the teaching and non-teaching staff for their support during the course of my programme.

My special thanks go to my supervisor Dr. Wilson Sakpere, Head of Computer Science Department, Lead City University, Ibadan, who despite his numerous engagements, find time to guide me and assisted me with useful inputs during the course of this research work. I want to express my gratitude to my amiable PG Coordinator Dr. Azeez Ajani Waheed. His staunch support and constant motivation really helped me a lot.

I am also greatly indebted to my loving and caring husband, Mr. Ademola Bello and my wonderful children: Monsurat Bello, Awwal Bello, Abdulhaqq Bello and Abdulmateen Bello for their kind support and understanding throughout the course of this study.

My gratitude also goes to all friends and colleagues who in one way or another has made this journey very memorable.

Finally, I appreciate the unquantifiable intellectual of several authors, scholars, and researchers whose works I've used. Although all the aforesaid people and institutions have helped in one way or other, all errors in this research report are solely mine if found.

Abstract

Cyberspace is increasingly attacked and there are limited means of mitigating this act. This is usually due to shifted degree of security features and management schemes within the cloud entity in cyberspace. The challenges are due to improvements in methods and the utilization of new technologies in committing crimes by criminals. The threat of cybercrime will continue to evolve and grow as criminals adapt to new security measures and take advantage of the changes in online behaviour. Hence, it is still challenging to identify and track down cybercriminals. This study focuses on implementing a cybercrime monitoring system for online data experts. After an in-depth understanding of cyber users' attacks, a possible solution could be proffered. A web application portal is designed using WordPress development tools that will serve as a platform to monitor and present possible vulnerabilities discovered. Tawk.to is integrated into the website for the implementation of real-life monitoring and My Structured Query Language is used as the database for storing and retrieval of information. This system will capture the digital signature of each piece of information sent to cyberspace, the user login parameter, the geographical location of the user, the Media Access Control address of the system used, the date, time and action carried out by the user while online. It will also aid cyber security experts in ascertaining the extent of activities carried out by cybercriminals in the domain. The result showed that the system can genuinely identify cyber users and their activities online.

Keyword: Cybercrime, Cyberspace, Cyber Criminals, Security Expert

Word Count: 247

Table of Contents

Content		Pages
Title Page		i
Certification		ii
Dedication		iii
Acknowledgement		iv
Abstract		v
Table of content		vi
List of Tables		ix
List of Figures		x
Chapter One: Introduction		
1.1	Background to the Study	1
1.2	Statement of the Problem	3
1.3	Aim and Objective of the Study	4
1.4	Research Components	4
1.5	Significant of the Study	5
1.6	Scope of the Study	5
1.7	Limitation of the Study	5
1.8	Operational Definition of Terms	6
	Endnotes	**7**

Chapter Two: Literature Review

2.1	Conceptual Review	8
2.1.1	Overview of Cybercrime and Cyber Security	10
2.1.2	Goals of Cyber Security	12
2.1.3	Brief History of Cybercrime	13
2.1.4	Definition of Cybercrime	13
2.1.5	Types of Cybercrime	14
2.1.6	Classification of Cybercrime	15
2.1.7	Cybercrime Monitoring System	17
2.1.8	Ethical Hacking	17
2.1.9	Benefit of Ethical Hacking	18
2.1.10	Phases of Ethical Hacking	18
2.1.11	Types of Hackers	22
2.1.12	Operating System Used by Hackers	24
2.1.13	Hacking Techniques Performed by Hackers	25
2.1.14	Types of Virus	27
2.1.15	Network Security	29
2.1.16	Network and Security Threat	30
2.1.17	Types of Network Security Attacks	30
2.1.18	Network Security Control	30
2.1.19	Network Protocols	31
2.1.20	Component of Network Protocol	31
2.1.21	Network Firewalls	31

2.1.22 Types of Firewalls 32

2.1.23 Network Traffic Monitoring 32

2.1.24 Cryptography 32

2.1.25 Network Attack 33

2.1.26 System Usability Scale (SUS) 36

2.2 Methodology Review 37

2.3 Review of Related Works 38

2.4 Summary of Gaps in Literature 51

Endnotes **53**

Chapter Three: Methodology

3.1 Research Approach 58

3.2 Requirement Specification 59

3.2.1 Software Implementation Tools 60

3.2.2 Hardware Specification 61

3.2.3 System Algorithm 62

3.3 System Design 65

3.4 Research Method 66

3.4.1 Input Design 67

3.4.2 Output Design 67

3.4.3 Database Design 67

3.4.4 Data Flow Diagram 68

Endnotes **71**

Chapter Four: Result and Discussion of Findings

4.1	Implementation	72
4.2	Testing	81
4.3	Performance Evaluation	82
4.3.1	System Usability Scale Questionnaire	82
4.3.2	Evaluation Using System Usability Scale(SUS)	83
4.3.3	SUS Scores for Participant of the Cybercrime Monitoring System	83
4.3.3.1	Lowest and Highest SUS Score	84
4.3.4	Usability Evaluation	84
4.3.5	Comparative Evaluation Analysis	86
	Endnote	**89**

Chapter Five:

5.1	Summary of Results	90
5.1.1	Conclusion	91
5.2	Contribution to Knowledge	91
5.5	suggested Areas for Research	92
	Bibliography	93
	Appendix	99
	Bio-data	138
	University Compliance Form	140

List of Tables

Tables	Title	Page
1.1	The Research Component of the Study	4
3.1	Database Output File	68
3.2	Specification of Program Modules	70
4.1	SUS Scores for Users of the Cybercrime Monitoring System Using 4-Point Likert Scale	83
4.2	Percentile, Grades, Adjectives and NPS to Describe Raw SUS Scores	85
4.3	SUS Scores for Cybercrime Monitoring System	86

List of Figures

Figures	Title	Page
3:1	System Flowchart of Website Monitoring system	64
3.2	System Architecture	65
3.3	Conceptual Diagram of the System	66
3.4	Data flow Diagram system Call Out function	69
3.5	Data flow Diagram Interaction in the Forensic Expert Interface	70
4.1	The Research Website	73
4.2	The Structure of the SQL Database	74
4.3	Tawk.to Integration to the Website	75
4.4	Administrator Email Linked to Tawk.to	76
4.5	Tawk.to Plugin Settings	78
4.6	Continuation of Tawk.to Plugin Settings	78
4.7	Cybercrime Monitoring Dashboard Login Portal	79
4.8	Two users detected on the Monitoring System	80
4.9	User Location and IP address Detected	81
4.10	Percentile Ranking for Common SUS Scores	85
4.11	Graphical Representation of the Comparative Analysis	98

Chapter One
Introduction

1.1 Background to the Study

Security of life and property is very vital to human life. The human life needs to be protected from critical and pervasive threats. The rate of security threats in the world is increasing at an exponential rate[1]. Due to this challenge, individuals and government have designed means to safeguard and protect themselves and citizens against such threats. These security threats may include physical and cybercrime threats[2].

Crime is a major issue in the world as at today. One of the factors influencing crime incidents is the technological advancement we are experiencing globally. Crime can include burglary, internet crime, theft and fraud. Usually people commit crime because of greed, anger, jealousy, revenge or pride and this affect other law abiding citizens[3]. More so, the commission of crime can lead to break down of organizational structure and governance which brings about the provision of security measures in every sphere of our life. To checkmate this menace, cyber security is critical.

Cyber security plays an important role in the area of Information Technology (IT). Protection of information has become an enormous problem in the present day. In the last 10 years, cyber security has become a major problem in Information Technology (IT) world. Individuals, organization and government are facing a lot of problems with cybercrime and different measures are taken to combat it. Despite these measures, Cyber security is still worrisome as

cybercrime assault can bring about everything from wholesale fraud to blackmailing big companies[4].

Cybercrime has been described as any crime that includes a computer and a network[5]. The computer may have been utilized in committing the crime, or it may be the target of a computer attack. A computer attack may be characterized as activities coordinated against computer system to disturb hardware operations, change processing control, or corrupt store data[6]. Any crime committed through computer networks are said to be cybercrimes. These offences are committed against individuals or groups of individuals with a criminal rationale to intentionally harm the reputation of the victim either directly or indirectly. This is done with the use of advanced media transmission system such as Internet, trojan, hacking, phishing, website cloning, copyright infringement and many more. In current scenario, the rate at which cybercrime is increasing is alarming and has led to an increase in security threats[7]. Criminals have taken advantage of the computer and internet to commit crime and remain anonymous, this makes cybercrime investigation to become a very complicated task as it is difficult to identify or trace cybercrime perpetrators[8]. These calls for a need of computer based monitoring systems for easy capture of evidence of intruders that compromise a network, in order to protect users from cyber terrorism.

It is worthy to note that cybercrime has been of great benefit to its Practitioners and their benefactors. While it has being dysfunctional to the victims of the scammers, their dependents, and to a large extent the society, it has become an image nightmare for most countries and their citizens. With the Internet creating limitless opportunities for commercial, social, and educational activities today, many businesses and personal transactions are conducted

electronically. For this reason, it is important that cybercrime should be taken seriously by industry experts and academics at large.

According to Information Systems Audit and Control Association (ISACA), Computer forensics is the collection, preservation, analysis and court presentation of computer related evidence''. In addition to civil and criminal jury trials, computer evidence often is presented in arbitration, administrative and mediation proceedings, congressional or government hearings and presentations to corporate management[9].

For the purpose of this study, computer forensics will be defined as the preservation, collection, identification, interpretation, analysis and presentation of digital evidence found using computers and digital storage for arbitration purposes.

This research deal with the implementation of cybercrime monitoring system for online security expert, a perfect way for tracking the activities of an account user and also for recovering digital evidence of crime committed in a computer system.

1.2 Statement of the Problem

Cybercrime is quite challenging due to shifted degree of security features and management scheme within the cloud entity in cyberspace[5]. The threat of cybercrime will continue to evolve and grow as criminals adapt to new security measures and take advantage of the changes to online behaviour[10]. Additionally, because of the nature of cybercrime, which is domiciled in cyber spaces, it is challenging for law enforcement agencies to find and prosecute cyber criminals[11]. Although several cyber monitoring systems have been in existence but it is still difficult to identify and track down cyber criminals. The problem is the cost implementation

and difficulty in integrating a Web Application Firewall to a website[12]. Also, to monitor large user group is tedious[13]. The humongous cost and difficulty in implementing an automated monitoring device discourage individuals and organizations in effectively monitoring their website. As a result of this, Cybercrime continues to increase. This has become a concern and still an open research study that will help in tracking the activities of internet users, for the recovery of digital evidence of cybercrime committed and also protect users from being hacked.

1.3 Aim and Objectives of the Study

The aim of this research work is to develop a cost effective model of Cybercrime Monitoring System for Online Security Expert.

The specific objectives of the study are to:

i. Develop a navigable and usable website suitable for monitoring threats.
ii. Integrate Tawk.to to the website.
iii. Evaluate the performance of the system.

1.4 Research Components

In view of the above aim and objectives, this study will address the following research components.

Table 1.1: The Research Components of the study

Research problem	Although several Cybercrime Monitoring Systems have been in existence, it is still difficult to identify cybercrime perpetrators.
Research Question	Why are the existing technology of Cybercrime Monitoring System expensive and difficult to implement.

Research Sub-question	Research Method	Objectives
How should a website be developed as a viable platform for cyber crime monitoring studies?	Software developement	To develop a navigable and usable website for cyber crime monitoring
How can websites be integrated to communicate seamlessly?	Experiment	To integrate "Tawk.to" to the website for effective monitoring
How should the system perform optimally?	Experiment and Evaluation	Evaluate the performance of the system.

1.5 Significance of the Study

This application when implemented will be able to monitor the activities of a computer user by taking screenshots of internet activities and capture the content of the index.dat file which will help forensic expert with substantial evidence to prosecute cyber criminals.

1.6 Scope of the Study

A web application portal is designed using WordPress development tools that will serve as a platform to monitor activity of users visiting the web Gateway. Tawk.to API is integrated into the hosted WordPress for the Implementation of real life Monitoring System that will aid forensic experts in their investigations and prosecution of cyber criminals.

1.7 Limitations of the Study

This study is limited to facial image identification of perpetretors when detected. Therefore, this may hinder law enforcement agency to identify the actual criminal. Also, criminal information is stored in a file format. Another limiting factor is that people see monitoring system as an intrusion to their privacy.

1.8 Operational Definition of Terms

Computer Forensic: Computer forensics is the application of investigative and analytical techniques to collect and store evidence from a particular computer device in a way that is suitable for presentation in the court of law.

Computer Network: Computer Network is a connection of computer devices that can exchange data and share resources with each other.

Crime: A crime is the intentional conduct of an act that is generally considered socially harmful or dangerous and is clearly defined, prohibited, and punishable by criminal law.

Cryptography: Cryptography is the art of keeping information private and secure by transforming it into form that unintended recipients cannot understand.

Cybercrime: Cybercrime is any criminal activity involving a computer, connected device, or network.

Cyber Security: Cybersecurity is the protection of computer systems and networks from disclosure of information, theft or damage of hardware, software, or electronic data, and interruption or misdirection of the services they provide.

Information Technology(IT): Information technology is the use of computers and communications to store, retrieve, and transmit information.

Internet: The Internet is a huge network that connects computers all over the world. The Internet allows people to share information and communicate from anywhere.

Security: Security is the protection or resistance from potential harm or other unwanted coercive changes caused by restricting the freedom of action of others.

Endnotes

1. S. Walker-Roberts, M. Hammoudeh, O. Aldabbas, M. Aydin & A. Dehghantanha, Threats on the Horizon: Understanding Security Threats in the Era of Cyber-physical Systems. *The Journal of Supercomputing*, *76*(4), 2020, pp.2643-2664.

2. A.T. Chatfield, & C.G. Reddick, A Framework for Internet of Things-Enabled Smart Government: A Case of IoT Cybersecurity Policies and Use Cases in US Federal Government. *Government Information Quarterly,* 36(2), 2019, pp.346-357.

3. P. Paul, & P.S. Aithal, Cyber Crime: Challenges, Issues, Recommendation and Suggestion in Indian Context. *International Journal of Advanced Trends in Engineering and Technology.(IJATET), 3*(1), 2018, pp.59-62.

4. K.A.L.A.K.U.N.T.L.A. Rohit, V.A. Babu, & K.R. Reddy, Cyber Security. *HOLISTICA–Journal of Business and Public Administration,* 10(2), 2019, pp.115-128.

5. M.A. Agana-correspondence, Cyber Crime Detection and Control Using the Cyber User Identification Model, 2015.

6. M. Aiken, R. Farr, & D. Witschi, Cyberchondria, Coronavirus, and Cybercrime: A Perfect Storm. *In Handbook of Research on Cyberchondria. Health Literacy, and the Role of Media in Society's Perception of Medical Information*, 2022, pp. 16-34. IGI Global.

7. F. Prakash, Sadawarti, H.K. & K. Baskar, 2019. Cyber Crime: Challenges and its Classification. *In International Multi-disciplinary Academic Research Conference IMARC,* 2019, pp. 2-4.

8. A.R., Javed, W., Ahmed, M., Alazab, Z., Jalil, K., Kifayat, & T.R., Gadekallu, A Comprehensive Survey on Computer Forensics: State-Of-The-Art, Tools, Techniques, Challenges, And Future Directions. IEEE Access, 2022.

9. D.V., Forte, Computer Forensics: Are You Qualified*?*. *Computer Fraud and Security*, (12),2008, pp.18-20.

10. M., Eddolls, Making Cybercrime Prevention The Highest Priority. *Network Security*, (8), 2016, pp.5-8.

11. M.K., Rogers, & K., Seigfried, The Future Of Computer Forensics: A Needs Analysis Survey. *Computers & Security*, *23*(1), 2004, pp.12-16.

12. I.C., Mihai, Procedure for Detecting Cybercrime Activities on Websites.*SITECH Craiova, Romania,* 2017, ISBN 978-606-11-6119-5

13. Y., Ba, Understanding Cybercrime and Developing a Monitoring. *Turku University of Appied Sciences*, 2017.

Chapter Two

Literature Review

This chapter aim to give a detailed review of the existing literature concerning existing cybercrime monitoring system and framework, how they handled different cases through the existing models, the gap in the existing model is being identified giving foundation of the need for a new model, and then conceptual model is presented. This chapter also provides the detailed overview on the evolution of cybercrime, goal of cybercrime and its challenges.

2.1 Conceptual Review

The issue of cybercrime has been discussed by many with various perspectives, most coming at it from different sides than the others. Cybercrimes have gone beyond conventional crimes and now threatening the national security of all nations, even advanced countries like the United States[1]. Cybercrime is an obstacle that can close the door to the progress of any company or nation. It has been described as one of the fastest growing criminal activities[2].

Cybercrime is a side product of Internet development. It is a crime that has stronger characteristics than conventional crimes. But the destruction that cybercrime causes is the same as conventional crime[3]. Cybercrime is complex and mostly committed in the remote locations which make it difficult for law enforcement agency. The Internet has more potential for good than evil. The contradictory nature of the Internet is one of its unexpected attributes. Initially, no one could have predicted that the Internet would one day become a veritable platform for globalized criminal activity.

Cybercrime cannot be treated under one umbrella, such attacks do occur in various forms and styles. Researchers basically categorize cyber-attacks into physical attacks, software-based attacks, network-based attacks, social engineering attacks and web application based attacks. Directly or indirectly, all the aforementioned attacks are done with a destructive intent[4].

1. **Physical Attacks**:These are types of attacks carried out without the use of the internet or network channel that are connecting devices or computers through the target. Physical attacks are further categorized into natural attacks such as natural disasters, man-made attacks such as theft of devices like computers, tablets, PDAs and other similar handheld devices. In the recent years, physical attacks are becoming more prominent as the attackers are now equipped with mini devices which if attached to the target machine could cause harm such as key loggers and microchips.

2. **Software-based Attack**:This is a type of attack that occurs on the software system and depends on the vulnerability of the software system. The attacks can either be launched at the application level, operating system level or protocol level. Their occurrence is often resulted by loopholes that are caused by human error and failure to improve or upgrade the software. The attackers use malicious codes to cause anomalies within the functional levels of the software. The major key players in software-based attacks include backdoor, rootkits, viruses, worms, Trojans, logic bombs, spyware, and macros.

3. **Network-based Attacks**: This is considered as one of the most advanced types of attacks. They are referred to as network-based because they involve a sophisticated use of the internet or network in conducting such attacks. The attacker hides behind his computer and remotely accesses other people's computers without having any physical contact. The most prominent network attacks include social network attacks, DoS attacks, session hijacking, wireless device attacks, evil twining, blue jacking, war driving and so on.

4. **Social Engineering Attack**: In explaining social engineering attack, researchers can say that, it is a method or technique used by the attacker to influence as well as persuade the target to reveal sensitive information about their personal life, workplace or something they might be working on which requires confidentiality. Furthermore, social engineering includes the use of tricks, deception, lies and maneuvers to gain the trust of the victims and later the attacker uses that information he or she gained and attack the victims. An example of information that could be stolen through social engineering includes credit card information, passwords, security policies, staff information and much more. However, some example of social engineering includes spoofing, impersonation, hoaxing, whaling and many more.

5. **Web Application Attacks:**Web application attacks are closely associated with the network-based attack. This is because web applications are usually hosted on the networks, even though some of the web apps work offline, yet they require a certain amount of connection to be able to synchronize with other components of the application such as the database and web server. So, web application attacks are the types of attack that allow the attacker to directly or indirectly cause damage to the web application using the network as the gateway to the target. Most web application attacks are carried out directly using IP addresses, DNS and DHCP servers, password directory, and database of the web application. Some of the attacks on web application include SQL injection, web duplicate, password attacks, and information theft such as credit card information, cross-site scripting, zero-day exploits, cookies and header manipulation.

2.1.1 Overview of Cybercrime and Cyber Security

As technology evolves, so does the definition of cyberspace, cybersecurity, and cybercrime. It has been argued that the definition needs to emphasize the peculiarities, knowledge, or use of

computer technology, as computer crime can cover all categories of crime. Cyberspace refers to an infinite space called the Internet. It refers to the interdependent network of information technology components that underlie many of today's communications technologies. Cybersecurity is a collection of tools, policies, security concepts, safeguards, policies, risk management approaches, countermeasures, training, best practices, assurances, and technologies that you can use to protect your cyber environment and your business and user assets. Organizational and user assets include all information transmitted and or stored in connected computing devices, personnel, infrastructure, applications, services, communication systems, and cyber environments[5]. Cybersecurity strives to ensure that the security characteristics of organizations and users' assets are achieved and maintained against the associated security risks of the cyber environment. Cyber security is a set of rules for protecting cyberspace. But as we become more dependent on cyberspace, we are undoubtedly facing new risks. Cybercrime refers to the scope of organized crime that targets both cyberspace and cybersecurity. Experienced cybercriminals and nation-states pose risks, especially to our economy and national security. Most of the economic vitality and national security depends on a large number of interdependent and important networks, systems, services, and resources known as cyberspace. Cyberspace has transformed the way we communicate, travel, power our homes, run our economy and use government services[6]. Cybersecurity is a set of technologies, processes, and practices designed to protect networks, computers, programs, and data from attacks, damage, or authorized access. In the context of computing or cyber, the word security simply means cyber security. Ensuring cybersecurity requires the collaborative efforts of both national citizens and national information systems. Threats that compromise cybersecurity go faster than we can catch up. Efforts cannot be focused on just one aspect of the violation. Doing so means negligence and the spread of other

aspects of the violation. As a result of this, cyber security breaches have to be tackled. Cybercrime refers to criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes nonmonetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet. Perhaps the most prominent form of cybercrime is identity theft, in which criminals use the Internet to steal personal information from other users. Criminal acts related to IT infrastructure such as illegal access (illegal access) and illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damage, erasure, deterioration, modification, or suppression of computer data), System tampering (computer system). Computer data entry, transmission, damage, deletion, deterioration, tampering, or suppression), device misuse, forgery (ID card theft) and computer fraud[7].

2.1.2 Goals of Cyber Security

The following are the goals of Cyber security[8].

1. To reduce the vulnerability of Information and Communication Technology (ICT) systems and networks.
2. To assist people and establishment develop and nurture a tradition of cyber security.
3. To collaborate with public, private and international entities to secure cyberspace.
4. To assist in understanding the current trends in Information Technology/cybercrime and develop efficient and effective solutions.
5. Availability.
6. Integrity, which might also additionally encompass authenticity and non-repudiation.

7. Confidentiality.

2.1.3 Brief History of Cybercrime

Cybercrime is a by-product of Internet development. Compared to traditional crime, cybercrime is new. However, the destruction caused by cybercrime is the same as traditional crime. But, surprisingly, the first documented cybercrime was in the early 1820s. A group of Joseph Marie Jacquard employees tried to thwart the loom invented by Jacquard for fear of losing work on the device. However, this is a completely different example from the cybercrime we generally know. Ten The cybercrime we are familiar with, which relies on networks and modern computers, was discovered after the development of modern computers and the ARPANET. The first viral program, called the creeper, was developed by Thomas in 1971. Thomas has no intention of engaging in criminal activity. Since then, countless malicious software has been developed. Despite the fact that malicious software has become more complex and subtle, its main functionality and purpose have remained largely unchanged.

In the information age, society has become more and more dependent on computers and the Internet. Even if the malicious software hasn't changed much, the area of the application has expanded significantly. The prosperity of cybercrime is the evolution of our society. Moreover, traditional crime is adapting to our world in the flood of the information age through digitalization. Drug trafficking, illegal arms trafficking, and other traditional criminal activities have begun offering e-services that reduce the chances of being caught[9].

2.1.4 Definition of Cybercrime

Cybercrime is defined as any crime conducted using computers or other communications tools to cause fear and anxiety to people or damage, harm and destroy properties[10]. Cybercrime is categories into two namely, computer-assisted and computer-focused cybercrime. Examples of computer-assisted cybercrime are child pornography, fraud, money laundering and cyber stalking, while examples of computer-focused cybercrime are hacking, phishing and website defacement.

2.1.5 Types of Cybercrime

Cybercrime can be divided into two types[11].

1. Crimes that directly target computer networks or devices, such as hacks, malware, computer viruses, and DanielofService (DoS).

• Hacking is an attempt by a cybercriminal, also known as a hacker, to gain unauthorized access to your computer. Some hackers do this only to gain popularity, while others do this to harm enemies and other agencies. "Black hats" and crackers are also hackers. Hackers are usually high-level programmers. Some companies hire hackers called "white hackers" to investigate system errors and fix them before they attack.

• Malware This stands for Malicious Software. Malware is a virus that can attach to computer programs and circulate on your network. Malware, viruses, or worms can be used interchangeably. This malware can occupy and destroy your computer's memory and can cause loss.

• DanielOfService (DOS) This is an attempt by a criminal to deny the service requested by the user. Cyber criminals send unlimited requests to the server, user cannot acquire their required offerings from the server. DOS generally assaults the high-profile websites, together with institution.

2. Crimes that make use of computer or internet to conduct the crime, for example Fraud, identity theft, cyberstalking, Phishing, Email spoofing, Password sniffing.

• Fraud: Fraud, often referred to as credit card fraud, can occur using credit card details. Don't forget to receive the receipt after your credit card. Be careful when purchasing online. Do not store your credit card number on online websites. This type of crime usually occurs when you drop a prepin debit / credit card. Criminals have the opportunity to shop until the card is blocked. • Theft of personal information. If someone else steals your personal information and impersonates you, it is called personal information theft. Cybercriminals used the victim's ID to access their accounts and other activities. Cybercriminals often take out loans with lost documents and inboxes.

• Cyberstalking: Cyberstalker can be run by virtually tracking victims on the Internet. They cannot physically hurt the victim, but they can torture them mentally. Cyberstalker usually monitors the victim's Internet activity and can threaten the victim. Victims of cyberstalking are usually women and children who are unfamiliar with the security measures when using the Internet.

• Phishing: Phishing means extracting sensitive data such as debit / credit card information. A combination of account username and password. This can be done by email spoofing and password eavesdropping. Phishers send victims fake emails pretending to be from their institution. When a victim accesses this email, phishing malware can attack your system and steal sensitive data.

2.1.6 Classification of Cybercrime

Cybercrime can broadly be classified into four major categories.

1. **Crime Against individuals**: Cybercrime committed against individuals includes sending child pornography, harassing individuals through the use of computers such as email, cyber defamation, hacking, vulgar disclosure, email spoofing, and IRC (Internet Relay Chat). Distributing obscene material, including malicious code, trafficking, distribution, posting, phishing, credit card fraud, and software copyright infringement, including crimes of the type, Internet blackmail. The potential damage to such crimes against individuals is rarely greater.

2. **Crime against Property**:This is another category of cybercrime against all forms of property. These crimes include computer vandalism (destroying the property of others), intellectual property crimes, intimidation, and salami attacks. This type of crime is usually widespread at financial institutions or for the purpose of committing financial crimes. An important feature of this type of crime is that the changes are so small that they are usually overlooked.

3. **Crime against Organization**:The third type of cybercrime classification is related to cybercrime against organizations. Cyber terrorism is a clear category of this type of crime. The growth of the Internet shows that cyberspace standards are being used by individuals and groups not only to put pressure on international governments, but also to terrorize national citizens. This crime manifests itself as terrorism when humans "hack" into government or military-controlled websites. There is a global agreement that all systems in the world can be cracked.

4. **Crime against Society**:The fourth type of cybercrime is related to cybercrime against society. This category includes types of counterfeiting, cyber terrorism, webjacking, obscene youth pollution, financial crimes, illegal item sales, network blackmail, cyber smuggling, data manipulation, salami attacks, and logical bomb crimes. Counterfeit banknotes, revenue stamps, marking sheets, etc. can be counterfeited using computers and high quality scanners and

printers. Webjack hackers can access and control someone else's website, even if they modify the content of the website to achieve political goals or make money.

2.1.7 Cybercrime Monitoring System

Cybercrime monitoring system is the process of continuously observing an Information Technology (IT) system in order to detect data breaches, cyber threat or other system vulnerability[12]. It is a proactive cybersecurity practice that can help individual, organization and IT team sift through cyber events to determine what will pose threat to their systems**.** An effective monitoring system is capable of alerting Information Technology (IT) Administrator of criminal attack and take predefined lock down action as appropriate. Monitoring cybersecurity is useful to confirm the functionality and effectiveness of implemented security measures.The monitoring process include collecting, analyzing and evaluating indicators and warnings on detecting and responding to security incidents[13].

2.1.8 Ethical Hacking

Ethical hacking is a legal way of breaking into an organization computers system to evaluate or test the intruder threat to their interests. It is also known as penetrating testing or pen testing. Ethical hackers perform their job in a professionally based on the directive of the client. It's among the most exciting Information Technology(IT) jobs any person can be involved in. Literally individual can get paid to keep up with the latest technology and get to break into computer system without the threat of being arrested. Most Organisation engaged in ethical hacking in order to identify vulnerabilities in their systems and instructions on how to remedy them. Ethical hackers typically possess variety of skills in information Technology(IT) and they

must be completely trustworthy. They are mostly computer and network expert that attacks the security systems of an organization on behalf of the owner[14].

2.1.9 Benefit of Ethical Hacking

The primary **benefit** of **ethical hacking** is to prevent data from being stolen and misused by malicious attackers, as well as:

- Discovering vulnerabilities from an attacker's POV so that weak points can be fixed.
- Implementing a secure network that prevents security breaches.
- Defending national security by protecting from terrorists
- Gaining the trust of customers and investors by their products and data
- Helping protect network with real world assessment

2.1.10 Phases of Ethical Hacking

Ethical hacking is the process of detecting vulnerabilities in an application, system, or organizational infrastructure that an attacker can use to exploit an individual or organization. They use this process to legally hack systems and scan for vulnerabilities to prevent cyberattacks and breaches. Ethical hackers follow the steps and thought processes of a malicious attacker to gain authorized access and test an organization's strategy and network. An attacker or ethical hacker follows the same five-step hacking process to compromise a network or system. The ethical hacking process begins with finding different ways to hack system, exploiting vulnerabilities, maintaining steady access to the system, and lastly, clearing one's tracks.

The five phases of ethical hacking are:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Hackers don't have to follow these phases in accordingly but, Perform these phases in the same order It can lead to accurate hacking[15].

1. Reconnaissance

Reconnaissance is the first step in ethical hacking, it is also known as the footprint or information gathering phase. The goal of this preparatory stage is to collect as much information as possible. Before launching an attack, the attacker collects all necessary information about the target. The data can include passwords, important employee details, and more. An attacker could use tools such as HTTPTrack to download the entire website to collect information about an individual, or use a search engine such as Maltego to search for an individual survey through various links, work profiles, news and more. Education is an important stage of ethical hacking. This helps identify what attacks can be launched and how likely your organization's system is against these attacks. The footprint collects data from areas such as:

TCP and UDP services

- Vulnerabilities
- Through specific IP addresses
- Host of a network

2. Scanning

The second step in the hacking technique is scanning. In this scan, the attacker attempts to find different ways to retrieve the target's information. Attackers look for information such as user accounts, credentials, and IP addresses. This ethical hacking procedure consists of finding an easy and quick way to access the network and find information. Tools such as dialers, port scanners, network mappers, sweepers, and vulnerability scanners are used in the scan phase to scan data and records. Ethical hacking methodologies use four different types of scanning techniques. They are:

1. **Vulnerability Scanning:** This scanning method targets target vulnerabilities and vulnerabilities and attempts to exploit those vulnerabilities in various ways. This is done using automated tools such as Netsparker, OpenVAS, and Nmap.

2. **Port Ccan**: To do this, use a port scanner, dialer, and other data collection tools or software to listen to open TCP and UDP ports, run services, and operate the system on the target host. Is included. Intrusion testers or attackers use these scans to find open doors to access your organization's systems.

3. **Network Scan**: This method is used to detect active devices on your network and find ways to exploit your network. This could be an organizational network where all employee systems are connected to a single network. Ethical hackers use network scans to identify vulnerabilities and strengthen your organization's network by opening doors.

3. Gaining Access

The next step in hacking is to use the means an attacker needs to gain unauthorized access to a targeted system, application, or network. An attacker could use a variety of tools and methods to gain access to and break into your system. This hacking phase attempts to break into and

exploit your system by downloading malicious software and applications, stealing sensitive information, gaining unauthorized access, and demanding a ransom. Metasploit is one of the most widely used tools for gaining access and social engineering. get is a common attack that exploits the target. Ethical hackers and intrusion testers can protect potential entry points, ensure that all systems and applications are password protected, and protect network infrastructure with firewalls. You can send fake social engineering emails to your employees to identify them who are likely to be victims of cyberattacks.

4. Maintaining Access

Once an attacker has access to the targeted system, the attacker will do its best to maintain that access. During this phase, hackers continually exploit the system to launch DDoS attacks, use the hijacked system as a boot pad, or steal the entire database. Backdoors and Trojan horses are tools used to exploit vulnerable systems and steal credentials, important records, and more. In this phase, the attacker aims to maintain unauthorized access until the user completes malicious activity without their knowledge. Ethical hackers and intrusion testers can take advantage of this stage by scanning the entire organization's infrastructure to capture malicious activity and find the root cause of preventing system abuse.

5. Clearing Track

In the final stages of ethical hacking, hackers need to pave the way for themselves because they don't want the attackers to be caught. This procedure ensures that the attacker leaves no traceable clues or evidence. This is very important because ethical hackers need to stay connected within the system without being identified by incident response or forensic teams. This includes editing, corrupting, or deleting logs or registry values. Attackers also remove or

uninstall folders, applications, and software, or ensure that modified files are restored to their original values.

Ethical hackers can use the following ways to erase their tracks:

1. Using reverse HTTP Shells
2. Deleting cache and history to erase the digital footprint

Using ICMP (Internet Control Message Protocol) Tunnel

Ethical Hacking are categorised into five types

- Web Application Hacking
- System Hacking
- Web Server Hacking
- Hacking wireless Network
- Social Engineering

2.1.11 Types of Hacker

1. **White Hat Hackers**: The famous name for white hackers is "ethical hackers". They have in-depth knowledge of network protocols, software and hardware features, and professionally trained administrators. As all rights as an administrator. They perform penetration testing and vulnerability analysis. They work for the organization and are well paid. From an intruder's perspective, they are always thinking about what they can do to infect the targeted system, gain unauthorized access, and modify sensitive information. They follow the same procedure to see what the negative effects are. If the result is significant, they report the threat and it is presented to higher authorities and also, find a remedy.

2. **Black Hat Hackers**: Black hackers are commonly known as crackers. They have skills similar to white hackers. But they are using their abilities for the wrong purpose. Their main

purpose is to steal data through unauthorized access. They primarily target corporate data, invade privacy, damage systems, and block network communication channels.

3. **Gray Hat Hackers**: Gray hat hackers are a hybrid of white hackers and black hackers. They hack without the permission of the owner. Their main purpose is to exploit system vulnerabilities and warn owners of problems. They hack for fun and win recognition and small prizes from the owners. They even offered high-paying jobs from their owners. But you are not looking for a job.

4. **Red Hat Hackers**: They are a combination of white and black hackers. They are typically targeted at top-level channels such as government agencies, secret centers, or those that fall under the category of sensitive information.

5. **Blue Hat Hackers**: They are outsider. Security experts are enthusiastically invited by well-known companies to identify vulnerabilities and black security holes before releasing software products to the global market.

6. **Elite Hat Hackers**: They are actually at the forefront of both computing and networking channels. Newly discovered exploits are the first to be revealed among these hackers.

7. **Script Kiddie**: They are immature, inexperienced and unskilled hackers. People who access the system using off-the-shelf automated tools developed and programmed by others are usually called children. Someone who has little understanding of the underlying concept.

8. **Neophyte**: They are "beginners". Who has no prior knowledge of hacking? They are not as skilled as the children in the script. However, script kiddies are much better than newborns. Neophyte needs some time to develop its skills in order to be able to compete with Script Kiddie.

9. **Hacktivist**: They use tools and technology to disseminate secret, religious or political messages to the public. This is typically done by hijacking the website and leaving a warning message on the hijacked website. The main target websites are government websites.

10. **Phreaker**: They are Telecommunication network hackers. A person who illegally uses the telephony system to make a call without paying a fee. Their main reason is that they remain unknown. In addition, people threatened personal use and earned some money[16].

2.1.12 Operating System used by Hackers

BackTrack: This is a custom distribution designed for all levels of security testing, from beginners to professionals. It is a very comprehensive collection of tools such as wireless hacking, server exploits, web application evaluation, social engineering and more, available in a single Linux distribution.

Kali Linux: it is developed, managed and funded by Offensive Security Ltd. Kali is a Debian-derived Linux distribution specifically designed for digital forensics and penetration testing. This is one of the best operating systems for hackers.

Parrot-Sec Forensic Operating System: it is primarily a combination of Debian GNU / Linux with the Frozen box operating system and Kali Linux, used to perform all kinds of vulnerability analysis and mitigation, computer forensics, and anonymous surfing.

Cyborg Hawk Linux: It is a maximum potent, properly controlled Ubuntu-primarily based totally Penetration Testing Distro created through the group of Ztrela Knowledge Solutions Pvt.

Ltd. Specially Build for moral hackers and cybersecurity specialists who also are referred to as Penetration testers.

Back-Box: Back-Box is an Ubuntu-primarily based totally Linux distribution. It incorporates extra than 70 tools. It facilitates moral hackers and penetration testers in protection assessments. The important benefit is that its repositories get up to date at ordinary intervals.

Samurai Web Testing Framework: Its framework primarily based totally on Ubuntu 9.04. Moreover, absolutely Open Source. It incorporates masses of Web evaluation and exploitation tools. Mainly makes a speciality of trying out the safety of net applications.

Network Security Toolkit NST Primarily Based Totally on Fedora: It as a hundred twenty five open supply protection tools. Its Main Objectives are to perform community visitors analysis, intrusion detection, community scanning, and protection patching.

BlackArch: Linux BlackArch is a Linux-based distribution. Contains over 1600 tools. It is also valued as the first option for conducting web and application-based security testing.

GnackTrack: GnackTrack is an Ubuntu-based Linux distribution and open source. It features a GUI-based GNOME desktop with a simple user interface. In addition, it includes various essential tools such as Metaspoilt, Armitage and wa3f[17].

2.1.13 Hacking Techniques Performed by Hackers

Bait-and-switch: In this method, an attacker buys advertising space on your website. Than Display is a unique ad that uses catchy words to trick victims into clicking on banner ads. After clicking on an ad, the user may be redirected to a page infected with malware. Victims may see a pop-up asking them to install the software. If the victim installs the software on the hub they are working on, it is easy for hackers to remotely access the laptop / computer without the user's permission. Hackers use this technique to threaten hackers and make money.

Cookie theft: Cookies store details such as usernames, passwords, credit cards, etc. for the various websites you visit. If a hacker has access to these cookies, the hacker can authenticate himself as a real user and access the admin panel. This attack is also known as sidejacking or session hijacking. Most often it happens on a website. Do not add SSL (https). The traditional way to carry out this attack is to trick the user's IP packet through the attacker's computer. By monitoring packet flow, an attacker can gain unauthorized access to a real user.

ClickJacking: Another name for ClickJacking attacks is UIRedress. This is a way to fool Internet users. With this technique, the hacker hides the actual user interface that the victim is trying to access. This behavior can be seen on movie websites, software download websites, or torrent websites. This technique is used to redirect users to other web pages to get a view of the website and make money from ads. You may also be asked to enter details to access downloadable content. Once the user enters the details, it's easy for a hacker to steal the information.

Keylogger: This is a simple software designed primarily for logging keystrokes and keystrokes to log files. This log file contains all non-sensitive and non-sensitive information such as usernames, passwords, bank details, and more. For this reason, most payment gateways or bank websites require users to use a built-in virtual keyboard instead of a personal keyboard to prevent keyloggers from capturing the details entered. It is primarily designed to monitor what your child is surfing the internet when parents are out of town. However, it is used for illegal purposes because it tends to be captured.

Phishing: This is a technique for designing and developing a full-featured copy of a real website. When the user enters the credentials, the credentials are captured on a fake server. You will also see a message that the server is busy to build user trust. Real users may think that this website has a technical problem. Then log in after a while. In a sense, hackers can also use their

credentials to access the control panel and change details to prevent real users from logging in. This method of hacking is done by asking the user to click a link that goes through a message or email.

Brute force attack: A simple process for accessing a web page. Repeatedly attempt multiple combinations of passwords to break in. This repeating process works like a soldier attacking a fortress. However, it takes time because you have to try all the combinations.

SQL Injection: If a website's SQL database is vulnerable, hackers can trick the system into quickly accessing confidential information via SQL injection. However, this SQL statement allows hackers to access important information on your website.

Eavesdropping (passive attack): This attack is known as MITM (man-in-the-middle attack). Hackers insert themselves as invisible intermediaries between communication channels to monitor activity. They may even change the date without being detected. If the data turns out to be useful, it may also be shared publicly. • Fake WAP: Hackers create fake access points. This is one of the easiest hacks and requires simple software and a wireless network. The hacker then names the WAP with a legitimate name such as Starbucks WiFi or a well-known company name and begins monitoring the victim. One of the best ways to counter such attacks is to use a high quality VPN service.

Virus: A small piece of code that is inserted into a legitimate program. They are designed to self-replicate and contaminate other applications[18].

2.1.14 Types of Virus

1. **File Virus**: This type of Virus poisons the system by appending itself to the end of the execution file. It changes the behavior of the start program. In the middle of the execution, the control is handover to the attached piece of code. After getting executed, it returns to the main

execution program. It is unable to identify when the execution got completed. If your code contains programs written to capture user details, those details can be shared remotely with hackers without your permission.

2. **Boot Sector Virus**: These also are referred to as reminiscence virus. It poisons the boot quarter of the gadget, receives completed on every occasion while the gadget is booted and earlier than Operating System is loaded. It contaminates different bootable media like floppy disks. 3. Macro Virus: This Virus is programmed the use of high-degree language like Visual Basic (VB). It receives mechanically prompted while macros are enabled. Mostly get to look this kind of Virus coming via spreadsheets.

4. **Source Code Virus**: It unearths for a supply code report and alters it to consist of virus and unfold it.

5. **Encrypted Virus**: This type of virus uses encryption and decryption techniques. Antivirus should not be able to identify it. Therefore, it is always in encrypted form. The decoding algorithm is carried. It will be self-decrypted and distributed whenever needed.

6. **Stealth Virus**: A very complex virus. Change the code as soon as it is recognized. It is difficult to identify and correct. If detected, the virus attempts to trick the user by displaying the actual code instead of the modified code. – Tunneling virus: This virus attempts to evade antivirus scanner detection by installing itself in the interrupt handler chain. Program interception remains in the operating system background and it is difficult to catch such viruses.

7. **Multi-party Virus:** This type of virus can infect multiple parts of the system, including boot sectors, memory and records. It cannot be detected and corrected. 8 Armored virus: Encoded in a high-level language, even antivirus cannot be detected and removed. It tricks the antivirus by specifying the wrong path instead of the actual location where the antivirus is available.

Trojan Horse Trojan: A malicious software program. Installed on the victim's work hub, it shares victim information remotely with hackers. It also locks files, serves fraudulent ads, blocks traffic, and snoops data.

Denial of Service Service Deny: An attack that renders a web server unavailable or crashes the entire web server. In this type of attack, a hacker uses a bot or zombie machine to flood the web server with a large number of requests and shut down the server. Hackers can achieve this in less time.

Waterhole Attacks: In this type of attack, an attacker always tries to find out who is the most frequently visited user of a website or group. This attack is primarily targeted at well-known businesses as it tends to poison members of the targeted victim group. These are primarily focused on infecting websites with malware, making their targets more vulnerable and more difficult to identify.

Browser locker: Those who are not tech-savvy can easily fall into this type of attack. The attacker either encourages users to visit their website or forces users with attractive web posts to redirect to their website. The main trap starts from here. Hackers hijack the screen and display pop-up message boxes that make it difficult for visiting users to close. Pop-ups are always messages such as antivirus alerts, system cleanup, etc. to help users access support links on malicious computers. Victims who visit will pay the attacker to kill the virus from their computer.

Cross-site scripting websites are connected to various servers to optimize functionality to improve communication. If you don't need to verify authentication when switching to another server. This can lead to abuse of the website. Even hackers can insert scripts to control your website and attempt to steal your information.

IoT Attacks: Everyone is heading into the IoT era. People cannot live for a minute without the internet. It also made people's lives easier. However, new hacking technologies have infected and spread widely, stealing user data. Good examples are smart watches, smart TVs, and all smart gadgets built to make life happier and currently threatening them. Instead of a positive effect, it produced a negative effect on people's lives.

2.1.15 Network Security

Network security includes many technologies, devices, and processes. It refers to a set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data. Appropriate network security controls are recommended for organizations to reduce the risk of attacks and data breaches. These measures also enable the safe operation of IT systems. Network security consists of hardware and software technologies, ideally layers that include applications, antivirus, access control, servers, firewalls, physical access, and policies[19].

2.1.16 Network and Security Threat

Network threats are illegal or malicious activities aimed at exploiting network vulnerabilities. The purpose is to compromise, damage, or interfere with information or data that is valuable to the company. A malicious attacker can target your network to gain unauthorized access and manipulate it for your purposes[20].

2.1.17 Types of Network Security Attacks

Network security are categorized based on their ultimate goal and are called active and passive. Active: Hackers involved in active attacks attempt to destroy systems connected to the network.

Examples of active threats: masquerade, replay, message content modification, denial of service (DoS) Passive: The purpose here is to monitor / verify sensitive information. This is where the security of a company and its customers is at stake. Examples of passive threats: publishing news content and analyzing traffic

2.1.18 Network Security Control

Network Security Control are categorized based on their ultimate goal and are called active and passive. Active: Hackers involved in active attacks attempt to destroy systems connected to the network. Examples of active threats: masquerade, replay, message content modification, denial of service (DoS) Passive: The purpose here is to monitor / verify sensitive information. This is where the security of a company and its customers is at stake. Examples of passive threats: publishing news content and analyzing traffic

2.1.19 Network Protocols

Network protocols allow communication between two or more network devices. Without these protocols, the device will not be able to understand the electrical signals it is sharing. Various computer network protocols have specific purposes and scenarios.

2.1.20 Components of Network Protocols

Internet Protocol (IP): It is an Internet addressing system with core functionality for delivering packets of information. IP is the primary key for network connections.

Transmission Control Protocol (TCP): TCP works with IP to exchange packets of data. TCP organizes data to ensure secure transmission between clients and servers.

Wireless Network Protocols: These protocols work in wireless networks. e.g. WiFi, Bluetooth, LTE. This is useful for mobile and electronic devices that are not directly connected by a cable.

Network Routing Protocols: Routing protocols define routing paths for forwarding network messages and dynamic routing decisions. OSPF, BGP, and EIGRP are examples of routing protocols.

2.1.21 Network Firewalls

A firewall is a hardware or software program designed to improve network security. Its purpose is to block all unwanted incoming traffic while allowing allowed communication to flow freely. Traditional network security firewalls can only protect your internal network from incoming traffic. Nevertheless, firewalls have played an important role over the last three decades. The latest firewalls have been modified as NGFW and target NGFW to block new cyber threats.

2.1.22 Types of Firewalls

Proxy Firewall: Proxy firewalls protect private network resources by excluding messages tagged at the application layer.

Stateful Inspection Firewall: This type of firewall blocks inbound traffic based on status, port, and protocol.

Next-generation Firewall (NGFW): Next-generation firewalls can block the latest cyber threats such as advanced malware and application layer attacks.

Unified Threat Management (UTM) Firewall: UTM firewalls provide a single security solution that provides multiple security features.

Threat-focused NGFW: Threat-focused NGFWs offers advanced threat detection and remediation.

2.1.23 Network Traffic Monitoring

Network security is monitored to ensure the security of internal systems and data generated during the process. This data is useful for a variety of IT operations and case studies. Network traffic monitoring tools can be broadly divided into two types. There are deep packet inspection tools and flow-based tools. These tools are becoming more and more popular in the cybersecurity community as enterprises rely on mechanisms such as the cloud and VOIP. Network monitoring software helps you monitor network traffic when the load on your network increases.

2.1.24 Cryptography

Cryptography is the science of transforming information and making it secure while it is being sent or stored. This is done to prevent unauthorized users from viewing the data. You can use cryptography to ensure the integrity of your data. To ensure that the data has not been changed or changed in any way. It is best understood by dividing it into different areas. The main areas of cryptography are:

1. **Random Numbering**: This includes generating random numbers using an algorithm that produces pseudo-random numbers that appear randomly.
2. **Private keys**: Cryptography key is a mathematical value used to encrypt and decrypt messages. The private key, also known as symmetric or single-key encryption, uses the same

key for both encryption and decryption of the message. The big advantage of symmetric encryption is that it is fast, but symmetric encryption keeps the key secret from all users for best results. Otherwise, an attacker who discovers the key could read the message sent. It is difficult to transfer the private key to multiple users and ensure its confidentiality.

3. **Public key**: This is likewise referred to as uneven encryption which calls for using keys, a public key and a non-public key to encrypt and decrypt the message respectively. The public key, which encrypts the data, does now no longer must be saved secret, however the non-public key's saved confidentially, therefore, keeping off the want to soundly delivery keys.

4. **Hash Functions**: They improve performance when signing large blocks of data using asymmetric encryption, ensure integrity and authentication protocols by preventing messages from changing during transmission, and create pseudo-random data. Used Hash functions accept messages of any size and small computer messages, called digests or hashes. MessageDigest Algorithm 5 (MD5) is an example of a hash function. Data is always hashed to a normal digest, regardless of the calculated time. The only way to change the created digest is to change the data itself. Therefore, these functions guarantee the integrity of the data.

2.1.25 Network Attack

There are some attacks or threat that are conducted against network.

Classification of Internet Security Attack

1. Passive Attack:

Passive-aggressive attacks are attacks aimed at obtaining information by an attacker. I don't want to change the content of the original message. It is very difficult to detect because it does not change the data. News publishing, traffic analysis, sniffing, and keyloggers are several passive attack techniques.

Interception: Interception is a type of attack that is carried out with or without the user's permission. It breaks the rules of confidentiality in the principles of security. Simply put, interception leads to a loss of confidentiality in the message. This is a kind of passive attack. It is further divided into two subtypes. i.e Traffic analysis and publication of news content. There are four types:

Release of Message: When you send a message to a friend, make sure that only that person can read the message. You can use certain security mechanisms to prevent the publication of news content. For example, you can use an algorithm to encode the message.

Traffic Analysis: If many messages go through a single channel, a confused user could inform an attacker by believing that the message came from his party.

Sniffing:Sniffing is a method of sniffing outbound data sent by the sender. It just tries to find out what kind of message or data the sender is sending without the sender's permission.

Keyloggers:This is a program that runs in the background and records every keystroke. Once the keystrokes are logged, they are either hidden on the computer for later retrieval or sent live to the attacker. Attackers then carefully search for them to find passwords or other useful information that could be used to compromise the system or launch social engineering attacks. For example, keyloggers reveal the content of all emails created by users. Keyloggers are usually included in rootkits.

2. Active Attack

Active attacks are attacks that make changes to the original message or create fake messages. These attacks are extremely complex and cannot be easily prevented. It can be further divided into three types: destruction, manufacturing, and modification. Within these categories, common attacks include denial of service (DoS), DDoS, DRDoS, SQL injection, replay attacks, masquerade, and man-in-the-middle attacks.

Interruption: Interrupt attacks are active attacks. In this attack, the authorized entity pretends to be another entity. For example, there are three users A, B, and C. User A can impersonate User C and send a message to User B. User B believes that the message came from User C. If interrupted, resource availability is compromised. Classified into four types

Denial of Service (DoS):The system receiving the request is busy establishing a return communication path with the initiator (probably using a valid IP address) and remains in wait state because a legitimate user has been denied access.

Distributed Denial of Services (DDoS): A distributed denial of service (DDoS) attack is an attack in which multiple compromised systems attack a single target, thereby causing a denial of service to users of target system. A flood of incoming messages to the target system basically forces the system to shut down, thereby denying legitimate user service on the system.

Distributed DoS with Reflectors (DRDoS): It consists of reflectors that help the attacker launch a more effective and safe attack. This increases damage and reduces the risk of backtracking.

SQL Injection Attack: This is a security vulnerability that occurs in the database tier of an application. The SQL code is passed to the interactive web application used by the database service.

Fabrication: In this attack, the user uses an access service that is not authorized for use. It is possible without a proper authentication mechanism48. It is used in these two attack methods.

Replay Attack:Replay attacks are a type of active attack in which valid data transmissions are maliciously repeated or delayed. The attacker captures the authorized data and resends it for personal use of the For example, suppose User A wants to transfer an amount to User C's bank account. Both users A and C have a bank B account. User A sends an electronic message to Bank B requesting a remittance. User C was able to capture this message and send a second

copy to Bank B, but Bank B was unaware that this was a malicious message. Therefore, User C will benefit from the transfer twice. Replay attacks can be prevented by using a timestamp and a strong digital signature containing unique information from the previous transaction, such as: B. The value of the sequence number that increases continuously.

Masquerading: A masquerade attack is an attack in which one system impersonates another. This is a technique used by attackers to pretend to be someone who has been granted unauthorized access to sensitive information.

Modification: This causes losses of integrity principle. For example a person did an online transaction of Rs. 100. But the attacker hack this and modify it to Rs.1000. This is a case of integrity. Under this attack technique is man of the middle attack.

Man of the Middle Attack: It is abbreviated as MITM. This is an active internet attack that attempts to intercept, read, and modify information that floats between users of public networks and requested websites. Attackers use illegally obtained information in theft or other ways of personal information.

2.1.26 System Usability Scale (SUS)

The System Usability Scale is the usability evaluation framework employed in this study. System Usability Scale(SUS) is a standardize questionnaire based method for the assessment of preceieved usability. It has proven to be quick but not dirty. SUS was developed by John Brooke in the year 1996 reflected a strong need in usability community for a tool that could quickly and easily collected a user's subjective rating of a product usability.

2.2 Methodology Review

Procedure for Detecting Cybercrime Activities on Websites

The author emphasized the important of cyberspace security and method to mitigate cyberattacks. A model was developed to identify and classify website vulnerability, cyberattack prevention, improving method for monitoring website security, identifying method for alerting website owner in case there is a detection of intrusion.

Cybercrime Detection and Control using the Cyber user Identification Model.

The author uses a paradigm shift to detect and identify cyber criminals. An object-oriented paradigm was used for systems analysis and design. A three-tier authentication (facial image, fingerprint and password) is required during login which guarantees the security of the system.

Understanding Cybercrime and Developing a Monitoring Device.

The author developed a software to solve the problem of retrieving data log. The software runs on Windows platform which automatically execute cmd command to get netstat and upload logs to server every 5 mins. Files are transmitted through an encrypted channel.

A User Identification Management System for Cybercrime Control

A user identity management system called PythonIDM was developed. The system provided solution to the problem of Identity Theft with the help of privacy preserving multi-factor authentication. A two-factor authentication system was used in the implementation of the IDM solution that uses federated Identity Model. A trusted platform Module within the system was developed to ensure strong integrity

Security Monitoring of the Cyber Space

Despite the fact that this IT critical infrastructure provides various communication services, adversaries are abusing the Internet security and privacy to execute cyber attacks for various reasons. To cope with these threats, security operators utilize various security tools and techniques to monitor the cyber space. An efficient way to monitor and infer threat activities online is to collect information from trap-based monitoring sensors. This primarily defines the cyberspace trap-based monitoring systems and their taxonomies

2.3 Review of Related Works

A study on 'Cybercrime Detection and Control using the Cyber user Identification Model'. The author proposes a paradigm shift from simply detecting and controlling cyberattacks to detecting and identifying cybercriminals in order to be anonymous. The survey focused on identifying cyber users in corporate networks (banks and malls). The methodology used was an object-oriented paradigm for systems analysis and design. The system implementation platforms were PHP and Java, and MySQL was used as the database. The hardware used for the implementation includes a built-in webcam or connected digital camera for capturing facial images, a GPS sensor for locating cyber users, and a fingerprint scanner. This study captures the digital signature of all information sent to cyberspace, the user's fingerprint and facial image as a required login parameter, identifies the user's geographic location and system MAC address, date, it is modeled to provide an interface for recording time and type, recording actions taken by users on the Internet and recording security threats for further investigation by cybercrime investigators. The results show that the system can actually identify cyber users and their criminal activity on the Internet[22].

"Digital Forensic Investigation Models: An Evolution Study" perceived the status of different I.T comprising organizations in terms of cybercrime and forensic investigation process and Pakistan was taking as case of study". On this a questionnaire was designed to survey different organizations to find out that how effectively they have secured their technology infrastructure and how supportive this setup could be for any forensic firm to perform the forensic investigation in case of occurrence of any cybercrime. In the critical analysis, the main finding reckoned as flaw found in these organizations was that they do not pay much importance to forensic investigation and because of this they don't incorporate forensic supportive tools such as employees' awareness training programs, clauses in hiring documents and acquiring the services of forensic firms as per requirement. They concluded that if this situation is not addressed it may lead organizations to different types of losses in case of occurrence of cybercrime[23].

A study on "Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime" analysis series of legal actions against cybercrime, it also explored in to the Chinese model of regulation of cyberspace. In order to exercise control over the Internet, China has implemented statutory laws and administrative regulations revolving activity of criminals, content filtering and user monitoring so as to maintain security and stability at both community and state levels. A tight legal and regulatory network has gradually weaved through recruitment of cyber police, investment on security technology, regulations on communications enterprises, and surveillance over users. Regardless of critics, this model was proved to have the merits of effectiveness in the specific socio-legal context in a short term[24].

A study on "The Application of Network Forensics" detailed the concept of network forensics, forensics process, forensics model and some common techniques and methods; the analysis of the real time intrusion forensics and other four kinds of typical network forensics system framework on the basis of the Intrusion detection system is discussed combined with network Forensics system. The feasibility of the proposed and analyzed system is based on Intrusion tolerance, monitoring technologies such as network forensics system design thought"[25].

A study on "Computer Forensics Investigation; Implications for Improved Cyber Security in Nigeria" detailed the role of computer forensics in collecting digital evidence related to cybercrime is relatively new in Nigeria, but it is promised to act as a watchdog in cybercrime containment and checkmates, as well as ensuring cybersecurity. The author wanted to explore the concepts of cybercrime, cybersecurity, and the impact of computer forensics on cybersecurity in Nigeria, and emphasize the impact of computer forensics on national cybersecurity[26].

A study on "Understanding Cybercrime and Developing a Monitoring Device" The author studies the Current problem with cybercrime that cyber-criminals target people with little computer knowledge. Besides that, a lot of evidences were erased by intruder which makes computer forensic difficult to proceed. Although large company may have different method ensure the safety of data log, there is no software for standard user. This thesis presents software to potentially solve the current problem of data log. Other suggestions from different angles will also be made. He concluded that, more effort need to be made regarding cyber security. Countless effort and investment have been made, yet statistics have proven that it doesn`t work as well as we expected[27].

A study on "Security Monitoring of the Cyber Space" perceived the status of adversaries abusing the Internet security and privacy to execute cyber-attacks for various reasons. To cope with these threats, security operators utilize various security tools and techniques to monitor the cyber space. An efficient way to monitor and infer threat activities online is to collect information from trap-based monitoring sensors. The paper primarily defines the cyberspace trap-based monitoring systems and their taxonomies. In a nutshell, the papers aim to provide an overview on the Internet monitoring space and provides a guideline for readers to help them understand the concepts of observing, detecting and analyzing cyber-attacks through network traps[28].

A study on "Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing" The purpose of this study is to develop the theorisation of cybercrime in the context of the pandemic, and to sketch out a vision of how law enforcement might respond to a transformed landscape of online crime and offending. The authors identify specific practical implications for law enforcement, namely, that the role of local police in policing cybercrime should be re-envisioned, with a democratic, community-oriented approach at its heart[29].

A study on "cybercrime victimization and prevention: exploring the use of online crime prevention behaviour and strategies" This study aims to explore the experience of victimization, perceptions of cybercrime and use of online crime prevention strategies. The research takes a different perspective from much of the previous research seeking to better understand how

attitudinal factors (perceived prevalence of cybercrime and perceived harm of cybercrime) might motivate or influence the use of online crime prevention strategies by potential victims[30]

A study on "A User Identity Management System for Cybercrime Control" This research therefore, presents the development of a user identity management system for cybercrime control. The four stages of an identity management life cycle were developed using some mathematical tools. A two-factor authentication technique was used in developing the system, the traditional username and password was also included with biometric features for robustness. A simulation was run on the model for users ranging from 10 to 1000 using life wild dataset, and accuracy was found to be 80.01%[31].

A study on "Enhancing the effectiveness of cybercrime prevention through policy monitoring" This article examines the feasibility of designing and implementing a cybercrime prevention monitoring approach to enhance the quality of knowledge about policies that aim to reduce the prevalence and impact of online harms[32.]

A study on "Precautions That Are Taken by It Firms to Prevent Cybercrime" In this study, data is collected from the companies operating in the IT industry in Turkey. If companies faced with cybercrime, the measures taken observed and analysed by using Data Mining Techniques[33].

A study on 'user identification in cyber-physical space: a case study on mobile query logs and trajectories' This paper focuses on identifying users by integrating activities in cyberspace and physical space. This gives you a comprehensive understanding of your online behavior and offline visits. The basic insight to solve this problem is that stable location distribution of IP addresses allows you to create a connection between cyberspace and physical space. Therefore,

we propose a new framework for user identification in cyber physical space. It consists of three main steps: 1) Model the position distribution of each IP address. 2) Use inverted indexes to calculate co-occurrence, reducing space and time costs. 3) Ranking learning tactics to combine user features shared by both domains to improve accuracy. Run experiments to identify individual users from mobile query logs (generated in cyberspace) and trajectory data (generated in physical space) to demonstrate the efficiency and effectiveness of the framework[34].

A study on 'Implementation of a Large-Scale Platform for Cyber-Physical System Real-Time Monitoring'. The author presents a large-scale platform for CPS real-time monitoring based on big data technologies, which aims to perform real-time analysis that targets the monitoring of industrial machines in a real work environment. This paper is validated by implementing the proposed solution on a real industrial use case that includes several industrial press machines. The formal experiments in a real scenario are conducted to demonstrate the effectiveness of this solution and also its adequacy and scalability for future demand requirements. As a result of the implantation of this solution, the overall equipment effectiveness has been improved[35].

A study on 'A Cyber-Physical Production System Framework of Smart CNC Machining Monitoring System' this author proposed a smart monitoring system for CNC machining based on Cyber-Physical Production System (CPPS) framework. It is built on the CNC machine tool physical and virtual modeling, process monitoring, and big data analytics, and then synergized into a system through a distributed network. Under the CPPS framework, the smart monitoring system is divided into control layer, network layer, and decision layer. The function of each

layer and the key technologies of the CPPS involved are discussed. Case studies of machining process monitoring are studied in the applications[36].

A study on 'The design of cybercrime spatial analysis system' this study detailed the spatial rules of typical cybercrime are explored on base of GIS with Internet searching and IP tracking technology: (1) Setup spatial database through IP searching based on criminal evidence. (2) Extend GIS data-structure and spatial models, add network dimension and virtual attribution to realize dynamic connection between cyber and real space. (3) Design cybercrime monitoring and prevention system to discover the cyberspace logics based on spatial analysis[37].

A study on 'Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles'. This paper provided an AI approach for cyber-threats detection, primarily based totally on synthetic neural networks. The proposed approach converts multitude of accumulated safety activities to character occasion profiles and use a deep studying-primarily based totally detection approach for stronger cyber-chance detection. For this work, we evolved an AI-SIEM machine primarily based totally on a aggregate of occasion profiling for statistics preprocessing and extraordinary synthetic neural community strategies, together with FCNN, CNN, and LSTM. The machine makes a speciality of discriminating among proper fantastic and fake fantastic alerts, for this reason assisting safety analysts to swiftly reply to cyber threats. All experiments on this observe are completed with the aid of using authors the usage of benchmark datasets (NSLKDD and CICIDS2017) and datasets accumulated withinside the actual world. To examine the overall performance assessment with present strategies, we performed experiments the usage of the 5 traditional machine-studying strategies (SVM, k-NN, RF, NB, and DT). Consequently, the experimental outcomes of this observe make sure that our proposed strategies are able to being hired as studying-primarily based totally fashions for

community intrusion-detection, and display that even though it is hired with inside the actual world, the overall performance outperforms the traditional machine-studying strategies[38].

A study on 'Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective'. This author presents some evaluations of widely used machine learning techniques used to detect some of the most sinister cyber threats to cyberspace. Three major machine learning techniques are being considered, including Deep Belief Network, Decision Tree, and Support Vector Machine. Based on commonly used benchmark datasets, we've presented a quick study to measure the performance of these machine learning techniques in spam detection, intrusion detection, and malware detection[39].

A study on 'Optimal Machine Learning Algorithms for Cyber Threat Detection' The author elaborated on a machine learning (ML) -based analysis of security machine data. It is intended for security data mining, with the goal of discovering highly targeted cyber threat actors and minimizing operational costs for maintaining static association rules. However, choosing the best machine learning algorithm for security log analysis is a factor that hinders the success of data science in cybersecurity, especially for large or global security operations centers (SOCs). Because there is. Detection of false positives) environment. This fact presents an urgent need for an efficient machine learning-based cyber threat detection model that can minimize false positive rates. This white paper uses a variety of prediction, classification, and prediction algorithms to propose optimal machine learning algorithms with an implementation framework based on analytical and empirical evaluation of the collected results[40].

A study on 'Performance Evaluation of Cyber Criminal Detection Techniques' This paper analyzes the performance evaluation of various cybercriminal determination methods. First, the

detection of synthetic ID theft is checked. Next, intrusion detection is checked by the honeypot security mechanism. Third, detection is further enhanced by using lie detection techniques to determine a person's wrong language. Finally, by analyzing user profiles, clustering techniques are used to perform cybercrime detection. The method of stealing synthetic personal information outperforms other methods in evaluation. According to the experimental results, when comparing the final criminal list with the confirmed criminal list, 41 out of 100 real users were excluded, but of the real users who were otherwise excluded. The numbers are 16, 36 and 38, respectively. Only 4 attributes are used, but 5, 10, and 25 are used for other methods. The performance metric percentage is also 37.1 and the slope is 31.1. This is superior to the other methods being considered in performance analysis[41].

A study on 'Implementation of data mining techniques for cyber crime detection'. This paper provides a complete examine on information mining strategies and its obligation on detection of cyber crimes in actual time applications. Data mining automatically sieves thru large amount of information to discover known/unknown styles that fetches out valuable, modern perceptions and formulate predictions. Data mining that is alienated into studying abilities viz., supervised and unsupervised is engaged to stumble on fraudulent asserts. Basically those strategies are used for fraud detection in lots of sectors consisting of health, insurance, E-commerce and it is going on[42].

A study on 'Visualizing cyber attacks using IP matrix'. The author described how to visualize cyber threats using a two-dimensional matrix representation of IP addresses. The advantages of this method are: (1) The logical distance of the IP address is displayed intuitively. (2) The Internet address space is economically visualized. (3) Macroscopic information (Internet level)

and microscopic information (local level) are visualized at the same time. By using this visualization framework, the spread of Welchia worms and Sasser.D worms is visualized[43].

A study on 'Cyber crime investigation, data archival and analysis using big data tool'. The author has ideas for using cybercrime investigation tools to analyze data, create reports, and provide this data in MongoDB to manage big datasets and extract structured datasets. And introduce the strategy. The threat does not recure[44].

A study on 'Forensic Investigation Processes for Cyber Crime and Cyber Space'. This author considered two aspects. First, different types of crime in cyberspace and different sources of cyberattacks, then different cyberattack investigation steps using digital forensic tools such as WinHex[45].

A study on 'Generic Proactive IoT Cybercrime Evidence Analysis Model for Digital Forensics'. This author proposed a general proactive model of the IoT cybercrime analysis process. This model focuses on pre-classifying evidence based on its importance and relationship to past crimes and the severity of the evidence in relation to the likelihood of cybercrime. This model is designed to save time and effort in the automated forensic investigation process[46].

A study on 'A Multi-level Evidence-based Cyber Crime Prosecution Information System'. This article aims to leverage a multi-layered cybercrime detection and control system to provide cybercrime investigators with real-time, enhanced evidence to assist in the prosecution of cybercriminals. The design was based on a robust system that combines user IDs, device IDs, geographic locations, and user activities to uniquely identify cyber users and provide evidence

to reveal the crimes committed. The system captures the user's facial image and bio-fingerprint as required login parameters in addition to the username and password before granting access. This system has been tested and implemented on the real-time cybersecurity website www.ganamos.org. The results show that it is possible to identify cyber users and associate their activities with the device they are using, the date of operation, the time of day, and the location. These can provide law enforcement agencies with real-time evidence to track and prosecute cybercriminals[47].

A Study On 'Various Cyber Attacks and A Proposed Intelligent System For Monitoring Such Attacks'. The author presents research on various cyberattacks unleashed in India and other countries in recent years. Various prevention methods previously proposed to combat this type of attack. These prevention methods are based on machine learning algorithms such as Random Forest, kmeans clustering, support vector machines, and artificial neural networks applied to prevent cyber attacks. The author also proposed an intelligent system based on unsupervised and unsupervised learning techniques to avoid these cyber attacks. This proposed system can provide high efficiency with minimal human intervention and can be implemented and used as a universal solution to the most common cyber attacks[48].

A study on 'Automated Data analytics approach for examining the background economy of Cybercrime'. The motivation for this task is to study the problems encountered in cybercrime using data analysis methods for designing information systems. To achieve this, a framework for investigating cybercriminal activity will be created first. In the second step, you need to create a CaaS definition. The third step is to use a classification model to classify different activities. It is used to evaluate proposed techniques tested on datasets collected by the online

hacking community. The research gap develops effective information systems to address various cybercrime problems and provides practical insights for both the private and public sectors to record attacks encountered in cybercrime. It will be filled by doing.[49].

A Study on 'the Real-time Cyber Attack Intrusion Detection Method' This author has defined a violation detection method for the main component module to improve the problem with the existing violation detection method. Through performance testing of each module, we propose effective security control measures and consider effective ways to detect attack threats by updating the control system with Security Information and Event Management (SIEM)[50].

A study on 'Cybercrime Categories and Prevention'. This author provides information on cybercrime and various types, and how to protect your data from threats[51].

A study on 'Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models'. This paper outlines developments over the last decade to use machine learning models (MLMs) to facilitate the creation of intelligent solutions aimed at mitigating the threat of cybercrime. It follows an exploratory perspective and utilizes materials published from well-known databases. It emphasizes some applicability and potential of documented intelligent cybercrime countermeasure strategies, while downplaying some intended benefits. This paper has been overwhelming as the cost of cybercrime continues to rise steadily, although much effort has been spent over the last decade to develop an intelligent approach to combating cybercrime. We conclude that success has not been achieved. To that end, this paper proposes a new integrated approach called a single-window cybercrime countermeasure strategy that emphasizes the incorporation of social and intuitive elements into cybercrime detection and management, as well as technology[52].

A study on ‘Enhancing the effectiveness of cybercrime prevention through policy monitoring’. This author outlines the principles and benefits of a policy monitoring approach, reviews the key characteristics of 18 policy monitoring platform samples, evaluates 12 cybersecurity policy evaluation initiatives, and only a few of them are frameworks. Concludes that it contains cybercrime. Next, we will provide a template to create a dedicated cybercrime prevention monitoring tool to help scholars, policy makers and practitioners[53].

A study on ‘Monitoring and early warning of new cyber-telecom crime platform based on BERT migration learning’. The author described 's critical surveillance and early warning research on the new cyber telecom crime platform, which lays the foundation for establishing preventative and control systems to protect civilian property. However, the deep learning techniques used to monitor and warn new cyber-telecom crime platforms have some obvious drawbacks. For example, these methods suffer from data distribution discrepancies and heavy manual labor in labeling the data. Therefore, new cyber-telecom crime platform monitoring and early warning methods based on the BERT migration learning model have been proposed. This procedure first identifies the text data and its tags, and then performs migration training based on a pre-training model. Finally, this method uses a fine-tuned model to predict and classify new cyber-telecom crimes. Experimental analysis of criminal data collected by public security agencies shows that higher classification accuracy can be achieved with the proposed method compared to deep learning methods[54].

A study on ‘Legal Design and Implementation of Cyber crime Monitoring System in Nigeria’. The author examines plans created to show the appearance or function of cybercrime

surveillance systems under Nigerian law. Identify effective strategies for reducing cybercrime for young people and society as a whole. The author aimed to design and implement a cybercrime surveillance system in Nigeria. The specific purpose is to identify the causative factors of cybercrime between young people and society, and how the impact of cybercrime on the Nigerian economy and how the economy will be affected by the high rate of cybercrime, especially in Nigeria. Is to clarify. Researchers used teaching methods to gather information. This involved collecting material related to the topic and performing important analysis and explanation of the data. It relied on both primary and secondary data sources such as the Constitution, law, legislative books, legal journals, legislative reports, conference papers, treaties. The Studies show that Nigeria is one of the countries with the most cybercrime. Another discovery of this work is that Nigerian internet technology has led to the modernization of fraud among young people. Cyber fraud seems to be a well-established livelihood for young people in Nigeria. In conclusion, he made the necessary recommendations by asking the government to develop political will by providing law enforcement agencies with the technical equipment to properly prosecute cybercriminals. Serious liability crime[55].

2.5 Summary of Gaps Literature

Several literature were reviewed in this study and some salient gap were identified for possible further study. It was found that several monitoring system as been in existence, it is still difficult to identify and track down cyber criminals. A study on Procedure for Detecting Cybercrime Activities on Website, the author developed a model to identify and classify website vulnerability, cyberattack prevention, improving method for monitoring website security, identifying method for alerting

website owner in case there is a detection of intrusion. In essence, a gap exists in the cost implementation and diffuilty in integrating a Web Application Firewall to a website. Also, to monitor large user group is tedious. The humongous cost and difficulty in implementing an automated monitoring device discourage individuals and organizations in effectively monitoring their website. As a result of this, cybercrime continues to increase.

Endnotes

1. I., Frank, & E., Odunayo, Approach to Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in science, engineering and education*, *1*(1), 2013, pp.100-110.

2. T., Alese, O., Owolafe, A.F. Thompson, & B.K., Alese, A User Identity Management System for Cybercrime Control. *Nigerian Journal of Technology*, *40*(1), 2021, pp.129-139.

3 N., Goyal, & D., Goyal, Cyber Crime in the Society: Security Issues, Preventions and Challenges. *Research Journal of Engineering and Technology*, *8*(2), 2017, p.73.

4 T. Richardson, & Thies, Secure Software Design, *Jones & Bartlett Publishers*, 2013.

5 M.C.B., Umanailo, I., Fachruddin, D., Mayasari, R., Kurniawan, D.N., Agustin, R., Ganefwati, P., Daulay, A., Meifilina, T., Alamin, R. Fitriana, & S., Sutomo, Cybercrime Case As Impact Development Of Communication Technology That Troubling Society. *Int. J. Sci. Technol. Res, 8*(9), 2019, pp.1224-1228.

6. V., Hahanov, O., Mishchenko, T., Soklakova, V., Abdullayev, S. Chumachenko, & E., Litvinova, Cyber-Social Computing. *In Green IT Engineering: Social, Business and Industrial Applications, 2019, (pp. 489-515). Springer, Cham*

7. M., Humayun, M., Niazi, N.Z., Jhanjhi, M. Alshayeb, & S., Mahmood, Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(4), 2020, pp.3171-3189.

8. K.S., Choi, , C.S., Lee & E.R., Louderback, Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp.27-43.

9. M.N., Alenezi, H., Alabdulrazzaq, A.A., Alshaher, & M.M., Alkharang, Evolution of Malware Threats and Techniques: A Review. *International Journal of Communication Networks and Information Security***,** 12(3), 2020, pp.326-337.

10. W.A., Al-Khater, S., Al-Maadeed, A.A., Ahmed, A.S., Sadiq, & M.K., Khan, Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access*, *8*, 2020, pp.137293-137311.

11. N., ALI, S., Samsuri, M.A., SEMAN, BROHI, I. & A., Shah, Cybercrime an Emerging Challenge for Internet Users: An Overview**.** *Sindh University Research Journal (Science Series)***,** 50(3D), 2018, pp.55-58.

12. L.M., Cristea, Current Security Threats in the National and International Context. *Journal of Accounting and Management Information Systems*, 2020, *19*(2), pp.351-378.

13. R., Ruefle, A., Dorofee, D., Mundie, A.D., Householder, M. Murray & S.J., Perl, Computer Security Incident Response Team Development and Evolution. *IEEE Security & Privacy*, 2014, *12*(5), pp.16-26.

14. A.A., Farsole, A.G. Kashikar, &, A., Zunzunwala, Ethical Hacking. *International Journal of Computer Applications***,** 1(10), 2010, pp.14-20.

15. A., Ushmani, Ethical Hacking. *International Journal of Information Technology (IJIT)*, 2018, *4*(6).

16. V.B Vooradi, & L., Jadhav, Ethical Hacking Techniques and its Preventive Measures for Newbies, 2019.

17. K., Michael, The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Vol. 31. 2012.

18 C.Y., Li, C.C., Huang, ,F., S.L. LaiLee, & J., Wu, A Comprehensive Overview of Government Hacking Worldwide. *IEEE Access*, *6*, 2018. pp.55053-55073.

19. D., Zissis, & D., Lekkas, Addressing Cloud Computing Security Issues. *Future Generation computer systems*, *28*(3), 2012, pp.583-592.

20. J.P.A., Yaacoub, O., Salman, H.N., Noura, N., Kaaniche, , A. Chehab & M., Malli, Cyber-physical Systems Security: Limitations, Issues and Future Trends. *Microprocessors and microsystems*, *77*, 2020,p.103201

21. P. Kaplesh, & A., Goel, Firewalls: A study on Techniques, Security and Threats.

22. M.A., Agana-correspondence, Cyber Crime Detection and Control Using the Cyber User Identification Model, 2015.

23. K., Mushtaque, K., Ahsan & A., Umer, Digital Forensic Investigation Models: An Evolution Study. JISTEM-Journal of Information Systems and Technology Management, 12(2), 2015, pp.233-243.

24. X., Li, Regulation of cyber space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology***,** 9(2), 2015, p.185.

25. S., Khan, A., Gani, W.A., A.Wahab, M. Shiraz, & , I., Ahmad, Network Forensics: Review, Taxonomy, And Open Challenges. *Journal of Network and Computer Applications,* 66, 2016, pp.214-235.

26. C.C., Chigozie-Okwum, D.O., Michael, & S.G., Ugboaja, Computer Forensics Investigation; Implications for Improved Cyber Security In Nigeria. *AFRREV STECH: An International Journal of Science and Technology,* 6(1**)**, 2017, pp.59-73.

27. Y., Ba, Understanding Cybercrime and Developing a Monitoring Device, 2017.

28. C., Fachkha, Security Monitoring of the Cyber Space. *In Cybersecurity Policies and Strategies for Cyberwarfare Prevention,* 2015, (pp. 62-83). IGI Global.

29. S., Horgan, B., Collier, R., Jones, & L., Shepherd, Reterritorialising The Policing Of Cybercrime in the Post-COVID-19 Era: *Towards a Vision of Local Democratic Cybercrime Policing,* 2021.

30. J.M., Drew, A Study of Cybercrime Victimisation and Prevention: Exploring the Use of Online Crime Prevention Behaviours and Strategies. *Journal of Criminological Research, Policy And Practice,* 2020.

31. T., Alese, O., Owolafe, A.F., Thompson, & B.K., Alese, A User Identity Management System for Cybercrime Control. *Nigerian Journal of Technology*, *40*(1), 2021, pp.129-139.

32. B., Dupont, *Enhancing* The Effectiveness of Cybercrime Prevention Through Policy Monitoring. *Journal of crime and justice*, 42(5), 2019, pp.500-515

33. U.T., Gursoy, A Study on Precautions that are Taken by It Firms to Prevent Cybercrime, 2007.

34. T., Hao, T., Zhou, Y., Cheng, L., Huang & H., Wu, User Identification in Cyber-Physical Space: A Case Study On Mobile Query Logs and Trajectories**.** *In Proceedings of the 24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems,* 2016, (pp. 1-4).

35. M., Canizo, A., Conde, S., Charramendieta, R., Minon, R.G. Cid-Fuentes, & E., Onieva, Implementation of a Large-Scale Platform for Cyber-Physical System Real-Time Monitoring. *IEEE Access***,** *7*, 2019, pp.52455-52466.

36. K., Zhu, & Y., Zhang, A Cyber-Physical Production System Framework of Smart CNC Machining Monitoring System. *IEEE/ASME Transactions on Mechatronics***,** 23(6), 2018, pp.2579-2586.

37. W., Xiu, & X., Li, The Design of Cybercrime Spatial Analysis System. *In 4th IEEE International Conference on Information Science and Technology,* 2014, (pp. 132-135). IEEE.

38. J., Lee, J., Kim, I., Kim, & K., Han, Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles. *IEEE Access,* 7, 2019, pp.165607-165626

39. K., Shaukat, S., Luo, S. Chen, & D., Liu, Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective. *In 2020 International Conference on Cyber Warfare and Security (ICCWS),* 2020, (pp. 1-6).

40. V.B. Vooradi, & L., Jadhav, Ethical Hacking Techniques and its Preventive Measures for Newbies, 2019.

41. K. Veena, & K., Meena, Performance Evaluation of Cyber Criminal Detection Techniques. *International Journal of Simulation--Systems, Science & Technology*, 2018, *19*(4), pp.4-1

42. K.C., Lekha, & S., Prakasam, Implementation of Data Mining Techniques for Cyber Crime Detection. *International Journal of Engineering, Science and Mathematics,* 7(4), 2018, pp.607-613.

43. K., Ohnof, H., Koikef, & K., Koizumi, IPMatrix: An Effective Visualization Framework for Cyber Threat Monitoring. *In Ninth International Conference on Information Visualisation* (IV'05)*,* 2005, (pp. 678-685).

44. P., Dhaka, & R., Johari, Crib: Cyber Crime Investigation, Data Archival and Analysis Using Big Data Too*l*. *In 2016 International Conference on Computing, Communication and Automation (ICCCA),* 2016, (pp. 117-121).

45. K.K., Sindhu, R., Kombade, R. Gadge, & B.B., Meshram, Forensic Investigation Processes for Cyber Crime And Cyber Space. *In Proceedings of International Conference on Internet Computing and Information Communications,* 2014, (pp. 193-206). Springer, New Delhi.

46. M.R., Al-Mousa, Generic Proactive IoT Cybercrime Evidence Analysis Model for Digital Forensics. *In 2021 International Conference on Information Technology (ICIT),* 2021, (pp. 654-659). IEEE.

47. M.A. Agana, & R., Wario, A Multi-level Evidence-based Cyber Crime Prosecution Information System. *International Journal of Engineering & Technology***,** 7(3.19), 2018, pp.39-

48. A.S., Choudhary, A.S., Choudhary, & S., Salve, A Study on Various Cyber Attacks and A Proposed Intelligent System For Monitoring Such Attacks. *In 3rd International Conference on Inventive Computation Technologies (ICICT),* 2018, (pp. 612-617). IEEE.

49. S., Alagarsamy, K., Selvaraj, V., Govindaraj, A.A., Kumar, S. HariShankar, & Narasimman, G.L., Automated Data Analytics Approach for Examining The Background Economy of Cybercrime. *In 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA*)*,* 2021 (pp. 332-336). IEEE.

50. J.H. Choi, & H.J., Lee, A Study on the Real-time Cyber Attack Intrusion Detection Method. *Journal of the Korea Convergence Society***,** 9(7), 2018, pp.55-62.

51. J M., Aiswal, Cybercrime Categories And Prevention. *Manishaben Jaiswal, "Cybercrime Categories And Prevention", International Journal of Creative Research Thoughts (IJCRT),* ISSN, 2019, pp.2320-2882.

52. P.U., Chinedu, W., Nwankwo, F.U. Masajuwa, & Imoisi, S., Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. *Review of International Geographical Education Online***,** 11(7), 2021.

53. B., Dupont, Enhancing The Effectiveness of Cybercrime Prevention Through Policy Monitoring**.** *Journal of crime and justice***,** 42(5), 2019, pp.500-515.

54. S., Zhou, X. Wang, & Z., Yang, Monitoring and Early Warning of New Cyber-Telecom Crime Platform Based on BERT Migration Learning. *China Communications***,** 17(3), 2020. pp.140-148.

55. L.I., Nwokike, Legal Design And Implementation of Cyber Crime Monitoring System In Nigeria. *UNIZIK Law Journal,* 16(1), 2020, pp.92-107.

56. I.C., Mihai, Procedure for Detecting Cybercrime Activities on Websites.*SITECH Craiova, Romania*, 2017, ISBN 978-606-11-6119-5

Chapter Three

Methodology

This Chapter focuses on the methodology used to conduct the study. It discusses the techniques and methods used to fulfill the study's objective. The following section discusses the research techniques and programming used to create an online cybercrime monitoring system for forensic experts.

3.1 Research Approach

Research Approach can be classified into three types; Qualitative, Quantitative and Mixed Method.

Quatitative Approach: Quantitative methods are objective measurements and statistical, mathematical, or numerical analyzes of data collected through surveys, questionnaires, polls, or by manipulating existing statistical data using computer technology[1].

It also uses descriptive and categorise words to study human experiences and realities from the subjects perspective[2]. This is often an iterative process, where theories and hypotheses emerge from the data collected, and researchers play a key role in the data collection and analysis process. The study design is urgent and flexible, responding to changing circumstances during the course of the study. The goal is to understand the phenomenon from the viewpoint of the participants; with its particular institutional and social context intact; this data and context is lost if attempts to quantify the data are made. The validity of qualitative methods can be improved by using a combination of data collection methods and by analysis of the data by more than one person[3].

Qualitative Approach: It is an interpretative approach that seeks to gain insight into the specific meanings and experienced behaviors of specific social phenomena through the subjective experiences of participants [4]. The researcher build abstracts, concepts, hypotheses or theories by asking questions as why, how and in what way? Quantitative approach can also be decribed as the descriptive and conceptual findings collected through questionnaires, interviews, or observation. It deals with words and meanings and offers a dynamic approach to research, the researcher has an opportunity to foolow up on answers given by respondants in real time.

Mixed methods Approach: A research methodology that combines and integrates qualitative and quantitative research methods into one research study[5]. It involves collecting and analyzing qualitative and quantitative data to understand a phenomenon better and answer the research questions.

The study is based on a quantitative method of research which is the process of collecting and analyzing numerical data. It can be used to find patterns and averages, make predictions, test causal relationships, and generalize results to wider populations.

3.2 Requirement Specification

The requirement specification to achieve the success of this system required both hardware and software tools. The hardware tools are those physical electronic devices while the software tools are the written instructions in form of programs.

3.2.1 Software Implementation Tools

WordPress: is a free and open-source content management system written in PHP and paired with a MySQL or MariaDB database. Features include a plugin architecture and a template system, referred to within WordPress as Themes[1].

My Structured Query Language (MySQL): MySQL is a database system used for developing web-based software applications. MySQL is an Oracle-backed open source relational database management system (RDBMS) based on Structured Query Language (SQL). MySQL is fast, reliable, and flexible and easy to use[6].

MySQL runs on virtually all platforms, including Linux, UNIX and Windows. Although it can be used in a wide range of applications, MySQL is most often associated with web applications and online publishing. MySQL is an important component of an open source enterprise stack called LAMP. LAMP is a web development platform that uses Linux as the operating system, Apache as the web server, MySQL as the relational database management system and PHP as the object-oriented scripting language. Originally conceived by the Swedish company MySQL AB, MySQL was acquired by Sun Microsystems in 2008 and then by Oracle when it bought Sun in 2010. Developers can use MySQL under the GNU General Public License (GPL), but enterprises must obtain a commercial license from Oracle.Today, MySQL is the RDBMS behind many of the top websites in the world and countless corporate and consumer-facing web-based applications.

PHP: is short for Hypertext Preprocessor. It is a widely-used open source general purpose language that is suited for web and web application development. It can be embedded into HTML (The PHP Group, 2000). PHP is focused on server-side scripting, command line scripting and writing desktop applications. It also runs on all operating systems such as Windows, Linux and MAC. PHP supports wide range of databases including MySQL, ODBC and PDO.

HTML, CSS, JavaScript and Bootstrap: HTML were used for the frontend web pages design. CSS (cascading style sheets) used for styling. JavaScript will handle web page requests by sending client-side scripts to the browser. Bootstrap is the frame work that would be used to develop responsive and interactive web app.

Tawk.to: This is a JavaScript Application Programme Interface documentation which provide a flexible set of method in your web project.

3.2.2 Hardware Requirement

The basic hardware requirement are;

Dual Core Processor: The processor is the logic circuitry that responds and processes the basic instruction that drive the computer. Its primary functions are fetch, decode, execute and write back. For the development of the monitoring system the least processor needed is a dual core processor, anything less would cause the system to run very slow.

5GB RAM: The RAM (Read-Access Memory) is a volatile Memory in the computer system that store data and machine code currently being used. A random-access memory device allows

data items to be read or written in almost the same amount of time irrespective of physical location of data inside the memory. RAM is measured both in size and speed. RAM size determine how much temporary data the computer can store and how fast it runs.

For the development of this system, a RAM size and speed less than 5gigabyte will result in a slow and tiresome performance.

2TB Hard Disk (HDD): The hard disk is the main, and usually largest, data storage hardware device in a computer. The operating system, software title, and most files are stored in the hard disk drive. The least expected size of storage for this system to work effectively is 2Terabytes or more.

Moderm: Modem is short for "Modulator-Demodulator." It is a hardware component that allows a computer or another device, such as a router or switch, to connect to the Internet. It converts or "modulates" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize.

3.2.3 System Algorithms

Steps:

1: Start

2: Active Local Network Sever

Goto Step 3 IF Local Network is equal to TRUE

3: Load Local Hosted Web: Load Web Monitor Dashboard

4: Active Remote web Traffic Sensor

Goto step 5 if Traffic is equal to Count 1

5: Detect and Decode web Traffic

Goto Step 6,7,8,9, IF Step 5 Is Equal to True

6: Capture the digital signatures

7: Capture Traffic Geographical location

8: Capture MAC/IP address

9: Capture Date and Time

10: Capture Cyber Crime Activity

Goto11 IF Cyber Crime Detected

11: Block user or Else END

11: End

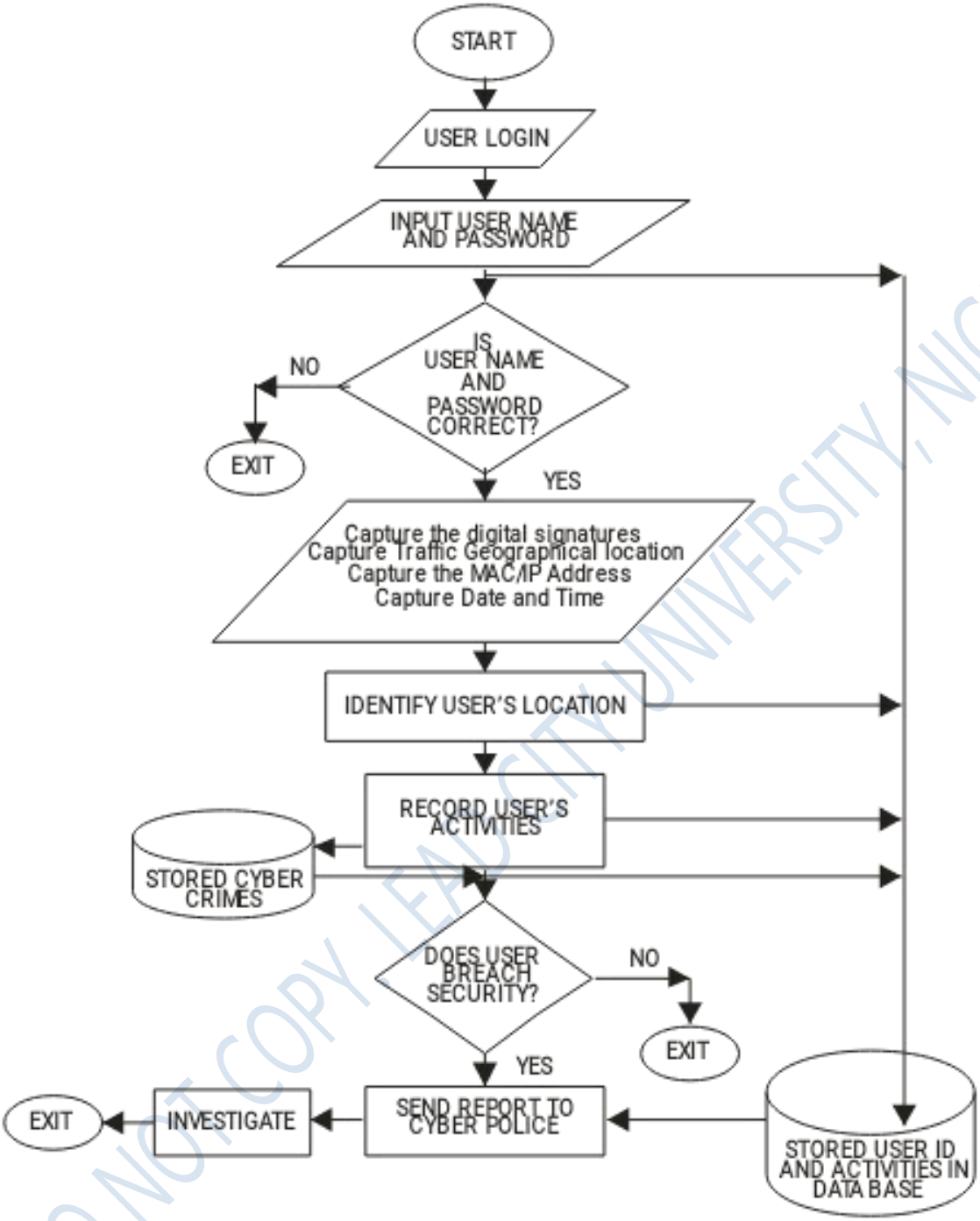


Fig 3:1 System Flowchart of Website Monitoring System

3.3 System Design

After determining and understanding how user are attacked online, a suitable method and methodology of developing enhanced Cyber Crime Monitoring System for Online Security Expert is implemented. A web application portal is designed using WordPress development tools that will serve as a platform to monitor activity of users visiting the web Gateway. Tawk.to API is integrated to the website for the Implementation of real life Monitoring System and MySQL is used as the database for the storage of information of users that visited the website.

This system will capture the digital signatures of each information sent to the cyberspace, the users login parameters, as well as identify and record the geographical location of the user, the MAC addressed of the system used, the date, time and the kind of action carried out by user while online. It will aid forensic experts in their investigations and prosecution of cyber criminals.

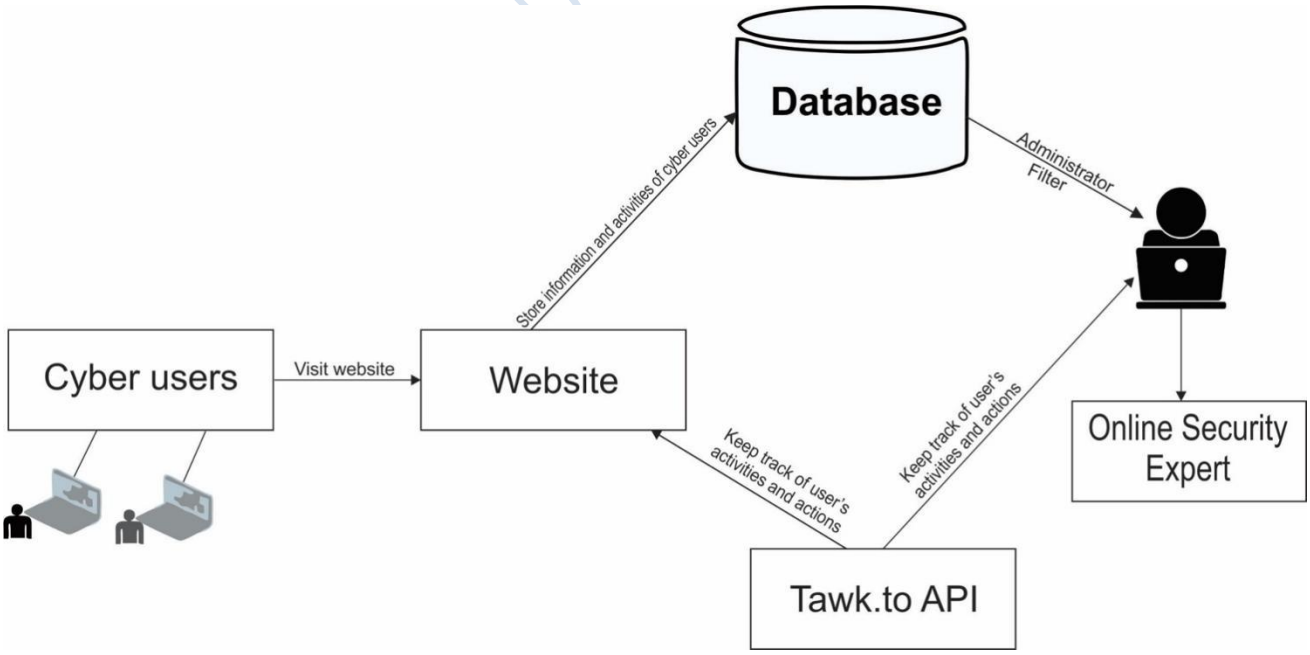


Figure 3.2: System Architecture

3.4 Research Method

The research method adopted for this study are:

1. **Software Development**: A navigable and usable website is developed using WordPress development tools and PHP is used as the programing language. MySQL database is integrated to the website for storage of information of users that visit the website. Tawk.to is integrated to the website for proper monitoring.

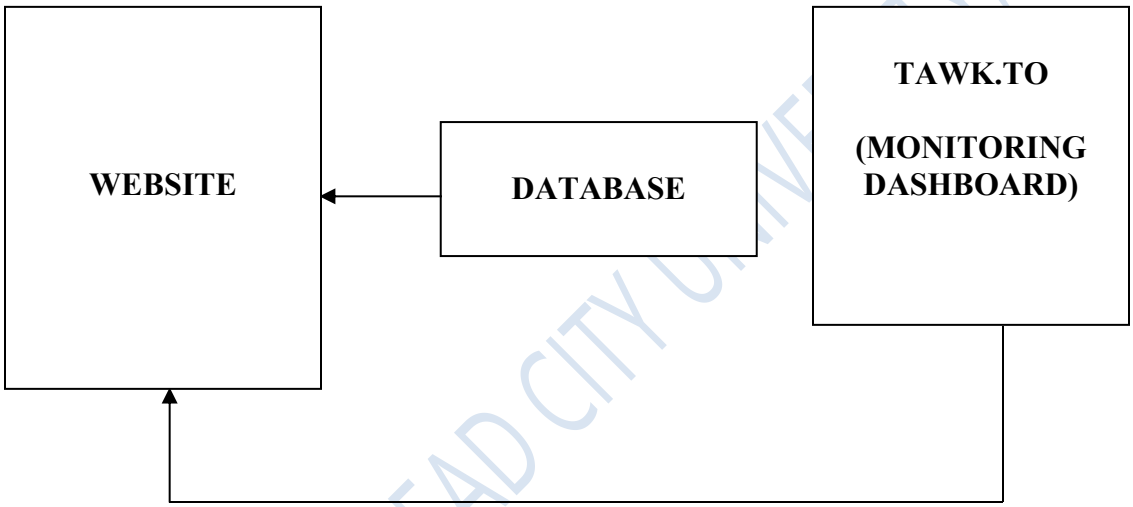


Figure 3.3: Conceptual Diagram of the System

Figure 3.1 above illustrate the major component of the system and how they are integrated to perform optimally for online security expert.

2. **Experiment**: In this phase, all the component of the system is tested to accertain the aim of the study.
3. **Evaluation**: System Usability Scale is adopted for the evaluation performance of the system. It is a standardize questionnaire based method for the assessment of preceieved usability. Questionnaire is distributed to twenty (20) participant to gain their feedback about the functionality of the system.

3.4.1 Input Design

The data types are keyed into the system using the input device. The following fields are entered for a complete record set, screen display in Chapter four.

i. Date

ii. Time

iii. Computer name

iv. Serial no

3.4.2 Output Design

The information will be displayed on the screen shot in chapter four showing the result of a particular query. The record of each activity is captured including the browser history with date and time. The management or forensic expert can read and interpret the log of activity each user did on his/her account. This can as well be printed out on a hard copy.

3.4.3 Database Design

To get a precise output the screen captures are saved in jpeg format while the process log is saved as a text file. A folder was created where the files are saved. Once the images are taken they are transferred to the folder. The necessary data that will be stored in the database are entered alongside the dates, time, day, and file format.

Table 3.1 Database output File

S/N	Field Name	Field Type	Index
1	Image log	String	N
	Process log	String	N
2			
3	Index.dat	String	N
4	Name of account	String	N
5	Date	Varchar(100)	N
6	Time		N
7	File type		N

3.4.4 Data Flow Diagram

This main menu explains the whole concept of the project. It encapsulates the entire function of the system. In fig 3.2 below, the forensic expert interface application pulls up the content of the captured running processes, captured screenshots and content of Index.dat. All this process happened by making request; the module reacts through a response. This is as shown below;

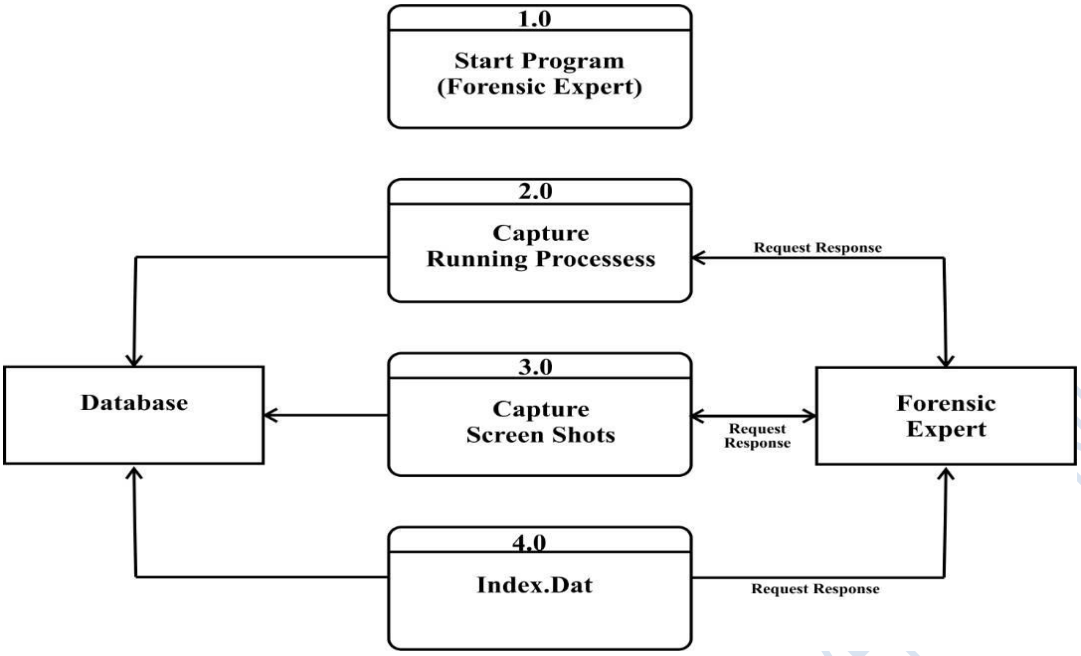


Fig 3.4 Data flow Diagram system Call Out function

The Data flow diagram shown in fig 3.3 is basically an interaction in the forensic expert interface. Once the forensic expert passes the authentication test, he can view the processes, the screenshots and Index. Dat files.

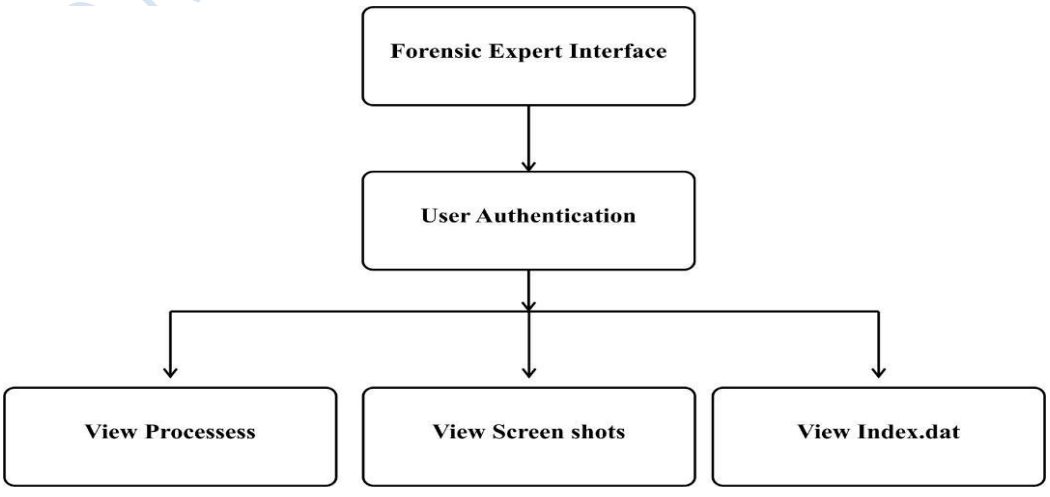


Fig 3.5. Data flow Diagram interaction in the website interface

Below is the list of program modules that make up the system.

Table 3.2 Specification of Program Modules

S/N	Module	Description
1	Frm Login.Frm	This is the initial module where the user is expected to enter the type of assessment to gain access to the application
2	Frm Main Menu.Frm	This displays the main form
3	Frm Category.Frm	This is the module that displays all the categories of system activity.

Endnotes

1 A., Rathore, Quantitative Research-Characteristics, 2019.

2. H.K., Mohajan, Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*, *7*(1), 2018, pp.23-48.

3. K. Einola, & M., Alvesson, Behind the Numbers: Questioning Questionnaires. *Journal of Management Inquiry*, *30*(1), 2021, pp.102-114.

4. R.M., Miller, C.D. Chan, & L.B., Farmer, Interpretative Phenomenological Analysis: A Contemporary Qualitative Approach. *Counselor Education and Supervision*, *57*(4), 2018, pp.240-254.

5. J.W. Creswell, & M., Hirose, Mixed Methods and Survey Research in Family Medicine and Community Health. *Family Medicine and Community Health*, *7*(2), 2019.

6. A., Prappa, E., Papaioannou, & C., Kaklamanis, A Web Application for Scheduling Educational Visits. In Edulearn22 Proceedings*,* 2022, (pp. 274-282). IATED.

Chapter Four

Testing and Evaluation

The foundation of this study has been laid and all necessary explanations and definitions have been provided in previous chapters. Chapter two presented related works from which the insight of this study was developed. The software and hardware requirements used for the implementation of the system are presented in chapter three.

This chapter discusses the implementation of the objectives of which are to:

i. Develop a navigable and usable website suitable for monitoring threats.
ii. Integrate Tawk.to script to the website.
iii. Evaluate the performance of the system.

It summarily demonstrated the application menu and their functions are finally presented and concluded.

4.1 Implementation

A temporary website is designed and hosted online which serves as the platform to be monitored. The monitoring dashboard is launched which pops up a login page. At the login page, the administrator enters a username and password to gain access to the system. The administrator was able to view two users on the website and the actions they are carrying out while online. The system was able to capture the geographical location of the users and the MAC address of the system used, and any suspected user would be immediately banned from the website.

Figure 4.1: The research website

The website is developed to serve as a platform in which the activities would be easily monitored. It is structured in four categories to present information about:

- Cyber crime Monitorying System
- Monitor Control Login
- WordPress Admin
- Developer

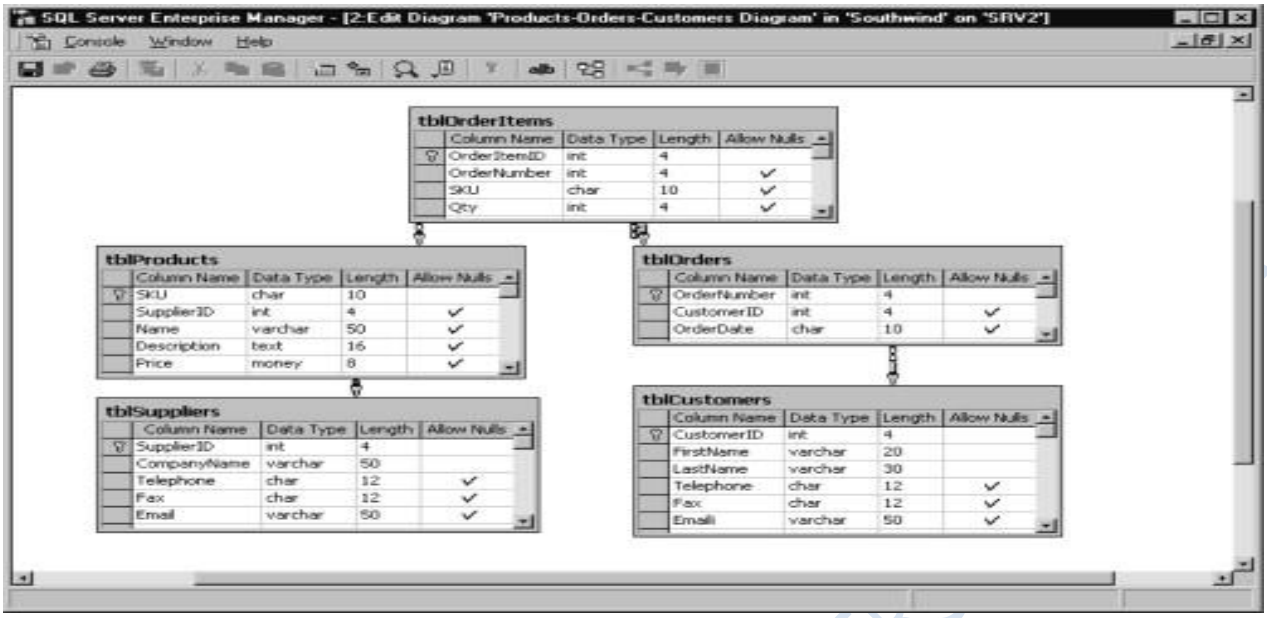


Figure 4.2: The Structure of the MySQL Database

The database design of the proposed system establishes the organizational structure of data and the relationships between them. It specifies each constraint that will be applied to the data. The purpose of the MySQL database is to serve as medium for storage of information of users that visit the website.

The screenshot below shows the process of integrating Tawk.to to the website

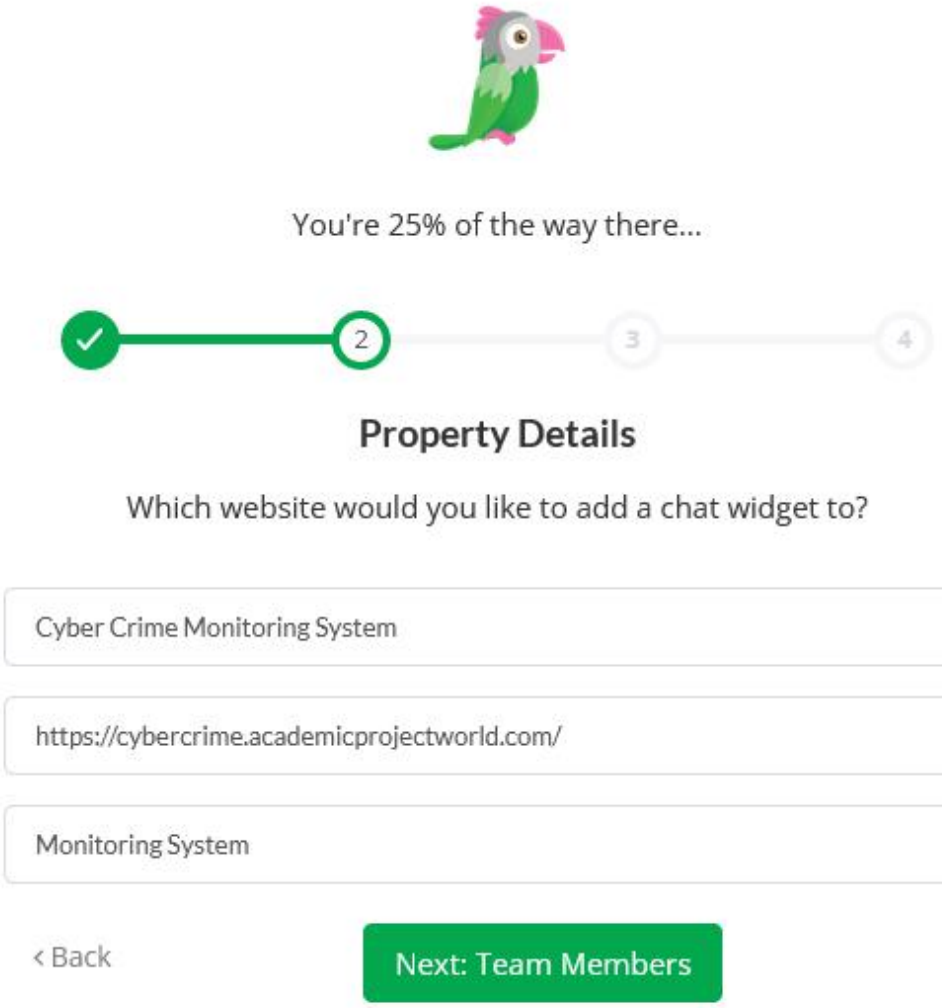


Figure 4.3: Tawk.to Integration to the Website

This screenshot shows the administator email address being linked to Tawk.to

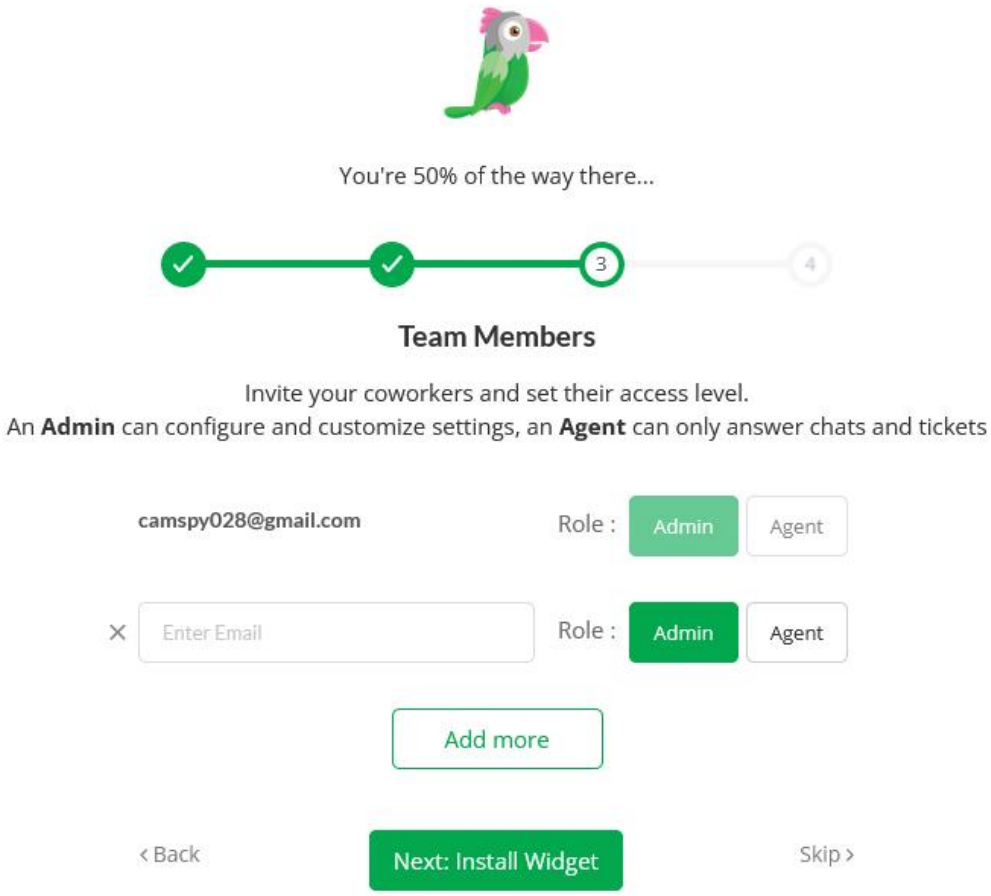
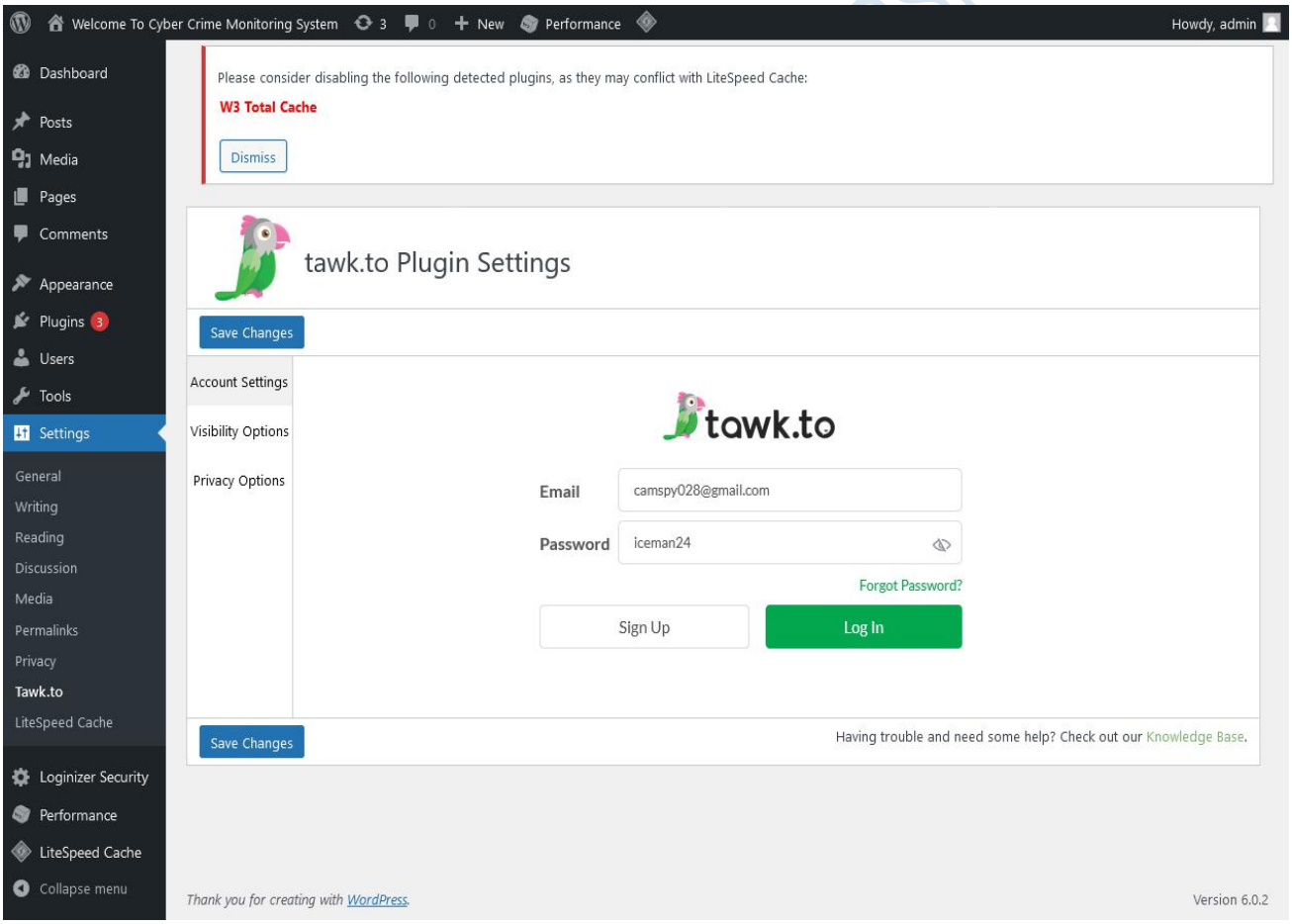


Figure 4.4: Administrator Email Linked to Tawk.to

Tawk.to Script Code Embeded to the Website

```
<!--Start of Tawk.to Script-->
<script type="text/javascript">
var Tawk_API=Tawk_API||{}, Tawk_LoadStart=new Date();
(function(){
var s1=document.createElement("script"),s0=document.getElementsByTagName("script")[0];
s1.async=true;
s1.src='https://embed.tawk.to/63443b4a54f06e12d899628a/1gf18f7a9';
s1.charset='UTF-8';
s1.setAttribute('crossorigin','*');
s0.parentNode.insertBefore(s1,s0);
})();
</script>
<!--End of Tawk.to Script-->
```



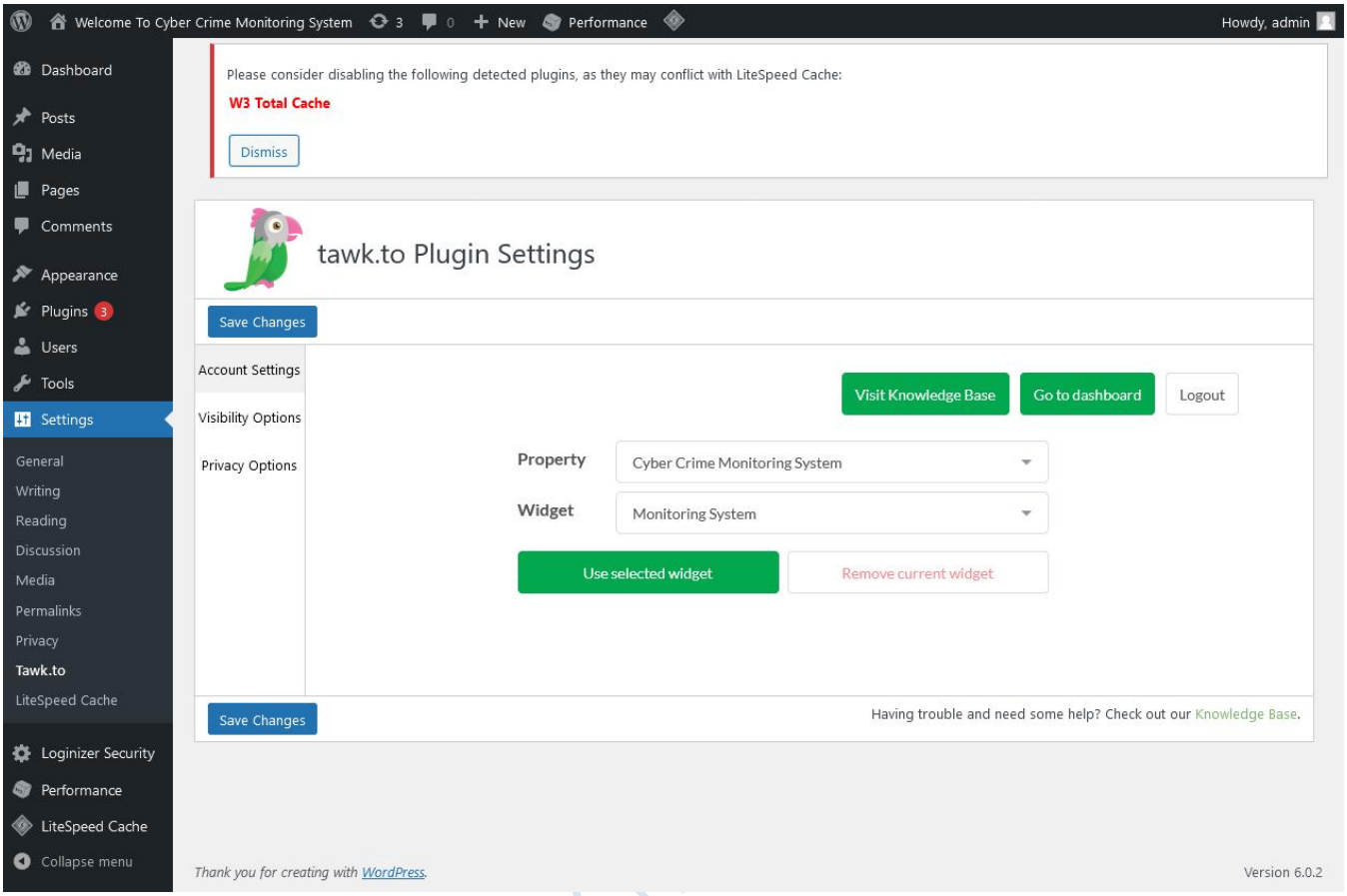


Figure 4.5: Tawk.to Plugin Settings

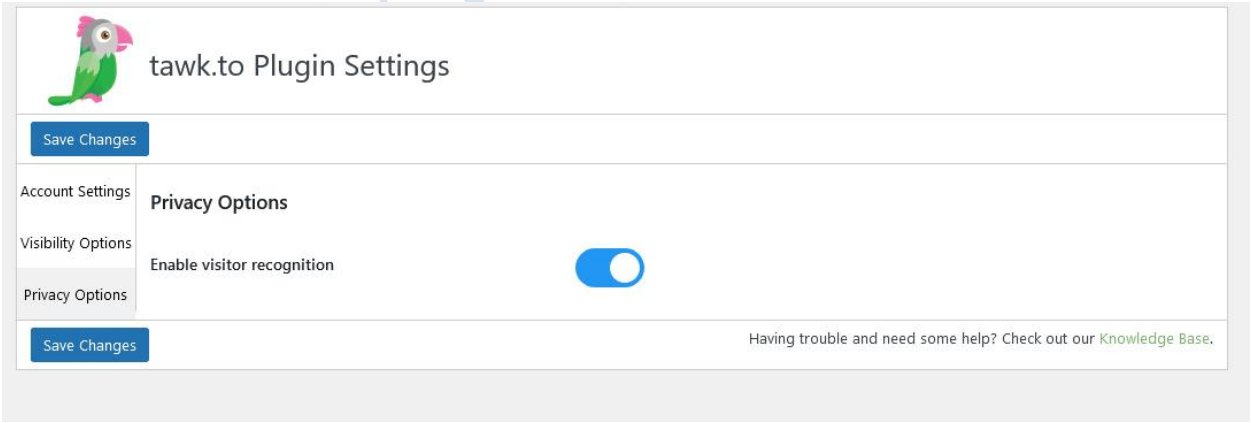


Figure 4.6: Continuation of Tawk.to Plugin Settings

Cybercrime Monitoring Dashboard Login Portal

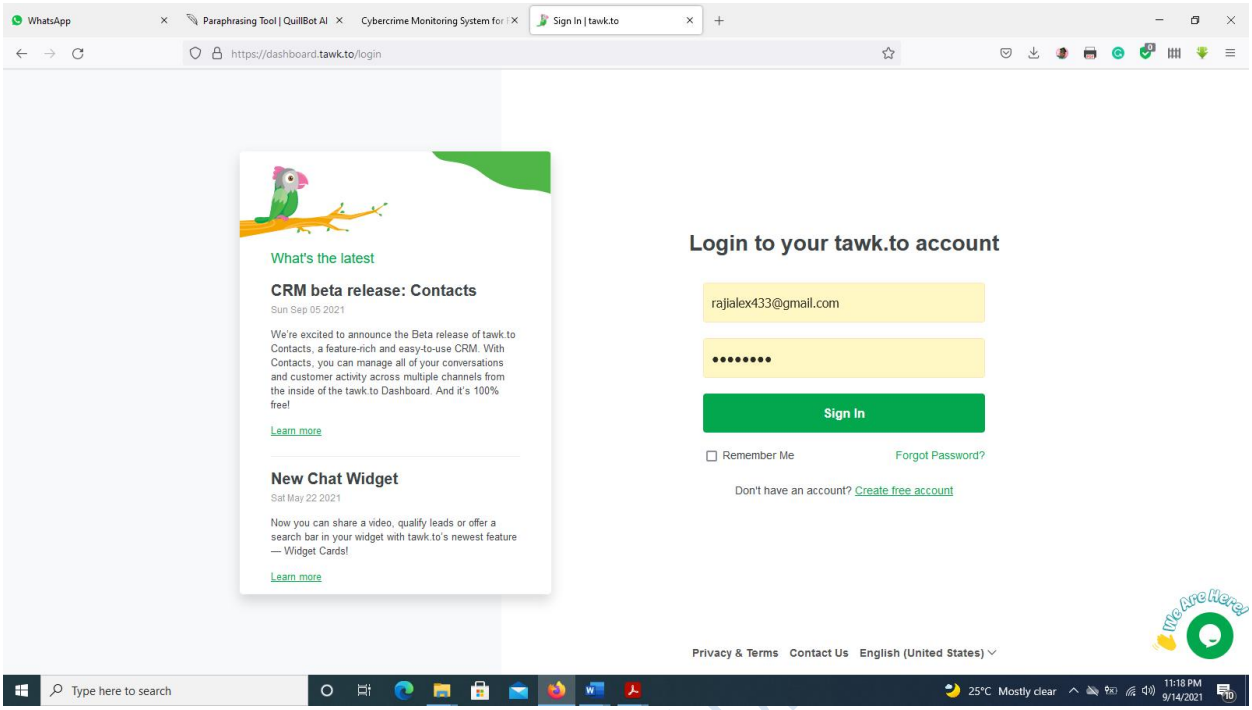


Figure 4.7: Cybercrime Monitoring Dashboard Login Portal

The Cybercrime Monitoring Dashboard Login Portal as shown in figure 4.7, is the screenshot system login page. The login Page contains two basic and necessary information, the username and password to gain access to the system. The username is the name of the administrator or any user authorized or allowed to gain access to the application while the password is a string of characters used to verify the identity of the user during the authentication process.

Three users detected on the monitored screen

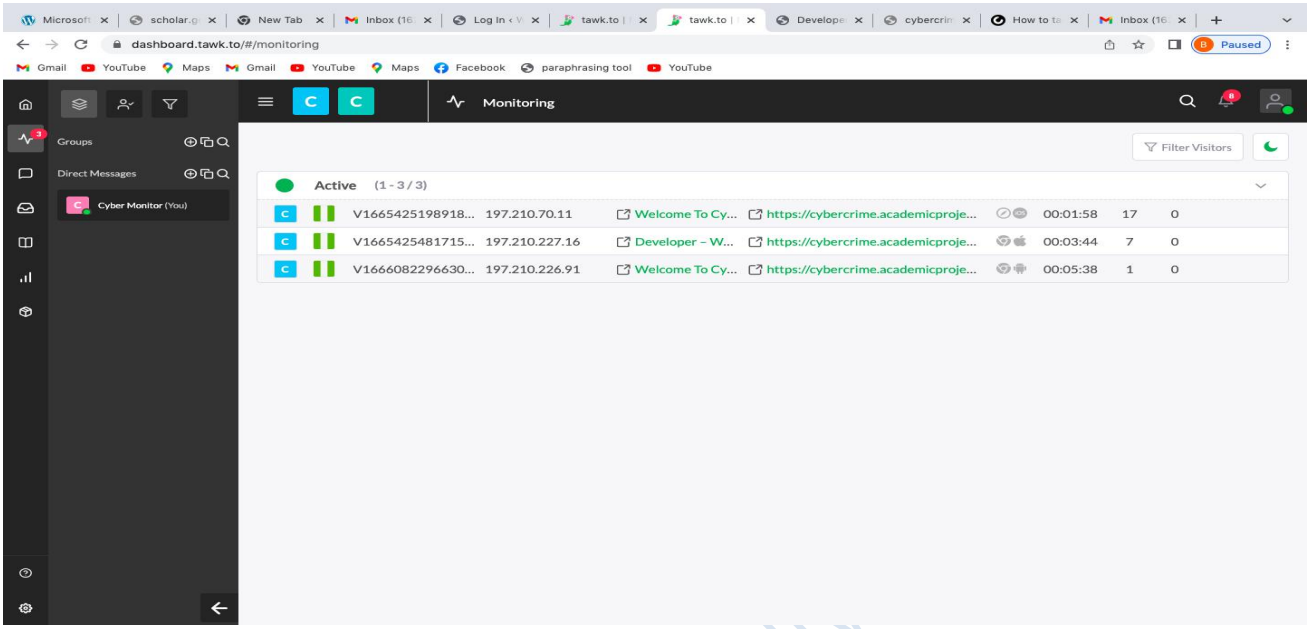


Figure 4.8: Three users detected on the Monitoring System

Three users detected on the monitoring system as shown in figure 4.8, the administrator was able to view three users on the website and the actions they are carrying out while online.

Detected User Location and IP address Detected

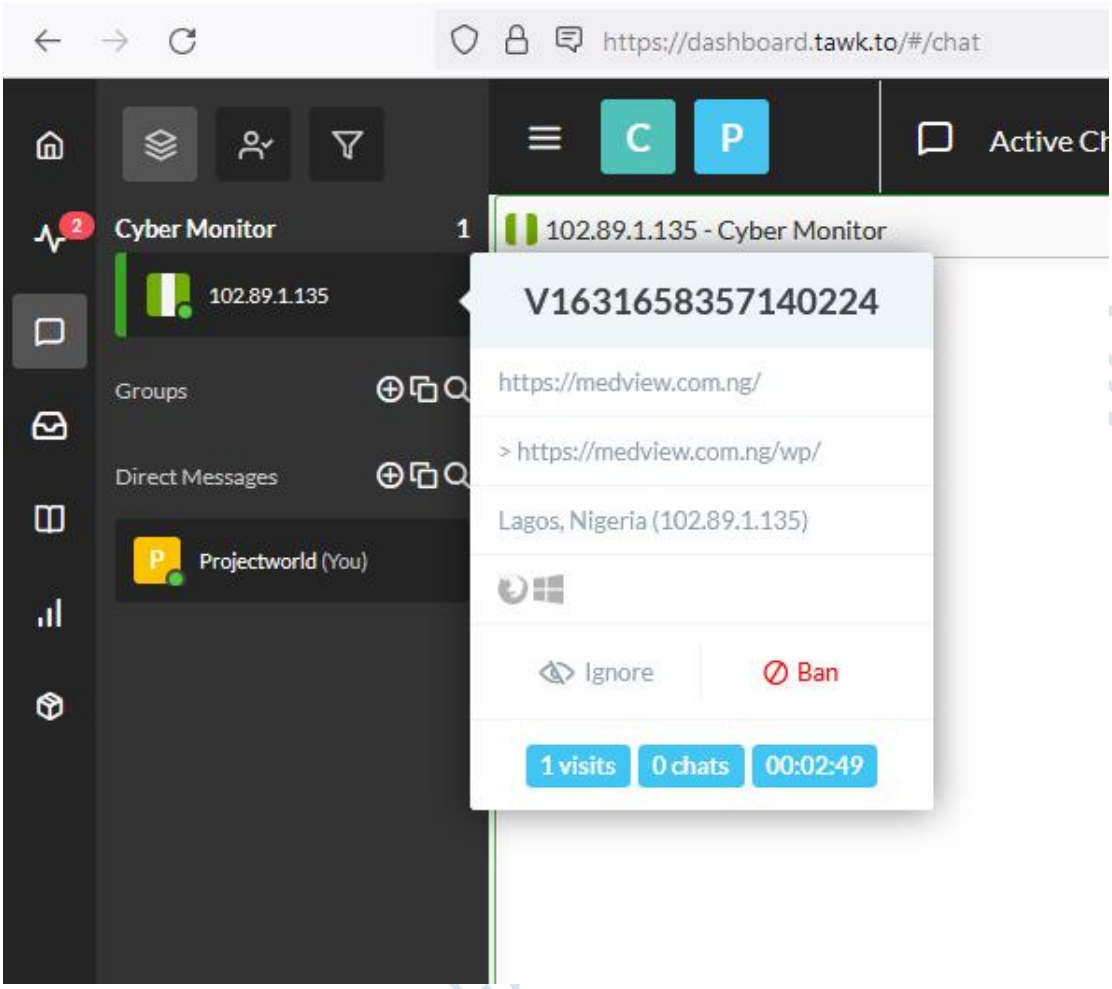


Figure 4.9: User Location and IP address Detected

Screenshot of User Location and IP address Detected as shown in figure 4.9, The system was able to capture the geographical location of the users and the MAC address of the system used, and any suspected user would be immediately banned from the website.

4.2 Testing

Software testing is an examination that is carried out in order to provide stakeholders with information about the quality of the software product or service under test. Product testing can

also provide an impartial, unbiased picture of the software, allowing the organization to realize and comprehend the risks associated with software implementation. The practice of executing a program or application with the goal of identifying software bugs (errors or other problems) and verifying that the software is fit for use is referred to as testing technique[1].

After the completion of the system, Unit testing was carried out to check the functionality of each component of the system or to know if the component are integrated as planned. When all the modules hav been successfully integrated and tested, complete system testing was carried out. The system testing helped ensured requirement and design conformance.

4.3 Performance Evalution

The performace evaluation of the system is done using System Usability Scale. System Usability Scale (SUS) is a standardize questionnaire based method for the assessment of preceieved usability. It has proven to be quick but not dirty[2]. SUS was developed by John Brooke in the year 1996 reflected a strong need in usability community for a tool that could quickly and easily collected a user's subjective rating of a product usability[3].

4.3.1 System Usability Scale Questionnaire

The evaluation questionnaire(see Appendic B) was given to twenty (20) participants to gain their feedback about the functionality of the usability of the application. The System Usability Scale is the usability evaluation framework employed.

4.3.2 Evaluation using System Usability Scale(SUS)

The System Usability Scale (SUS) is used to determine the level of satisfaction, effectiveness and efficiency. The SUS consis of ten (10) standardized question based on 4-point Likert Scale where Strongly Disagree = 1, Disagree = 2, , Agree = 3, Strongly Agree = 4.

SUS uses complex scoring system because it comprises of five (5) positive odd numbered questions and five (5) even negative numbered questions.

SUS score = (X +Y) * 2.5 where

X = Add up the total score of all odd numbered questions then subtract 5 while

Y = Add up the total score of all even numbered questions then subtract from 25.

$$\text{Average} = \frac{\sum \text{ of all SUS Scores}}{\text{Number of Participants}}$$

4.3.3 SUS Scores for Participants of the Cybercrime Monitoring System

Table 4.1: SUS Score for Users of the Cybercrime Monitoring System Using 4-Point Likert Scale

Users	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score	NPS
1	4	1	3	1	3	1	4	1	4	1	87.5	Promoter
2	4	1	4	2	4	2	4	2	4	1	80.0	Passive
3	4	1	3	2	4	2	4	1	4	1	80.0	Promoter
4	3	1	4	2	4	1	4	1	4	1	82.5	Promoter
5	4	1	4	1	4	1	4	1	4	1	87.5	Promoter
6	4	1	4	2	4	1	3	1	3	2	77.5	Passive
7	4	1	4	1	4	1	4	1	4	1	87.5	Promoter
8	4	2	4	1	4	2	4	1	4	1	82.5	Promoter
9	3	1	4	2	4	2	4	2	4	2	75.0	Passive
10	4	1	3	2	3	1	4	2	3	2	72.5	Passive
11	4	2	4	2	3	1	4	1	4	2	77.5	Passive
12	3	1	4	2	4	2	3	2	4	1	75.0	Passive
13	4	2	4	1	4	2	4	1	4	1	82.5	Promoter
14	3	1	3	1	4	2	4	2	3	1	75.0	Passive
15	4	1	4	1	3	1	3	1	4	2	80.0	Promoter

16	4	1	3	2	4	1	4	1	4	1	82.5	Promoter
17	4	1	3	1	4	1	4	1	4	1	85.0	Passive
18	4	1	4	1	4	2	4	1	3	1	82.5	Promoter
19	3	1	4	1	4	1	4	2	4	1	82.0	Promoter
20	3	1	4	1	4	1	4	1	4	2	82.5	Passive

User 1 = 87.5, User 2 = 80.0 User 3 = 80.0, User 4 = 82.5, User 5 = 87.5, User 6 = 77.5, User 7 = 87.5, User 8= 82.5, User 9 = 75.0, User 10 = 72.5, User 11 = 77.5, User 12 = 75.0, User 13 = 82.5, User 14 = 77.5, User 15 = 80.0, User 16 = 82.5, User 17= 85.0, User 18 = 82.5, User 19 = 85.0, User 20 = 82.5

Average = $\frac{\sum \text{ of all SUS Scores}}{\text{Number of Participants}}$

Sum of all SUS Scores for all Participants = 87.5 + 80.0 + 80.0 + 82.5 + 87.5 + 77.5 + 87.5 + 82.5 + 75.0 + 72.5 + 77.5 + 75.0 + 82.5 + 75.0 + 80.0 + 82.5 + 85.0 + 82.5 + 82.0 + 82.5

$= \frac{1617}{20} = 80.9$

The Average SUS score = 80.9

4.3.3.1 Lowest and Highest SUS Score

The Lowest and Highest SUS score for the cybercrime monitoring system is stated at 72.5 and 87.5 respectively.

4.3.4 Usability Evaluation

System Usability Scale (SUS) scores becomes meaningful by normalizing scores to produce percentile ranking

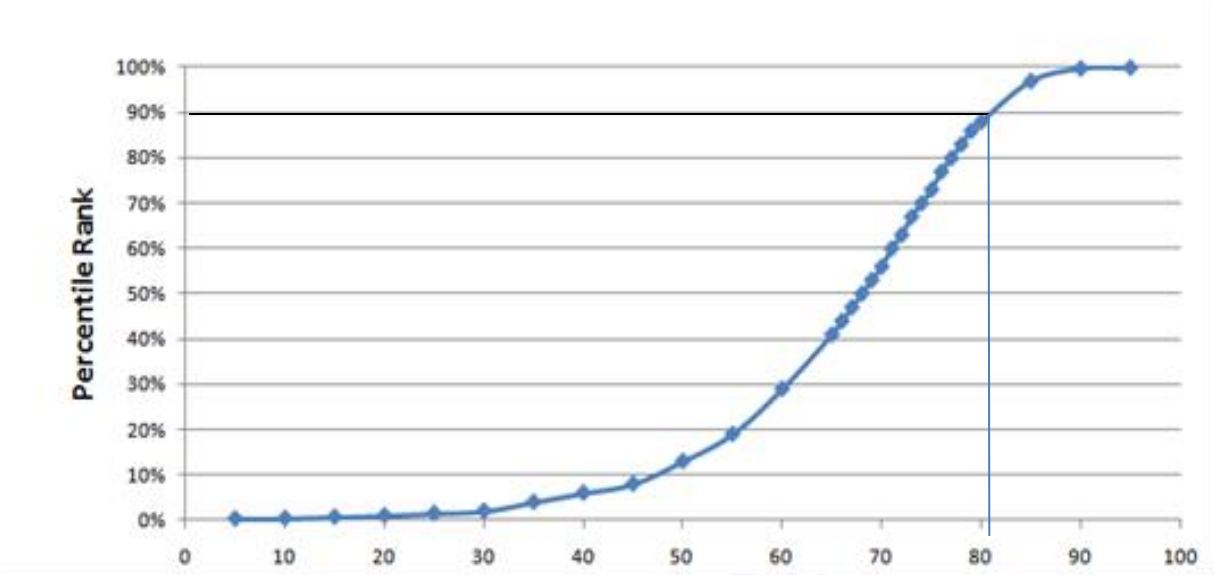


Figure 4.10 Percentile Ranking for Common SUS Scores

The raw and mean SUS score is 80.9 for the cybercrime monitoring system. It was normalized to percentile ranking 90.

Table 4.2: Percentiles, Grades, Adjectives, and NPS Categories to Describe Raw SUS Scores

Grade	SUS	Percentile range	Adjective	Acceptable	NPS
A+	84.1-100	96-100	Best Imaginable	Acceptable	Promoter
A	80.8-84.0	90-95	Excellent	Acceptable	Promoter
A-	78.9-80.7	85-89		Acceptable	Promoter
B+	77.2-78.8	80-84		Acceptable	Passive
B	74.1 – 77.1	70 – 79		Acceptable	Passive
B-	72.6 – 74.0	65 – 69		Acceptable	Passive
C+	71.1 – 72.5	60 – 64	Good	Acceptable	Passive
C	65.0 – 71.0	41 – 59		Marginal	Passive
C-	62.7 – 64.9	35 – 40		Marginal	Passive
D	51.7 – 62.6	15 – 34	OK	Marginal	Detractor
F	25.1 – 51.6	2– 14	Poor	Not Acceptable	Detractor
F	0-25	0-1.9	Worst Imaginable	Not Acceptable	Detractor

Source: Online (2022)

The percentile rank of 90 for the System was interpreted to be grade A. This indicate that the system was excellent and acceptable and the users were promoters. The users will not discourage others from using the proposed system as illustrated above.

4.3.5 Comparative Evaluation Analysis

A comparative Analysis of the system has been carried out to establish the functionality of the study as described in table 4.3 while the bar chart in figure 4.7 Shows the graphical analysis of the system. The study was compared with the Initial System and the result shows that the cybercrime monitoring system has an edge over the existing system.

Table 4.3 SUS Score for Cybercrime Monitoring System

Users	**SUS Score** CMS	SUS Initial System
1	87.5	70.0
2	80.0	72.5
3	80.0	75.0
4	82.5	80.0
5	87.5	72.5
6	77.5	77.5
7	87.5	70.0
8	82.5	70.0
9	75.0	72.5
10	72.5	77.5
11	77.5	80.0
12	75.0	75.0

13	82.5	70.0
14	75.0	72.5
15	80.0	77.5
16	82.5	70.0
17	85.0	72.5
18	82.5	70.0
19	82.0	75.0
20	82.5	80.0

From the result in table 4.3 The raw and mean SUS score is 80.9 for the cybercrime monitoring system. It was normalized to percentile ranking 90. This indicate that the system was excellent and acceptable and the users were promoters. The users will not discourage others from using the proposed system while the mean SUS score for the initial system is 75.25 was normalized to percentile ranking 72. This indicate that the system is acceptable and the users were passive. The users will discourage others from using the system.

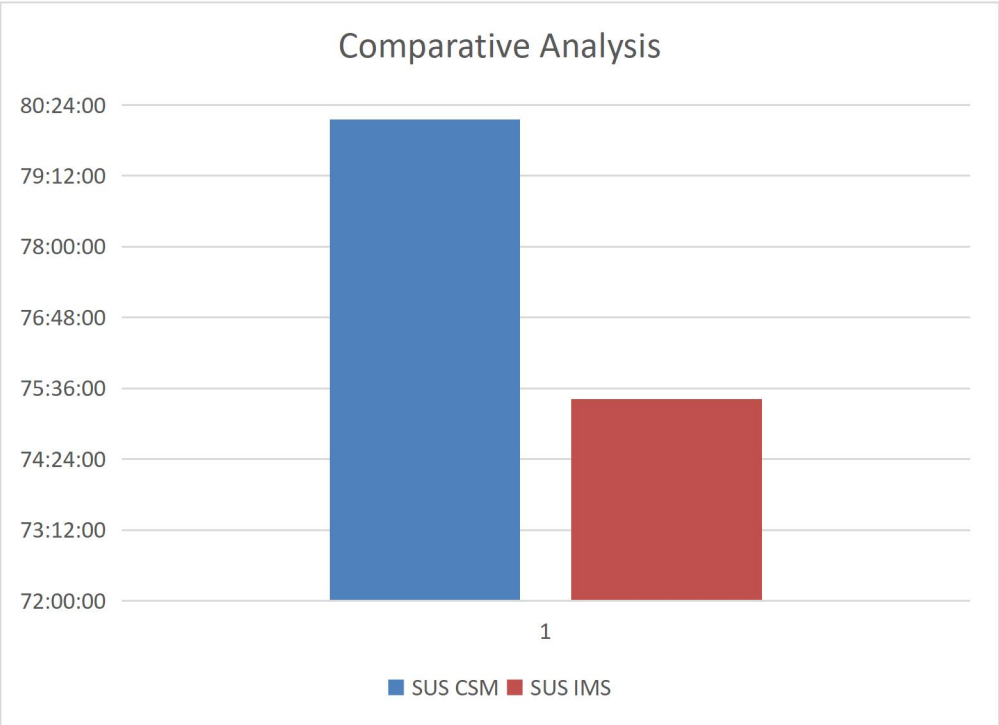


Figure 4.11: Graphical Representation of the Comparative Analysis

Endnotes

1. L., Cayola & J.A., *Macías,* Systematic Guidance on Usability Methods in User-centered Software Development. *Information and Software Technology*, *97*, 2018, pp.163-175.

2. J.R., Lewis, The System Usability Scale: Past, Present, and Future, *International Journal of Human–Computer Interaction, 34*(7), 2018, pp.577-590.

3. A., Bangor, P.T, Kortum, & J.T., Miller, An Empirical Evaluation of the System Usability Scale. *Internation Journal of Human–Computer Interaction*, *24*(6), 2008, pp.574-594.

Chapter Five

Conclusion

5.1 Summary of Results

The aim of this work is to implement a cybercrime monitoring system that will effectively monitor cyber criminals as at the time of access to aid Online Expect to perform their work optimally. The work began with an introduction to the framework that comprises the main focus of the research. A brief introduction of computer forensic and cybercrime which was the main focus was discussed. It went ahead to review related literatures. The design and limitation of each reviewed work was noted, from which the insight into the reasons for this work arose. After identifying the limitation of existing works, an improved algorithm was proposed and implemented.

For the studies reviewed, it was concluded that there was need for an improved monitoring system

i. Develop a navigable and usable website suitable for monitoring threats.
ii. Integrate Tawk.to script to the website.
iii. Evaluate the performance of the system.

With the increasing volume and sophistication of cyber-attacks, cyber security is an important factor for individuals, families, businesses, and governments. To effectively tackle this threat, all hands must be on deck, because cyber-attacks, by definition, require a loophole or access point through which the attack may be duplicated. Infected devices have a habit of infecting other devices, and compromised systems make everyone susceptible in the end.

5.1.1 Conclusion

Cyber security is a continual process that must be updated on a regular basis. As new programs and cyber criminals discover and exploit new vulnerabilities in computer programs and systems, network defenders are constantly fighting back. The fundamental principles of cyber security are the same as they are for physical and general security. The process begins with a vulnerability assessment. Vulnerability assessment includes risk assessment and threat identification, as well as documenting the findings and developing an action plan. One of the most serious risks to cyber security is internet vulnerability. Any web-based system has significant security flaws due to the use of e-mail, web browsers, and other technologies.

Governments all across the world keep massive amounts of personal data and records on their residents, as well as sensitive government secrets, making them easy targets. Despite this, many government institutions face challenges such as inadequately secured infrastructure, a lack of awareness, and competing budget and resource objectives. Better security enables government agencies to deliver dependable services to the public, maintain citizen-to-government communications, safeguard sensitive information, and defend national security. Taking into consideration the increase in the rate of crimes using computers, one has to take every security measure to protect his cybers space.

5.2 Contribution to Knowledge

1. This research contributed theoretically to the existing body of knowledge through a more extensive understanding of the emerging technologies, with potential for future research.

2. This system is executed at a minimal cost and will reduce the difficulty of integrating a monitoring system to a website which will make individual, organization and government agencies find it easier to protect their website effectively.

5.5 Suggested Areas for Research

This work has been able to answer all its research questions, thereby accomplished all of its objectives as well. It is therefore advised that the listed below be considered in the future.

1. To combat cybercrime, you need to establish a special cybercrime police and train them on the use of information technology in cyber crime.

2. Cybersecurity education should be implemented at all levels of education to educate Internet users and their outlook on the threats they may face when using the Internet.

3. Hardware and software developers should be persuaded to incorporate technical solutions to common cyber anxieties into their new products.

4. All websites on the Internet must specify and include monitoring software for security checks against threats so that cyber police can check for threats to identify and arrest criminals.

5. Organizations need to take strict security measures to protect their digital data.

Bibliography

Journals

Agana-correspondence, M.A., Cyber Crime Detection and Control Using the Cyber User Identification Model, 2015.

Agana, M.A. & Wario, R., A Multi-level Evidence-based Cyber Crime Prosecution Information System. *International Journal of Engineering & Technology*, *7*(3.19), 2018, pp.39-48.

Aiken, M., Farr, R. & Witschi, D., Cyberchondria, Coronavirus, and Cybercrime: A Perfect Storm. *In Handbook of Research on Cyberchondria, Health Literacy, and the Role of Media inSociety's Perception of Medical Information,* 2022, (pp. 16-34). IGI Global.

Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S. & Khan, M.K., Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, *8*, 2020, pp.137293-137311.

Al-Mousa, M.R., Generic Proactive IoT Cybercrime Evidence Analysis Model for Digital Forensics. *In International Conference on Information Technology (ICIT),* 2021, (pp. 654-659). IEEE.

Alagarsamy, S., Selvaraj, K., Govindaraj, V., Kumar, A.A., HariShankar, S. & Narasimman, G.L., , September. Automated Data Analytics Approach for Examining the Background Economy of Cybercrime. *In Third International Conference on Inventive Research in Computing Applications (ICIRCA,* 2021 (pp. 332-336). IEEE.

Alenezi, M.N., Alabdulrazzaq, H., Alshaher, A.A. & Alkharang, M.M., Evolution of Malware Threats and Techniques: *A Review. International Journal of Communication Networks and Information Security*, *12*(3), 2020, pp.326-337.

Alese, T., Owolafe, O., Thompson, A.F. & Alese, B.K., A User Identity Management System for Cybercrime Control. *Nigerian Journal of Technology, 40*(1), 2021, pp.129-139.

ALI, N., Samsuri, S., SEMAN, M.A., BROHI, I. & Shah, A., Cybercrime an Emerging Challenge for Internet Users: An Overview. *Sindh University Research Journal (Science Series)*, *50*(3D), 2018, pp.55-58.

Ba, Y., Understanding Cybercrime and Developing a Monitoring Device, 2017.

Bangor, A., Kortum, P.T, & Miller, J.T., An Empirical Evaluation of the System Usability Scale. *Internation Journal of Human–Computer Interaction, 24*(6), pp.574-594, 2008.

Canizo, M., Conde, A., Charramendieta, S., Minon, R., Cid-Fuentes, R.G. & Onieva, E., Implementation of A Large-Scale Platform for Cyber-Physical System Real-Time Monitoring. *IEEE Access, 7*, 2019, pp.52455-52466.

Cayola L., & *Macías,* J.A., Systematic Guidance on Usability Methods in User-centered Software Development. *Information and Software Technology*, *97*, 2018, pp.163-175.

Chatfield, A.T. & Reddick, C.G., A Framework for Internet of Things-Enabled Smart Government: A Case of Iot Cybersecurity Policies and Use Cases In US Federal Government. *Government Information Quarterly, 36*(2), 2019, pp.346-357.

Chigozie-Okwum, C.C., Michael, D.O., & S.G., Ugboaja, Computer Forensics Investigation; Implications for Improved Cyber Security In Nigeria. *AFRREV STECH: An International Journal of Science and Technology, 6*(1), 2017, pp.59-73.

Chinedu, P.U., Nwankwo, W., Masajuwa, F.U. and Imoisi, S., Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models. *Review of International Geographical Education Online, 11*(7), 2021.

Choi, J.H. & Lee, H.J., A Study on the Real-time Cyber Attack Intrusion Detection Method. *Journal of the Korea Convergence Society*, *9*(7), 2018, pp.55-62.

Choi, K.S., Lee, C.S. & Louderback, E.R., Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. *The Palgrave Handbook of International Cybercrime and Cyberdeviance,* 2020, pp.27-43.

Choudhary, A.S., Choudhary, P.P. and Salve, S., November. A Study on Various Cyber Attacks And a Proposed Intelligent System for Monitoring Such Attacks. *In 3rd International Conference on Inventive Computation Technologies (ICICT),* 2018, (pp. 612-617). IEEE.

Creswell, J.W. & Hirose, M., Mixed Methods and Survey Research in Family Medicine and Community Health. *Family Medicine and Community Health*, *7*(2), 2019

Cristea, L.M., Current Security Threats in the National and International Context. *Journal of Accounting and Management Information Systems*, 2020, *19*(2), pp.351-378.

Eniola, K. & Alvesson, M., Behind the Numbers: Questioning Questionnaires. *Journal of Management Inquiry*, *30*(1), 2021, pp.102-114.

Dhaka, P. & Johari, R., Crib: Cyber Crime Investigation, Data Archival and Analysis Using Big Data Tool. *In International Conference on Computing, Communication and Automation (ICCCA),* 2016, (pp. 117-121). IEEE.

Drew, J.M., A Study of Cybercrime Victimisation and Prevention: Exploring The Use Of Online Crime Prevention Behaviours And Strategies. *Journal of Criminological Research, Policy and Practice,* 2020.

Dupont, B., Enhancing the Effectiveness of Cybercrime Prevention Through Policy Monitoring. *Journal of Crime and Justice, 42*(5), 2019, pp.500-515.

Fachkha, C., Security Monitoring of the Cyber Space. *In Cybersecurity policies and strategies for cyberwarfare prevention,* 2015, (pp. 62-83). IGI Global.

Farsole, A.A., Kashikar, A.G. & Zunzunwala, A., Ethical Hacking. *International Journal of Computer Applications, 1*(10), 2010, pp.14-20.

Frank, I., & Odunayo, E., Approach to Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in science, engineering and education, 1*(1), 2013, pp.100-110.

Goyal, N., & Goyal, D., Cyber Crime in the Society: Security Issues, Preventions and Challenges. *Research Journal of Engineering and Technology, 8*(2), 2017, p.73.

Gursoy, U.T., A Study on Precautions that are Taken by it Firms to Prevent Cybercrime, 2007.

Hahanov, V., Mishchenko, O., Soklakova, T., Abdullayev, V., Chumachenko, S. & Litvinova, E., 2019. Cyber-Social Computing. *In Green IT Engineering: Social, Business and Industrial Applications* (pp. 489-515). Springer, Cham

Hao, T., Zhou, J., Cheng, Y., Huang, L. & Wu, H., User Identification In Cyber-Physical Space: A Case Study on Mobile Query Logs and Trajectories. *In Proceedings of the 24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems,* 2016, (pp. 1-4).

Horgan, S., Collier, B., Jones, R. & Shepherd, L., Reterritorialising the Policing of Cybercrime In the Post-COVID-19 Era*: Towards a Vision of Local Democratic Cybercrime Policing*, 2021.

Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. & Mahmood, S., Cyber Security Threats and Vulnerabilities*:* A Systematic Mapping Study. *Arabian Journal for Science and Engineering, 45*(4), 2020, pp.3171-3189.

Jaiswal, M., Cybercrime Categories and Prevention. Manishaben Jaiswal," *Cybercrime Categories And Prevention", International Journal Of Creative Research Thoughts (Ijcrt), ISSN*, 2019, pp.2320-2882.

Javed, A.R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K. & Gadekallu, T.R., A Comprehensive Survey on Computer Forensics: State-of-the-art, Tools, Techniques, Challenges, and Future Directions. IEEE Access*,* 2022.

Kaplesh, P. & Goel, A., Firewalls: A study on Techniques, Security and Threats.

Khan, S., Gani, A., Wahab, A.W.A., Shiraz, M. & Ahmad, I., Network forensics: Review, Taxonomy and Open Challenges. *Journal of Network and Computer Applications*, *66*, 2016, pp.214-235

Lewis, J.R., The System Usability Scale: Past, Present, And Future, *International Journal of Human–Computer Interaction*, *34*(7), 2018, pp.577-590.

Lee, J., Kim, J., Kim, I. & Han, K., Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles. IEEE Access, *7*, 2019, pp.165607-165626

Lekha, K.C. & Prakasam, S., Implementation of Data Mining Techniques for Cyber Crime Detection. *International Journal of Engineering, Science and Mathematics, 7*(4), 2018, pp.607-613.

Li, C.Y., Huang, C.C.F., LaiLee, S.L. & Wu, J., A Comprehensive Overview of Government Hacking Worldwide. *IEEE Access*, *6*, 2018. pp.55053-55073.

Li, X., Regulation Of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology, 9*(2), 2015, p.185.

Michael, K., The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Vol. 31. 2012.

Miller, R.M., Chan, C.D. & Farmer, L.B., Interpretative Phenomenological Analysis: A Contemporary Qualitative Approach. *Counselor Education and Supervision*, *57*(4), 2018, pp.240-254.

Mohajan, H.K., Qualitative Research Methodology in Social Sciences and Related Subjects. *Journal of Economic Development, Environment and People*, *7*(1), 2018, pp.23-48.

Mushtaque, K., Ahsan, K. & Umer, A., Digital Forensic Investigation Models: An Evolution Study. *JISTEM-Journal of Information Systems and Technology Management*, *12*(2), 2015, pp.233-243.

Nwokike, L.I., Legal Design and Implementation of Cyber Crime Monitoring System In Nigeria. *UNIZIK Law Journal*, *16*(1), 2020, pp.92-107.

Ohnof, K., Koikef, H. & Koizumi, K., IPMatrix: An Effective Visualization Framework for Cyber Threat Monitoring. *In Ninth International Conference on Information Visualisation* (IV'05*),* 2005, (pp. 678-685). IEEE

Paul, P. & Aithal, P.S., Cyber Crime: Challenges, Issues, Recommendation and Suggestion in Indian Context. *International Journal of Advanced Trends in Engineering and Technology(IJATET)*, *3*(1), 2018, pp.59-62.

Prakash, F., Sadawarti, H.K. & Baskar, K., Cyber Crime: Challenges and its Classification. *In International Multi-disciplinary Academic Research Conference IMARC*, 2019,
(pp. 2-4).

Prappa, A., Papaioannou, E., & Kaklamanis, C., A Web Application for Scheduling Educational Visits. *In Edulearn22 Proceedings,* 2022, (pp. 274-282). IATED.

Rathore, A., Quantitative Research-Characteristics, 2019.

Richardson, T. & Thies, C.N., Secure Software Design. Jones & Bartlett Publishers, 2013.

Rohit, K.A.L.A.K.U.N.T.L.A., Babu, V.A. & Reddy, K.R., Cyber Security. *HOLISTICA–Journal of Business and Public Administration, 10*(2), 2019, pp.115-128.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A.D., Murray, M. & SPerl, J., Computer Security Incident Response Team Development and Evolution. *IEEE Security & Privacy*, *12*(5), 2014, pp.16-26.

Shaukat, K., Luo, S., Chen, S. and Liu, D., Cyber Threat Detection Using Machine Learning Techniques*:* A Performance Evaluation Perspective*. In International Conference on Cyber Warfare and Security (ICCWS),* 2020, (pp. 1-6). IEEE.

Sindhu, K.K., Kombade, R., Gadge, R. & Meshram, B.B., Forensic Investigation Processes for Cyber Crime and Cyber Space. *In Proceedings of International Conference on Internet Computing and Information Communications,* 2014, (pp. 193-206). Springer, New Delhi.

Umanailo, M.C.B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D.N., Ganefwati, R., Daulay, P., Meifilina, A., Alamin, T., Fitriana, R. & Sutomo, S., Cybercrime Case as Impact Development of Communication Technology that Troubling Society. *International Journal Science Technology Res, 8*(9), 2019, pp.1224-1228.

Ushmani, A., Ethical Hacking. *International Journal of Information Technology (IJIT), 4*(6), 2018.

Veena, K. & Meena, K., Performance Evaluation Of Cyber Criminal Detection Techniques. *International Journal of Simulation--Systems, Science and Technology, 19*(4), 2018, pp.4-1.

Vooradi, V.B. and Jadhav, L., Ethical Hacking Techniques and its Preventive Measures forNewbies, 2019.

Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M.& Dehghantanha, A., *Threats On* The Horizon: Understanding Security Threats in the Era of Cyber-Physical Systems. *The Journal of Supercomputing, 76*(4), 2020, pp.2643-2664.

Xiu, W. & Li, X., The Design of Cybercrime Spatial Analysis System. *In 4th IEEE International Conference on Information Science and Technology,* 2014, (pp. 132-135). IEEE.

Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab A. & Malli, M., Cyber-physical Systems Security: Limitations, Issues and Future Trends. *Microprocessors and microsystems*, *77*, 2020,p.103201

Zhou, S., Wang, X. & Yang, Z., Monitoring and Early Warning of New Cyber-Telecom Crime Platform Based on BERT Migration Learning. *China Communications, 17*(3), 2020, pp.140-148

Zhu, K. & Zhang, Y., A Cyber-Physical Production System Framework of Smart CNC Machining Monitoring System. *IEEE/ASME Transactions on Mechatronics, 23*(6), 2018, pp.2579-2586.

Zissis, D., & Lekkas, D., Addressing Cloud Computing Security Issues. *Future Generation computer systems*, *28*(3), 2012, pp.583-592.

Appendix A
(Program Codes)

Index.php

```
<?php include_once("header.php"); include("login.php"); include_once("footer.php");
?>
```

Header.php

```
<?php
   include("server.php");
?>
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<meta name="description" content="">
<meta name="author" content="">
<title>Crime Record Management System</title>
<!-- Custom fonts for this template-->
<link href="vendor/fontawesome-free/css/all.min.css" rel="stylesheet" type="text/css">
<link
href="https://fonts.googleapis.com/css?family=Nunito:200,200i,300,300i,400,400i,600,600i,70
0,700i,800,800i,900,900i" rel="stylesheet">
<!-- Custom styles for this template-->
<link href="css/sb-admin-2.min.css" rel="stylesheet">
<link href="vendor/jquery/jquery-ui.min.css" rel="stylesheet">
<link href="css/style.css" rel="stylesheet">
</head>
```

Login.php

```
<?php
   include_once("header.php");
?>
<li class="nav-item">
<li class="nav-item">
<a class="nav-link js-scroll-trigger" href="main/index.php"><h6><strong>BACK TO
HOME</h6></strong></a>
</li>
<body class="bg-gradient-danger">
<div class="container">
<!-- Outer Row -->
<div class="row justify-content-center">
<div class="col-xl-10 col-lg-12 col-md-9">
```

```
<div class="card o-hidden border-0 shadow-lg my-5">
<div class="card-body p-0">
<!-- Nested Row within Card Body -->
<div class="row d-flex justify-content-center">
<div class="col-lg-6">
<div class="p-5">
<div class="text-center">
<h1 class="h9 text-gray-900 mb-4">Welcome!</h1>
</div>
<form class="user"method="post" action="login.php">
<?php include('errors.php'); ?>
<div class="form-group">
<input type="text" class="form-control form-control-user" id="exampleInputEmail" aria-describedby="emailHelp" placeholder="User Name" name="username">
</div>
<div class="form-group">
<input type="password" class="form-control form-control-user" id="exampleInputPassword" placeholder="Password"  name="password">
</div>
<div class="form-group">
<div class="custom-control custom-checkbox small">
<input type="checkbox" class="custom-control-input" id="customCheck">
<label class="custom-control-label" for="customCheck">Remember Me</label>
</div></div>
<button type="submit" class="btn btn-danger btn-user btn-block" name="login_user">
                Login
</button>
</form>
<hr>
<div class="text-center">
<a class="small" href="forgot-password.php">Forgot Password?</a>
</div>
</div>
</div></div>
</div>
</div>

</div>

</div>

</div>

<?php
  include("footer.php");
 ?>
```

Footer.php

```
<!-- Bootstrap core JavaScript-->
<script src="vendor/jquery/jquery.min.js"></script>
<script src="vendor/jquery/jquery-ui.min.js"></script>
<script src="vendor/bootstrap/js/bootstrap.bundle.min.js"></script><!-- Core plugin JavaScript-->
<script src="vendor/jquery-easing/jquery.easing.min.js"></script>
<!-- Custom scripts for all pages-->
<script src="js/sb-admin-2.min.js"></script>
<!-- Page level plugins -->
<script src="vendor/datatables/jquery.dataTables.min.js"></script>
<script src="vendor/datatables/dataTables.bootstrap4.min.js"></script>
<!-- Page level custom scripts -->
<script src="js/demo/datatables-demo.js"></script>
<script>
  $( function() {
    $( "#datepicker" ).datepicker({ dateFormat: 'yy-mm-dd' });
  } );
</script>
</body>
</html>
```

Home.php

```
<?php include("layout-top.php") ?>
<?php include("report/criminal.php") ?>
        <?php include("layout-footer.php") ?>
```

Report-criminal.php

```
<?php include("layout-top.php") ?>
<?php include("report/criminal.php") ?>
<?php include("layout-footer.php") ?>
```

Criminal.php

```
<!-- Begin Page Content -->
<div class="container-fluid">
<!-- DataTales Example -->
<div class="card shadow mb-4">
<div class="card-header py-3">
<h6 class="m-0 font-weight-bold text-primary">Criminal Information</h6>
</div>
<div class="card-body">
```

```
<div class="table-responsive">
<table class="table table-bordered" id="dataTable" width="100%" cellspacing="0">
<thead>
<tr>
<th></th>
<th>Information</th>
<th>Identity</th>
<th>Date Of Birth</th>
<th></th>
</tr>
</thead>
<tfoot>
<tr>
<th></th>
<th>Information</th>
<th>Identity</th>
<th>Date Of Birth</th>
<th></th>
</tr>
</tfoot>
<tbody>
<?php
                $result = mysqli_query($db, "SELECT * FROM `criminal` ORDER BY `criminal`.`id` DESC");                while ($row = mysqli_fetch_array($result))
{                    echo "<tr>
<td><img                                                src='".$row['image']."'class='"."rounded-circle"."'width='"."50"."'height='"."50"."'></td><td>".$row['fName']." ".$row['lName']."<br>
                        Father's Name: " .$row['fathersName']."<br>
                        Mothers's Name: " .$row['mothersName']."<br>
                        Mark Symbol: " .$row['symbol']."<br>
<a href='read-criminal.php?id=". $row['id'] ."' title='View Record' data-toggle='tooltip'><span class='fa fa-eye'></span></a>
</td>
<td> NID: ".$row['poneNumber']."<br>
                        Contact No:  ".$row['contactno']."
</td>
<td>".$row['dateOFbirth']."
</td>
<td>
<a href='read-criminal.php?id=". $row['id'] ."' title='View Record' data-toggle='tooltip'><span class='fa faeye'></span></a>"

?>
<?php
    if($_SESSION['userRoll'] != "court"){
    ?>
<?php        };
```

```
    ?
<?php echo"
</td>
</tr> ";
                    }
                   ?>
</tbody>
</table>
</div>
</div>
</div>
</div>
<!-- /.container-fluid -->
```

Report-crime.php

```
<?php include("layout-top.php") ?>
<?php include("report/crime.php") ?>
<?php include("layout-footer.php") ?>
```

Crime.php

```
<!-- Begin Page Content -->
<div class="container-fluid">
<!-- DataTales Example -->
<div class="card shadow mb-4">
<div class="card-header py-3">
<h6 class="m-0 font-weight-bold text-primary">Crime Information</h6>
</div>
<div class="card-body">
<div class="table-responsive">
<table class="table table-bordered" id="dataTable" width="100%" cellspacing="0">
<thead>
<tr>
<th>Case No</th>
<th>Image</th>
<th>Criminal</th>
<th>Type</th>
<th>prison</th>
<th>Crime location</th>
<th>Court</th>
<th>Duty Police</th><th>Punishment</th>
<th>Date</th>
<th></th>
</tr>
</thead>
```

```
<tfoot>
<tr>
<th>Case No</th>
<th>Image</th>
<th>Criminal</th>
<th>Type</th>
<th>Prision</th>
<th>Crime location</th><th>Court</th>
<th>Duty Police</th><th>Punishment</th>
<th>Date</th>
<th></th>
</tr>
</tfoot>
<tbody>
<?php
                $result = mysqli_query($db, "SELECT * FROM `crime` ORDER BY `crime`.`id` DESC");                while ($row = mysqli_fetch_array($result))
{                    $data = $row['criminal_ID'];
                $criminal = mysqli_fetch_array(mysqli_query($db, "SELECT * FROM `criminal`  where id = $data"));                $data = $row['police_Id'];
                $police = mysqli_fetch_array(mysqli_query($db, "SELECT * FROM `police` where id = $data"));                echo "<tr>
<td>".$row['caseno']."</td>
<td><img                                                src='".$row['image']."'class='"."rounded-circle"."'width='"."50"."'height='"."50"."'></td><td>".$criminal['fName']."
".$criminal['lName']."</td>
<td>".$row['crimeType']."</td>
<td>".$row['prision']."</td>
<td>".$row['place']."</td>
<td>".$row['court']."</td>
<td>".$police['fName']." ".$police['lName']."</td>
<td>".$row['punishment']."</td>
<td>".$row['date']."</td>
<td>
<a href='read-crime.php?id=". $row['id'] ."' title='View Record' data-toggle='tooltip'><span class='fa faeye'></span></a>
                                                <a href='update-crime.php?id=". $row['id'] ."' title='View Record' data-toggle='tooltip'><span class='fa fa-pen'></span></a>
</td>
</tr> ";
                }
                ?>
</tbody>
</table>
</div>
</div>
```

```
</div>
</div>
<!-- /.container-fluid -->
```

Report-police.php

```
<?php include("layout-top.php") ?>
<?php include("report/police.php") ?>
<?php include("layout-footer.php") ?>
```

Police.php

```
<!-- Begin Page Content -->
<div class="container-fluid">
<!-- DataTales Example -->
<div class="card shadow mb-4">
<div class="card-header py-3">
<h6 class="m-0 font-weight-bold text-primary">Police Information</h6>
</div>
<div class="card-body">
<div class="table-responsive">
<table class="table table-bordered" id="dataTable" width="100%" cellspacing="0">
<thead>
<tr>
<th></th>
<th>Name</th>
<th>Height</th>
<th>Weight</th>
<th>Eye Clore</th><th>NID</th>
<th>Date Of Birth</th>
<th></th>
</tr>
</thead>
<tfoot>
<tr>
<th></th>
<th>Name</th>
<th>Height</th>
<th>Weight</th>
<th>Eye Clore</th>
<th>NID</th>
<th>Date Of Birth</th>
<th></th>
</tr>
</tfoot>
<tbody>
```

```
<?php
                $result = mysqli_query($db, "SELECT * FROM `police` ORDER BY `police`.`id` DESC");                while ($row = mysqli_fetch_array($result))
{                    echo "<tr>
<td><img                                                src='".$row['image']."'class='"."rounded-circle"."'width='"."50"."'height='"."50"."'></td><td>".$row['fName']." ".$row['lName']."</td>
<td>".$row['height']."</td>
<td>".$row['weight']."</td>
<td>".$row['eayColor']."</td>
<td>".$row['poneNumber']."</td>
<td>".$row['dateOFbirth']."</td>
<td>
<a href='read-police.php?id=". $row['id'] ."' title='View Record' data-toggle='tooltip'><span class='fa faeye'></span></a>
<a href='update-police.php?id=". $row['id'] ."' title='Update Record' data-toggle='tooltip'><span class='fa fa-pen'></span></a>
</td>
</tr> ";
                }
                ?>
</tbody>
</table>
</div>
</div>
</div>
</div>
<!-- /.container-fluid -->
```

Page-court.php

```
<?php include("layout-top.php") ?>
<?php include("court.php") ?>
<?php include("layout-footer.php") ?>
```

Court.php

```
<!-- Begin Page Content -->
<div class="container-fluid d-flex justify-content-between"><div class="body-area w-100 pr-5">
<h1 class="text-center">Add Crime Punishment</h1>
<hr>
<form method="POST"  enctype="multipart/form-data">
<div class="form-group">
<label for="exampleFormControlSelect1">Case No</label>
<select class="form-control" id="exampleFormControlSelect1" name="ids">
<?php
```

```
                        $sql = mysqli_query($db, "SELECT id,caseno From crime");
                        $row = mysqli_num_rows($sql);
                        if($row > 0){
                           while ($row = mysqli_fetch_array($sql)){
                           echo "<option value='". $row['id'] ."'>" .$row['caseno'] ."</option>" ;
                           }
                        }else  echo "<option value=''> No Data found</option>";
                     ?>
</select>
</div>
<div class="form-group">
<label for="exampleFormControlInput2">Punishment</label>
<input type="text" class="form-control" id="exampleFormControlInput2" name="punishment">
</div>
<button type="submit" class="btn btn-primary" name="addcrime">Submit</button>
</form>
</div>
<div class="right-body">
<!-- Sidebar -->
<ul class="navbar-nav bg-gradient-info sidebar sidebar-dark ">

<!-- Sidebar - Brand -->
<a class="sidebar-brand d-flex align-items-center justify-content-center" href="index.html">
<div class="sidebar-brand-icon rotate-n-15">
<i class="fas fa-gavel"></i>
</div>
<div class="sidebar-brand-text mx-3">Quick Link</div>
</a>
<!-- Divider -->
<hr class="sidebar-divider my-0">

<!-- Nav Item - Dashboard -->
<li class="nav-item">
<a class="nav-link" href="">
<i class="fas fa-fw fa-tachometer-alt"></i>
<span>Link</span></a>
<a class="nav-link" href="">
<i class="fas fa-fw fa-tachometer-alt"></i>
<span>Link</span></a>
</li>
</ul>
<!-- End of Sidebar -->
</div>
</div>
<!-- /.container-fluid --><?php                    if(! $db ) {
```

```
                die('Could not connect: ' . mysql_error());
            }

        if (isset($_POST['addcrime'])) {

          $id = mysqli_real_escape_string($db, $_POST['ids']);
                $punish = mysqli_real_escape_string($db, $_POST['punishment']);
 $insert = $db->query("UPDATE crime SET     punishment = '$punish' WHERE id = $id");
header('location: home.php');
                echo "<script> alert('Data stored successfully'); </script>";                    }
else{
                $statusMsg = 'Please select ';
            }

             // Display status message
            // echo $statusMsg;
          ?>
```

Page-Crime.php

```
<?php include("layout-top.php") ?>
<?php include("content/criminal-content.php") ?>
<?php include("layout-footer.php") ?>
```

Content-crime.php

```
<!-- Begin Page Content -->
<div class="container-fluid d-flex justify-content-between">
<div class="body-area w-100 pr-5">
<h1 class="text-center">Add Crime</h1>
<hr>
<form method="POST"  enctype="multipart/form-data">
        <div class="form-group">
<label for="exampleFormControlInput2">Case No</label>
<input type="text" class="form-control" id="exampleFormControlInput2" name="caseNo">
</div>
<div class="form-group">
<label for="exampleFormControlSelect1">Select Duty Officer</label>
<select class="form-control" id="exampleFormControlSelect1" name="police">
<?php
                        $sql = mysqli_query($db, "SELECT id,fName,lName From police");
                        $row = mysqli_num_rows($sql);                        while ($row
= mysqli_fetch_array($sql)){
                        echo    "<option    value='".    $row['id']    ."'>"    .$row['fName']    ."
".$row['lName'] ."</option>" ;
                        }
```

```
                    ?>
</select>
</div>
<div class="form-group">
<label for="exampleFormControlSelect1">Select Criminal </label>
<select class="form-control" id="exampleFormControlSelect1" name="criminal">
<?php
                    $sql = mysqli_query($db, "SELECT id,fName,lName,poneNumber
From criminal");
                    $row = mysqli_num_rows($sql);                    while ($row
= mysqli_fetch_array($sql)){
                    echo "<option value='". $row['id'] .'">" .$row['fName'] ."
".$row['lName'] ." ".$row['poneNumber'] ."</option>" ;
                    }
                    ?>
</select>
</div>
<div class="form-group">
<label for="exampleFormControlSelect1">Select Crime Type</label>
<select class="form-control" id="exampleFormControlSelect1" name="crimetype">
<?php
                    $sql = mysqli_query($db, "SELECT name From crimetype");
                    $row = mysqli_num_rows($sql);                    while ($row
= mysqli_fetch_array($sql)){
                    echo "<option value='". $row['name'] .'">" .$row['name'] ."</option>" ;
                    }                    ?>
</select>
</div>
<div class="form-group">
<label for="exampleFormControlSelect1">Select Category</label>
<select class="form-control" id="exampleFormControlSelect1" name="crimecat">
<?php
                    $sql = mysqli_query($db, "SELECT name From crimecategory");
                    $row = mysqli_num_rows($sql);                    while ($row
= mysqli_fetch_array($sql)){                    echo "<option value='".
$row['name'] .'">" .$row['name'] ."</option>" ;
                    }                    ?></select>
</div>
<div class="form-group">
<label for="exampleFormControlSelect1">Select Prision</label>
<select class="form-control" id="exampleFormControlSelect1" name="prision">
<?php
                    $sql = mysqli_query($db, "SELECT name From prision");
                    $row = mysqli_num_rows($sql);                    while ($row
= mysqli_fetch_array($sql)){
                    echo "<option value='". $row['name'] .'">" .$row['name'] ."</option>" ;
                    }
```

```
                        ?>
</select>
</div>
<div class="form-group">
<label for="exampleFormControlSelect1">Select Court</label>
<select class="form-control" id="exampleFormControlSelect1" name="court">
<?php
                            $sql = mysqli_query($db, "SELECT name From court");
                            $row = mysqli_num_rows($sql);                                   while ($row
= mysqli_fetch_array($sql)){
                            echo "<option value='". $row['name'] ."'>" .$row['name'] ."</option>" ;
                            }
                        ?>
</select>
</div>
<div class="form-group">
<label     for="exampleFormControlInput1">Date</label><input     type="text"     class="form-
control" id="datepicker"                                    placeholder="yyyy/mm/dd" name="date"
required>
</div>
<div class="form-group">
<label for="exampleFormControlInput2">Place</label>
<input type="text" class="form-control" id="exampleFormControlInput2" name="place">
</div>

<div class="form-group">
<label for="exampleFormControlTextarea1">Description</label>
<textarea          class="form-control"          id="exampleFormControlTextarea1"          rows="3"
name="description"></textarea>
</div>
<div class="form-group">
<label for="exampleFormControlInput2">Image</label><br>
<input type="file" name="image">
</div>
<button type="submit" class="btn btn-primary" name="addcrime">Submit</button>
</form>
</div>
<div class="right-body">
<!-- Sidebar -->
<ul class="navbar-nav bg-gradient-info sidebar sidebar-dark ">

<!-- Sidebar - Brand -->
<a class="sidebar-brand d-flex align-items-center justify-content-center" href="index.html">
<div class="sidebar-brand-icon rotate-n-15">
<i class="fas fa-gavel"></i>
</div>
<div class="sidebar-brand-text mx-3">Quick Link</div>
```

```
</a>
<!-- Divider -->
<hr class="sidebar-divider my-0">

<!-- Nav Item - Dashboard --><li class="nav-item">
<a class="nav-link" href="">
<i class="fas fa-fw fa-tachometer-alt"></i>
<span>Link</span></a>
<a class="nav-link" href="">
<i class="fas fa-fw fa-tachometer-alt"></i>
<span>Link</span></a>
</li>
</ul>
<!-- End of Sidebar -->
</div>
</div>
<!-- /.container-fluid --><?php                                    if(! $db ) {
                    die('Could not connect: ' . mysql_error());
                }

        if (isset($_POST['addcrime'])) {

                    // File upload path
                    $targetDir = "uploads/crime/";
                    $fileName = basename($_FILES["image"]["name"]);
                    $targetFilePath = $targetDir . $fileName;
                    $fileType = pathinfo($targetFilePath,PATHINFO_EXTENSION);

                    $allowTypes = array('jpg','png','jpeg','gif','pdf');

                    $police = mysqli_real_escape_string($db, $_POST['police']);
                    $criminal = mysqli_real_escape_string($db, $_POST['criminal']);
                    $crimetype = mysqli_real_escape_string($db, $_POST['crimetype']);
                    $crimecat = mysqli_real_escape_string($db, $_POST['crimecat']);
                    $prision = mysqli_real_escape_string($db, $_POST['prision']);
                    $court = mysqli_real_escape_string($db, $_POST['court']);
                    $date = mysqli_real_escape_string($db, $_POST['date']);
                    $place = mysqli_real_escape_string($db, $_POST['place']);
                    $caseNo = mysqli_real_escape_string($db, $_POST['caseNo']);
                    $description = mysqli_real_escape_string($db, $_POST['description']);

                      // Allow certain file formats
                      $allowTypes                    =                    array('jpg','png','jpeg','gif','pdf');
if(in_array($fileType, $allowTypes)){
                        // Upload file to server
                        if(move_uploaded_file($_FILES["image"]["tmp_name"],
$targetFilePath)){
```

```
                    // Insert image file name into database                    $insert =
$db->query("INSERT INTO
crime(police_Id,criminal_ID,crimeType,crimeCategory,prision,court,date,place,image,descripti
on,uploads_on,caseno)

VALUES('$police','$criminal','$crimetype','$crimecat','$prision','$court','$date','$place','$target
FilePath','$description',NOW(),'$c aseNo')");

                        if($insert){
                            echo "<script> alert('Data stored successfully');
</script>";                         }else{
                            $statusMsg = "File upload failed, please try again.";
                        }
                    }else{
                        $statusMsg = "Sorry, there was an error uploading your file.";
                    }
                }else{
                    $statusMsg = 'Sorry, only JPG, JPEG, PNG, GIF, & PDF files are allowed
to upload.';
                }
            } else{
                $statusMsg = 'Please select a file to upload.';
            }
            // Display status message
            // echo $statusMsg;
        ?>
```

Page-criminal.php

```
<?php include("layout-top.php") ?>
<?php include("content/criminal-content.php") ?>
<?php include("layout-footer.php") ?>
```

Content-criminal.php

```
<!-- Begin Page Content -->
<div class="container-fluid d-flex justify-content-between">
<div class="body-area">
<h1 class="text-center">Add Criminal</h1>
<hr>
<div class="row">
<form method="POST"  enctype="multipart/form-data">
<div class="col-sm-12">
<div class="row">
<div class="col-sm-6 form-group">
<label>First Name</label>
```

```
<input type="text" placeholder="Enter First Name Here.." class="form-control" name="fName" required></div>
<div class="col-sm-6 form-group">
<label>Last Name</label>
<input type="text" placeholder="Enter Last Name Here.." class="form-control" name="lName" required></div>
</div>
<div class="row">
<div class="col-sm-6 form-group">
<label>Father's Name</label>
<input type="text" placeholder="Enter Father's Name Here.." class="form-control" name="fathersName" required>
</div>
<div class="col-sm-6 form-group">
<label>Mother's Name</label>
<input type="text" placeholder="Enter Mother's Name Here.." class="form-control" name="mothersName" required>
</div>
</div>
<div class="row">
<div class="col-sm-6 form-group">
<label>Contact No</label>
<input type="text" placeholder="Enter Here.." class="form-control" name="contactno" >
</div>
<div class="col-sm-6 form-group">
<label>Mark Symbol</label>
<input type="text" placeholder="Enter Here.." class="form-control" name="symbol" >
</div>
</div>
<!-- <div class="row">
<div class="col-sm-4 form-group">
<label>Height</label>
<input type="text" placeholder="Enter Height Here.." class="form-control" name="height" >
</div>
<div class="col-sm-4 form-group">
<label>Weight</label>
<input type="text" placeholder="Enter Weight Here.." class="form-control" name="weight" >
</div>
<div class="col-sm-4 form-group">
<label>Eye Color</label>
<input type="text" placeholder="Enter Eye Color Here.." class="form-control" name="eColor" ></div>
</div> -->
<div class="form-group">
<label>Address</label>
```

```
<textarea placeholder="Enter Address Here.." rows="3" class="form-control" name="address"></textarea required>
</div>
<div class="row">
<div class="col-sm-4 form-group">
<label>City</label>
<input type="text" placeholder="Enter City Name Here.." class="form-control" name="city">
</div>
<div class="col-sm-4 form-group">
<label>State</label>
<input type="text" placeholder="Enter State Name Here.." class="form-control" name="state">
</div>
<div class="col-sm-4 form-group">
<label>Zip</label>
<input type="text" placeholder="Enter Zip Code Here.." class="form-control" name="zip">
</div>
</div>
<div class="row">
<div class="form-group col-sm-6 ">
<label>NID</label>
<input type="text" placeholder="Enter NID Here.." class="form-control" name="pNumber" >
</div>
<div class="form-group col-sm-6 ">
<label>Date</label>
<input type="text" placeholder="dd/mm/yyyy" id="datepicker" class="form-control" name="date" required>
</div>
</div>
<div class="form-group">
<label>Email Address</label>
<input type="text" placeholder="Enter Email Address Here.." class="form-control" name="email">
</div>
<div class="form-group">
<label for="exampleFormControlInput2">Image</label><br>
<input type="file" name="image">
</div>
<button type="submit" class="btn btn-lg btn-info mb-5" name="addcriminal">Submit</button>
</div>
</form>
</div>
</div>
<div class="right-body">
```

```
<!-- Sidebar -->
<ul class="navbar-nav bg-gradient-info sidebar sidebar-dark ">

<!-- Sidebar - Brand -->
<a class="sidebar-brand d-flex align-items-center justify-content-center" href="index.html">
<div class="sidebar-brand-icon rotate-n-15">
<i class="fas fa-gavel"></i>
</div>
<div class="sidebar-brand-text mx-3">Quick Link</div>
</a>

<!-- Divider -->
<hr class="sidebar-divider my-0">

<!-- Nav Item - Dashboard -->
<li class="nav-item">
<a class="nav-link" href="">
<i class="fas fa-fw fa-tachometer-alt"></i>
<span>Link</span></a>
<a class="nav-link" href="">
<i class="fas fa-fw fa-tachometer-alt"></i>
<span>Link</span></a>
</li>
</ul>
<!-- End of Sidebar -->
</div>
</div>
<!-- /.container-fluid --><?php                                    if(! $db ) {
                    die('Could not connect: ' . mysql_error());
                }

        if (isset($_POST['addcriminal'])) {


                    // File upload path
                    $targetDir = "uploads/criminal/";
                    $fileName = basename($_FILES["image"]["name"]);
                    $targetFilePath = $targetDir . $fileName;
                    $fileType = pathinfo($targetFilePath,PATHINFO_EXTENSION);

                    $allowTypes = array('jpg','png','jpeg','gif','pdf');


                    $fname = ucfirst(mysqli_real_escape_string($db, $_POST['fName']));
                    $lname = ucfirst(mysqli_real_escape_string($db, $_POST['lName']));
                    $height = mysqli_real_escape_string($db, $_POST['height']);
                    $weight = mysqli_real_escape_string($db, $_POST['weight']);
```

```
$ecolor = ucfirst(mysqli_real_escape_string($db, $_POST['eColor']));
$address = ucfirst(mysqli_real_escape_string($db, $_POST['address']));
$city = ucfirst(mysqli_real_escape_string($db, $_POST['city']));
$state = ucfirst(mysqli_real_escape_string($db, $_POST['state']));
$zip = mysqli_real_escape_string($db, $_POST['zip']);
$phone = mysqli_real_escape_string($db, $_POST['pNumber']);
$date = mysqli_real_escape_string($db, $_POST['date']);
$email = mysqli_real_escape_string($db, $_POST['email']);
$fathersName = mysqli_real_escape_string($db, $_POST['fathersName']);
$mothersName = mysqli_real_escape_string($db, $_POST['mothersName']);
$contactno = mysqli_real_escape_string($db, $_POST['contactno']);
$symbol = mysqli_real_escape_string($db, $_POST['symbol']);

    // Allow certain file formats
    $allowTypes = array('jpg','png','jpeg','gif','pdf');
if(in_array($fileType, $allowTypes)){
    // Upload file to server
    if(move_uploaded_file($_FILES["image"]["tmp_name"],
$targetFilePath)){
        // Insert image file name into database $insert
= $db->query("INSERT INTO
criminal(fName,lName,height,weight,eayColor,address,city,state,zipCode,poneNumber,dateOF
birth,email,image,uploads_on,fath ersName,mothersName,contactno,symbol)

VALUES('$fname','$lname','$height','$weight','$ecolor','$address','$city','$state','$zip','$phone','
$date','$email','$targetFilePath',N
OW(),'$fathersName','$mothersName','$contactno','$symbol' )");

        if($insert){ echo "<script> alert('Data stored
successfully'); </script>"; }else{
            $statusMsg = "File upload failed, please try again.";
        }
    }else{
        $statusMsg = "Sorry, there was an error uploading your file.";
    }
```

```
INSERT INTO `crimetype` (`id`, `name`, `description`) VALUES
(7, ' murder', 'Dil'),
(8, 'Aggravated ', 'Xumeeyay  '),
(9, 'Assault', 'Takooray '),
(10, ' Robbery', 'Dhac'),
(11, 'Burglary', 'Jabsi'),
(12, 'Theft', 'Xatooyo'),
(13, 'Arson', 'Gubid'),
(14, 'Sexual orientation', 'Kufsi'),
(15, 'Gender identity', 'Qaniisnimo'),
(16, 'Religion', 'Diin');

-- --------------------------------------------------------

--
-- Table structure for table `criminal`
--
CREATE TABLE `criminal` (
  `id` int(11) NOT NULL,
  `fName` varchar(250) NOT NULL,
  `lName` varchar(250) NOT NULL,
  `height` varchar(50) DEFAULT NULL,
  `weight` varchar(50) DEFAULT NULL,
  `eayColor` varchar(100) DEFAULT NULL,
  `address` varchar(250) DEFAULT NULL,
  `city` varchar(250) DEFAULT NULL,
  `state` varchar(250) DEFAULT NULL,
  `zipCode` varchar(200) DEFAULT NULL,
  `poneNumber` varchar(50) DEFAULT NULL,
  `dateOFbirth` date DEFAULT NULL,
  `email` varchar(200) DEFAULT NULL,
  `website` varchar(200) DEFAULT NULL,
  `image` varchar(250) DEFAULT NULL,
  `uploads_on` datetime NOT NULL,
  `fathersName` varchar(250) NOT NULL,
  `mothersName` varchar(250) NOT NULL,
  `contactno` varchar(20) NOT NULL,
  `symbol` varchar(250) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `criminal`
--
```

```
INSERT INTO `criminal` (`id`, `fName`, `lName`, `height`, `weight`, `eayColor`, `address`, `city`, `state`, `zipCode`,
`poneNumber`, `dateOFbirth`, `email`, `website`, `image`, `uploads_on`, `fathersName`, `mothersName`, `contactno`, `symbol`)
VALUES
(26, 'Yahye ', 'Hassan ', '6.6\"', '99', 'Black', 'Mogadishu, buul hube', 'Mogadisho', 'Buulhube', '73827', '099672617', '2014-05-05',
'biike@gmail.com', NULL, 'uploads/criminal/0_epo3DUJGKyB7CXZw.jpeg', '2019-03-25 20:39:34', 'jamac ahmed ', 'Nuurto', '2342563', 'laceration on face'),
(27, 'Abdullahi', 'Noor', '', '', '', 'Shabelle, hose, afgoye', 'Shabelle hoose', 'Afgoye', '4200', '099273616', '1994-05-05',
'noor@gmail.com', NULL, 'uploads/criminal/20110607_farah-mohamed-beledi_33.jpg', '2019-03-27 16:52:20', 'Jim\'ale', 'Aasho', '1234567', 'No'),
(28, 'Biike', 'Yallahow', '', '', '', 'Mogadishu, buul hube', 'Mogadisho', 'Buulhube', '73827', '099271632', '1992-02-20',
'biike@gmail.com', NULL, 'uploads/criminal/abdirizak-mohamed-warsame.jpg', '2019-03-27 16:53:29', 'Hussien', 'Nuurto', '2342563', 'laceration on chine'),
(29, 'Aamir', 'Deylaaf', '6.6\"', '', '', 'Dhuusomareeb, galmudug', 'Dhuusomareeb', 'Galmudug', '3425', '099768546', '1980-07-21',
'aamir@hotmail.com', NULL, 'uploads/criminal/abdirizak-mohamed-warsame-ip.gif', '2019-03-27 16:55:07', 'ibarahim', 'haajiro', '24535245', 'No'),
(30, 'Osma Nuur', 'Mohamed', '6.6\"', '', '', 'Cadaado, galmudug', 'Cadaado', 'Galmudug', '3425', '099637261', '1989-02-18',
'aamir@hotmail.com', NULL, 'uploads/criminal/abdullahi-yusuf_1479144043441_2275730_ver1.0_640_360.jpg', '2019-03-27 16:57:51', 'ilmi', 'meymun ', '09675473', 'staples on head'),
(32, 'Nuur osma', 'Mohamed', '', '', '', 'Dhuusomareeb, galmudug', 'Dhuusomareeb', 'Galmudug', '3425', '099675436', '1996-05-05', 'aamir@hotmail.com', NULL, 'uploads/criminal/articleInline.jpg', '2019-03-27 17:01:00', 'Muhadiin', 'Nadiifo', '0997384734', ''), (33, 'Abdullahi', 'Haji', '', '', '', 'Mogadishu, hamar bile', 'Mogadisho', 'Hamar bile', '2342', '', '1992-02-12', 'noor@gmail.com',
NULL, 'uploads/criminal/guled-ali-omar.jpg', '2019-03-27 17:01:35', 'Muhidin', 'Kadijo', '2342563', 'No'),
(34, 'Yahye mohamed', 'Daadir', '', '', '', 'Mogadishu, hamar bile', 'Mogadisho', 'Hamar bile', '2342', '099737287', '1990-02-18',
'noor@gmail.com', NULL, 'uploads/criminal/image5174347x.jpg', '2019-03-27 17:09:43', 'Muhadiin', 'Kadijoo', '89283920',
'No'),
```

```
(35, 'Abdullahi', 'Mursal ', '', '', '', 'Mogadishu, hamar bile', 'Mogadisho',
'Hamar bile', '2342', '099718271', '1985-02-18',
'noor@gmail.com', NULL, 'uploads/criminal/images.jpg', '2019-03-27
17:11:02', 'Hussien', 'Qaali', '2342563', 'staples on head'),
(36, 'Rasher', 'Mohamed', '', '', '', 'Hamar,bile, house 27, road 19', 'Mugdishu ',
'Banadir ', '4200', '099893827', '1994-12-21',
'fowzoo18@gmail.com', NULL, 'uploads/criminal/mahamed-said1.jpg',
'2019-03-27 17:12:32', 'Muhadiin', 'Muumino', '6372634',
'laceration on face'),
(37, 'Daadir', 'Hassan', '', '', '', 'Dhuusomareeb, galmudug', 'Dhuusomareeb',
'Galmudug', '3425', '09983728999', '1980-03-25',
'aamir@hotmail.com', NULL, 'uploads/criminal/SOMALIA-articleInline-
v2.jpg', '2019-03-27 17:13:23', 'ibarahim', 'zahra', '24535234', 'no');

-- --------------------------------------------------------

--
-- Table structure for table `images`
--
CREATE TABLE `images` (
  `id` int(11) NOT NULL,
  `image` varchar(255) COLLATE utf8_unicode_ci NOT NULL,
  `uploaded_on` datetime NOT NULL,
  `status` enum('1','0') COLLATE utf8_unicode_ci NOT NULL DEFAULT
'1'
) ENGINE=InnoDB DEFAULT CHARSET=utf8
COLLATE=utf8_unicode_ci;

-- --------------------------------------------------------

--
-- Table structure for table `police`
--
CREATE TABLE `police` (
  `id` int(11) NOT NULL,
  `fName` varchar(250) DEFAULT NULL,
  `lName` varchar(250) DEFAULT NULL,
  `height` varchar(50) DEFAULT NULL,
  `weight` varchar(50) DEFAULT NULL,
  `eayColor` varchar(100) DEFAULT NULL,
  `address` varchar(250) DEFAULT NULL,
  `city` varchar(250) DEFAULT NULL,
  `state` varchar(250) DEFAULT NULL,
```

```
  `zipCode` varchar(200) DEFAULT NULL,
  `poneNumber` varchar(50) DEFAULT NULL,
  `dateOFbirth` date DEFAULT NULL,
  `email` varchar(200) DEFAULT NULL,
  `website` varchar(200) DEFAULT NULL,
  `image` varchar(250) DEFAULT NULL,
  `uploads_on` datetime NOT NULL,
  `jobid` varchar(200) NOT NULL,
  `polisestation` varchar(250) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `police`
--

INSERT INTO `police` (`id`, `fName`, `lName`, `height`, `weight`,
`eayColor`, `address`, `city`, `state`, `zipCode`,
`poneNumber`, `dateOFbirth`, `email`, `website`, `image`, `uploads_on`,
`jobid`, `polisestation`) VALUES
(14, 'Yasin Jamal ', 'Mohamed', '7.6\"', '64', 'Black', 'Mogadishu, hamar bile',
'Mogadisho', 'Hamar bile', '2342', '099356256', '1990-03-05',
'yassin@gmail.com', '', 'uploads/police/igp-orders-probe-into-ankaful-
shooting.jpg', '2019-03-27 16:13:52', '7774325', 'Hamar jabjab police-
station'),
(15, 'Dadir ahmed', 'Nuur', '5.6\"', '70', 'Black', 'Mogadishu, buul hube',
'Mogadisho', 'Buulhube', '73827', '099783473', '1980-03-
11', 'biike@gmail.com', '', 'uploads/police/images (1).jpg', '2019-03-27
16:15:43', '7774343', 'Yakshid Police-Station'),
(16, 'Nuur Kalid', 'Hassan ', '5.6\"', '70', 'Grey', 'Dhuusomareeb, galmudug',
'Dhuusomareeb', 'Galmudug', '3425', '099347623',
'1992-02-20', 'aamir@hotmail.com', '',
'uploads/police/BXPCSDK4ZVFS7NWPTR7ETKJGRU.jpg', '2019-03-27
16:17:18', '7774473', 'Abdi-aziz Police-Station '),
(17, 'Osma Nuur ', 'Mohamed', '7.6\"', '64', 'Grey', 'Dhuusomareeb,
galmudug', 'Dhuusomareeb', 'Galmudug', '3425', '0997384723',
'1994-02-12', 'aamir@hotmail.com', '',
'uploads/police/DNCQ4RAAVKBOBO5EBJXRBIPBZU.jpg', '2019-03-27
16:19:16', '7774335', 'Wadajir Police-Station'),
(18, 'ZamZam Hassan ', 'Hussien', '7.6\"', '64', '', 'Mogadishu, buul hube',
'Mogadisho', 'Buulhube', '73827', '099367216', '1960-03-
20', 'biike@gmail.com', '', 'uploads/police/download.jpg', '2019-03-27
16:25:52', '7774326', 'Waaber Police-station'),
```

```
(22, 'Nuur osma', 'Mohamed', '7.6\"', '70', 'Grey', 'Dhuusomareeb, galmudug',
'Dhuusomareeb', 'Galmudug', '3425', '0997384734',
'1999-03-12', 'aamir@hotmail.com', '', 'uploads/police/fake-cop.jpg', '2019-
03-27 16:37:41', '7774323', 'Hodan Police-Station'),
(23, 'Osma Noor', 'Mohamed', '5.6\"', '70', 'Grey', 'Dhuusomareeb, galmudug',
'Dhuusomareeb', 'Galmudug', '3425', '099782714',
'1992-02-12', 'aamir@hotmail.com', '', 'uploads/police/images.jpg', '2019-03-
27 16:39:02', '7774336', 'Hamar weyne PoliceStation ');

-- --------------------------------------------------------

--
-- Table structure for table `prision`
--
CREATE TABLE `prision` (
  `id` int(11) NOT NULL,
  `name` varchar(250) NOT NULL,
  `description` text NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `prision`
--

INSERT INTO `prision` (`id`, `name`, `description`) VALUES
(12, 'Juvenile', 'Tan caruurta'),
(13, 'Military ', 'Xabsiga ciidanka'),
(14, 'State prison', 'Xabsiga gobolka'),
(15, 'District Jail', 'Xabsiga degmada '),
(16, 'Hamar weyne pirson', ''),
(17, 'Hodan prison ', ''),
(18, 'Wadajir prison ', ''),
(19, 'Abdi-aziz prison ', ''),
(20, 'Warta nabada prison', ''),
(21, 'Afgoye prison', ''),
(22, 'Waaberi prison', ''),
(23, 'Hamar jab jab prison ', ''),
(24, 'Dayniile prison', ''),
(25, 'Hamar bile prison', ''),
(26, 'Boosaaso prison ', ''),
(27, 'Garowe prison', ''),
(28, 'Cadaado prison', ''),
(29, 'Dhuusamareb prison', ''),
```

```
(30, 'Yaaqshid prison', ''),
(31, 'Baladweyn prison', ''),
(32, 'Beydhaba prison', ''),
(33, 'Marka prison', ''),
(34, 'Shalanbood prison', ''), (35, 'Deynuunay prison', ''),
(36, 'Kismayo prison', ''),
(37, 'Baraawe prison', '');

-- --------------------------------------------------------

--
-- Table structure for table `roletype`
--
CREATE TABLE `roletype` (  `id` int(11) NOT NULL,  `name` varchar(250) NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `roletype`
--
INSERT INTO `roletype` (`id`, `name`) VALUES
(1, 'admin'),
(2, 'police'),
(4, 'court');

-- --------------------------------------------------------

--
-- Table structure for table `users`
--
CREATE TABLE `users` (
  `id` int(11) NOT NULL,
  `fName` varchar(250) DEFAULT NULL,
  `lName` varchar(250) DEFAULT NULL,
  `username` varchar(100) NOT NULL,
  `email` varchar(100) NOT NULL,
  `password` varchar(100) NOT NULL,
  `userRoll` varchar(250) DEFAULT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1;

--
-- Dumping data for table `users`
--
```

```
INSERT INTO `users` (`id`, `fName`, `lName`, `username`, `email`, `password`, `userRoll`) VALUES
(1, 'Rashedul', '', 'dev', 'shawon.my@gmail.com', '37d1703157da260a648d24613032bc8f', 'admin'),
(6, 'fowzi', 'jamal', 'admin', 'ozil2m@hotmail.com', '5730bb1ef815d9007df14d136e107614', 'admin'),
(20, 'Yassin', 'jamal', 'Subadmin', 'fowzoo18@gmail.com', '5730bb1ef815d9007df14d136e107614', 'subuser'),
(23, 'jamal ', 'barrow', 'Courtuser', 'fowzoo18@gmail.com', '5730bb1ef815d9007df14d136e107614', 'court'),
(24, 'Kaazi', 'hommie', 'POLICEUSER', 'kaazi@hotmail.com', '5730bb1ef815d9007df14d136e107614', 'police'), (28, 'jaabir', 'jamal', 'NORMAL-USER', 'kaazi@yahoo.com', '5730bb1ef815d9007df14d136e107614', 'user');

--
-- Indexes for dumped tables
--

--
-- Indexes for table `court`
--
ALTER TABLE `court`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `courttype`
--
ALTER TABLE `courttype`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `crime`
--
ALTER TABLE `crime`
  ADD PRIMARY KEY (`id`),
  ADD KEY `police_Id` (`police_Id`),
  ADD KEY `criminal_ID` (`criminal_ID`);

--
-- Indexes for table `crimecategory`
--
```

```
ALTER TABLE `crimecategory`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `crimetype`
--
ALTER TABLE `crimetype`
  ADD PRIMARY KEY (`id`);
--
-- Indexes for table `criminal`
--
ALTER TABLE `criminal`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `images`
--
ALTER TABLE `images`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `police` --
ALTER TABLE `police`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `prision`
--
ALTER TABLE `prision`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `roletype`
--
ALTER TABLE `roletype`
  ADD PRIMARY KEY (`id`);

--
-- Indexes for table `users`
--
ALTER TABLE `users`
  ADD PRIMARY KEY (`id`);
```

```
--
-- AUTO_INCREMENT for dumped tables
--

--
-- AUTO_INCREMENT for table `court`
--
ALTER TABLE `court`
  MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=43;

--
-- AUTO_INCREMENT for table `courttype`
--
ALTER TABLE `courttype`
  MODIFY `id` int(11) NOT NULL AUTO_INCREMENT;

--
-- AUTO_INCREMENT for table `crime`
--
ALTER TABLE `crime`
  MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=50;

--
-- AUTO_INCREMENT for table `crimecategory`
--
ALTER TABLE `crimecategory`
  MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=7;

--
-- AUTO_INCREMENT for table `crimetype`
--
ALTER TABLE `crimetype`
  MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=17;

--
-- AUTO_INCREMENT for table `criminal`
--
ALTER TABLE `criminal`
```

```
 MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=38;

--
-- AUTO_INCREMENT for table `images`
--
ALTER TABLE `images`
 MODIFY `id` int(11) NOT NULL AUTO_INCREMENT;

--
-- AUTO_INCREMENT for table `police`
--
ALTER TABLE `police`
 MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=24;

--
-- AUTO_INCREMENT for table `prision`
--
ALTER TABLE `prision`
 MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=38;

--
-- AUTO_INCREMENT for table `roletype`
--
ALTER TABLE `roletype`
 MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=5;

--
-- AUTO_INCREMENT for table `users`
--
ALTER TABLE `users`
 MODIFY `id` int(11) NOT NULL AUTO_INCREMENT,
AUTO_INCREMENT=29;

--
-- Constraints for dumped tables
--

--
-- Constraints for table `crime`
```

```
--
ALTER TABLE `crime`
 ADD CONSTRAINT `crime_ibfk_1` FOREIGN KEY (`police_Id`)
REFERENCES `police` (`id`) ON DELETE CASCADE, ADD
CONSTRAINT `crime_ibfk_2` FOREIGN KEY (`criminal_ID`)
REFERENCES `criminal` (`id`) ON DELETE
CASCADE;
COMMIT;

/*!40101 SET
CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET
CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS
*/; /*!40101 SET
COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;


-----------------------------------------------------------------
Antimalware source
Admin.php
<?php
include('adminlock.php');
include("config.php");
session_start();
if(isset($_POST['view']) || isset($_POST['view2'])){
$acct_name = trim($_POST['acct_name']);
$acct_num = trim($_POST['acct_num']);
if($acct_name == '' && $acct_num == ''){
$msg = "Please Insert Acount Name or Number";
}
else{
$sql="SELECT * FROM activities WHERE acct_name='$acct_name' or
acct_number='$acct_num' ORDER BY sn DESC LIMIT 1";
$result=mysql_query($sql);
$row=mysql_fetch_array($result);
$active=$row['active']; 46

$count=mysql_num_rows($result);
$_SESSION['acctt']=$row['acct_type'];
/* // If result matched $myusername and $mypassword, table row must be 1
row
if($count > 0){
session_register("myusername");
```

```
$_SESSION['login_user']=$myusername;
header ('Location: client.php');
}
else {
$msg="Your Login Name or Password is invalid";
} */
}
}
if(isset($_POST['view3']) || isset($_POST['view4']) ){
$acct_name2 = trim($_POST['acct_name2']);
$acct_num2 = trim($_POST['acct_num2']);
if($acct_name2 == '' && $acct_num2 == ''){
$msg = "Please Insert Acount Name or Number";
} 47

else{
$sql="SELECT * FROM activities WHERE acct_name='$acct_name2' or
acct_number='$acct_num2' ORDER BY sn DESC LIMIT 1";
$result=mysql_query($sql);
$row=mysql_fetch_array($result);
$active=$row['active'];
$_SESSION['acctt']=$row['acct_type'];
$count=mysql_num_rows($result);
}
}
if(isset($_POST['transact'])){
$acct_name = trim($_POST['acct_name']);
$acct_num = trim($_POST['acct_num']);
$acct_bal = trim($_POST['acct_bal']);
$amt_withdrawn = trim($_POST['amt_withdrawn']);
if($acct_name == '' || $acct_num == '' || $acct_bal == '' || $amt_withdrawn
== ''){
$msg = "Please complete the empty fields"; 48

}
else{
if($amt_withdrawn> $acct_bal){
$msg = "Transaction Cannot be Completed. Insufficient Account Balance!!";
}
else{
$x = 0;
$acct_type = $_SESSION['acctt'];
$client = $_SESSION['login_user'];
```

```
$today = date("m/d/y");
$new_balance = $acct_bal - $amt_withdrawn;
$sql="insert into activities values('$x', '$client', '$acct_num', '$acct_name',
'Withdrawal','$amt_withdrawn', '$new_balance', '$acct_type', '$today')";
$result=mysql_query($sql) or die(mysql_error());
/* $row=mysql_fetch_array($result);
$active=$row['active'];
$count=mysql_num_rows($result); */
header("location: account_debited.php"); 49

Clientlogin.php
<?php
include("config.php");
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST"){
// username and password sent from form
$myusername = trim(addslashes($_POST['username']));
$mypassword = trim(addslashes($_POST['password']));
if($myusername == '' || $mypassword == ''){
$error="Please Complete the Empty Field";
}
else{
$sql="SELECT * FROM members WHERE username='$myusername' and
password='$mypassword'";
$result=mysql_query($sql);
$row=mysql_fetch_array($result);
$active=$row['active']; 50

$count=mysql_num_rows($result);
// If result matched $myusername and $mypassword, table row must be 1
row
if($count > 0){
session_register("myusername");
$_SESSION['login_user']=$myusername;
header ('Location: client.php');
}
else {
$error="Your Login Name or Password is invalid";
}
}
}//end
?>
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
<head>
<meta name="Description" content="Information architecture, Web Design,
Web Standards." />
<meta name="Keywords" content="your, keywords" /> 51

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"
/>
<meta name="Distribution" content="Global" />
<meta name="Robots" content="index,follow" />
<link rel="stylesheet" href="images/HarvestField.css" type="text/css" />
<title>Network Activity Monitoring System - Login Page</title></head>
<body>
<!-- wrap starts here -->
<div id="wrap">
<!--header -->
<div id="header">
<h1 id="logo-text"><a href="client.php" title="">Network
Activity</a></h1>
<h2 id="slogan">Monitoring System</h2>
<!--header ends-->
</div>
<!-- navigation starts-->
<div id="nav"> 52

<div id="light-brown-line"></div>
<!-- navigation ends-->
</div>
<!-- content-wrap starts -->
<div id="content-wrap">
<div id="main">
<h1>Client Login Page </h1>
<form action="" method="post">
<table width="100%" border="0">
<tr>
<td colspan="2"><?php echo $error; ?></td>
</tr>
<tr>
<td width="18%"><strong>Username:</strong></td>
<td width="82%"><label>
<input type="text" name="username" id="username" />
```

```
</label></td>
</tr>
<tr>
<td width="18%"><strong>Password:</strong></td>
<td width="82%"><label>
<input type="password" name="password" id="password" />
</label></td> 53

</tr>
<tr>
<td width="18%">&amp;nbsp;</td>
<td width="82%"><label>
<input type="submit" name="login" id="login" value="Login" />
</label></td>
</tr>
</table>
<p><br />
</p>
</form>
<br />
<!-- main ends -->
</div>
<!-- content-wrap ends-->
</div>
<!-- column starts -->
<div id="column-wrap">
<!-- column-wrap ends-->
</div> 54

<!-- footer starts -->
<div id="footer">
<p>
&copy; 2013 <a href="client.php" title="">Network Activity Monitoring
System</a>
<!-- footer ends -->
</p>
</div>
<!-- wrap ends here -->
</div>
</body>
</html>
Openaccount.php
<?php
```

```
include('clientlock.php');
include("config.php");
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST"){
// username and password sent from form 55

$acct_type = trim(addslashes($_POST['acct_type']));
$acct_name = trim(addslashes($_POST['acct_name']));
$acct_number = trim(addslashes($_POST['acct_number']));
$transaction = trim(addslashes($_POST['transaction']));
$acct_bal = trim(addslashes($_POST['acct_bal']));
if($acct_type == '' || $acct_name == '' || $acct_number == '' || $transaction ==
'' || $acct_bal == '' ){
$error="Please Complete the Empty Field";
}
else{
$x = 0;
$client = $_SESSION['login_user'];
$today = date("m/d/y");
$sql="insert into activities values('$x', '$client', '$acct_number',
'$acct_name', '$transaction', '$acct_bal', '$acct_type', '$today')";
$result=mysql_query($sql);
/* $row=mysql_fetch_array($result);
$active=$row['active']; 56

$count=mysql_num_rows($result); */
header("location: thanks.php");
}
}//end
?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
Regadmin.php
<?php
include("config.php");
session_start();
if($_SERVER["REQUEST_METHOD"] == "POST"){
// username and password sent from form
$username = trim(addslashes($_POST['username']));
$password = trim(addslashes($_POST['password'])); 57

$cpassword = trim(addslashes($_POST['cpassword']));
```

```
$fullname = trim(addslashes($_POST['fullname']));
$age = trim(addslashes($_POST['age']));
$gender = trim(addslashes($_POST['gender']));
$address = trim(addslashes($_POST['address']));
$email = trim(addslashes($_POST['email']));
$phone = trim(addslashes($_POST['phone']));
if($username == '' || $password == '' || $cpassword == '' || $fullname == '' ||
$age == '' || $gender == '' || $address == '' || $email == '' || $phone == ''){
$error="Please Complete the Empty Field";
}
else{
if( $password != $cpassword){
$error="Passwords does not match";
}
else{
$x = 0;
$sql="insert into admin values('$x', '$username', '$cpassword', '$fullname',
'$age', '$gender', '$address', '$email', '$phone')";
$result=mysql_query($sql); 58

/* $row=mysql_fetch_array($result);
$active=$row['active'];
$count=mysql_num_rows($result); */
header("location: thanks.php");
}
}
}//end
```

Appendix B

Questionnaire on Cybercrime Monitoring System

I am BELLO Latifat Olubsayo, a post graduate(MSc) student of Lead City University, Ibadan Oyo State, Nigeria.

The purpose of this study is to conduct a techchnology acceptance on Cybercrime Monitoring System for Forensic Expert (CMS).

CMS is a resent development for both individual and organization to monitor their website optimally. The Cybercrime Monitoring System is meant for research purpose only. The identity of the participant remain safe.

Data from response shall be used only for research purpose and kept confidential.

Your prompt response will be appreciated.

Questions	**Stongly Disagree**	**Disagree**	**Agree**	**Strongly Agree**
I think that I will like to use this Cybercrime Monitoring System?				
I find this cyber monitoring system				

unneccessarily complex?	
I find the record retrieval process convinent to use?	
I think that I will need the support of a technical personel to be able to use this cybercrime monitoring system?	
Will the information collected from this monitoring system be easily utilized by forensic expert?	
I thought there was too much incostitency in this cyber monitoring system.	

I find the various function in the cybercrime monitoring system well integrated.	
I find the cybercrime monitoring system cumbersome to use.	
I felt confident using this cybercrime monitoring system.	
I needed to loan a lot of things before I could get going with this cybercrime monitoring system.	

Bio-data

Name:	Latifat Olubusayo BELLO
Date of Birth:	05/02/1986
State of Origin:	Ogun State
Nationality:	Nigeria
Marital Status:	Married
Address:	House 32, Wisdom Estate Afin Iyanu, Eleyele Ibadan
Postal Address:	P.M.B. 5382, NACGRAB, Moor Plantation, Ibadan.
E-mail Address:	bellolatifat05@gmail.com, Jkayfuad@yahoo.com
Phone Number:	+2347082152772

Goals
To be resourceful, versatile and dependable in carry out my professional activities.

Academic Qualification
Olabisi Onabanjo University Ogun State (BSC Computer Science)
2004-2009
Community Secondary School Idata Ilagbo Lagos State (SSCE)
1997- 2002

Work Experience
NYSC
CSS NSOFANG CROSSRIVER STATE
(**Mathematics Teacher)** March 2010 – Feb 2011

National Biotechnology Development Agency
(Programme Analyst) Oct 2012- Till Date

- Web setup, management and maintenance
- Data mining, storage and management
- Web profiling and surveillance
- LAN formation and management

Skills

- Team building abilities
- Ability to think and articulate thoughts logically.
- Ability to solve problems and devising a creative means.
- Analytical and organisation competencies to communication skill

Hobbies
Reading, writing and traveling

Referees

Dr. Sunday Aladele
Director/Chief Executive Officer
National Centre for Genetic Resources and Biotechnology (NACGRAB)
Moor Plantation, Ibadan, Oyo State, Nigeria
saladele6083@gmail.com

+2348038074937

Dr, Sakpere Wilson
Lead City University
Tollgate Area
Ibadan
0815958869

Mr. Afolabi Oluranti John
PMB 5382, Moor Plantation
NACGRAB Ibadan.
08060738505

_____ _____

Signature Date

University Compliance Certificate

This is to certify that this thesis by Latifat Olubusayo with Matriculation Number LCU/PG/000895 in the Department of Computer Science, Faculty of Natual and Applied Science, Lead City University, Ibadan is in full compliance with the approved University's Format and Style.

……..

…….

Name **Date**