INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 207-213

e-ISSN : 2583-1062

Impact Factor : 5.725

DECISION MAKING SYSTEM TO OPTIMIZE THE CYBER CRIME INVESTIGATIONS

V. Dinesh kumar[1], Mr. S. Arunraj[2], Ms. Sarika Jain[3], Dr. S. Geetha[4]

[1]M.Sc CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2,3]Center of Excellence in Digital Forensics, Perungudi, Chennai 600 089, Tamilnadu, India

[4]Head of the Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

ABSTRACT

Cybercrime refers to illegal activities committed on the internet or through technology. In the United States, common forms of cybercrime include hacking, identity theft, online fraud, and cyberstalking. These crimes can cause significant financial loss, damage to reputation, and loss of sensitive personal and confidential information. The U.S. government and law enforcement agencies have implemented various measures to combat cybercrime, Including increased. Funding for cybercrime investigations, Stronger laws and regulations, And partnerships with the private sector. However, the rapid pace of technology. Advancement. Continues to present new challenges in preventing and Prosecuting cybercrime. The Federal Bureau of Investigation (FBI) Is the primary law enforcement agency responsible for investigating cybercrime in the United States. The FBI’s Cyber Division. Works on prevent, Investigate, and prosecute cybercrime, including cyber terrorism, cyber-enabled financial crimes, and cyber intrusions targeting both government and private sector networks.

1. INTRODUCTION

Cybercrime complaints in the United States refer to reports of illegal or harmful activity committed using technology or the internet. These types of complaints can be made to local, state, or federal law enforcement agencies, or to organizations such as the Federal Bureau of Investigation (FBI). The IC3, for example, serves as a centralized reporting mechanism for victims of cybercrime, providing a means for individuals to report suspected fraudulent or illegal activity and assisting law enforcement agencies in the investigation and prosecution of cybercriminals. The IC3 also collects and analyses cybercrime data to identify trends and patterns in order to better understand and prevent these types of crimes. The increase in the number of cybercrime complaints highlights the growing concern and impact of cybercrime on individuals, businesses, and the broader economy.

2. LITERATURE SURVEY

Anjali Kumari et.al, around the world, billions of people access the internet today. Intrusion detection technology is a new generation of security technology that monitor system to avoid malicious activities. The paper consists of the literature survey of Internal Intrusion Detection System (IIDS) and Intrusion Detection System (IDS) that uses various data mining and forensic techniques algorithms for the system to work in real time. Data mining methods are proposed for cyber analytics in support of intrusion detection.

Dr. Yusuf Perwej et.al, in recent years, the Internet has become an integral element of people's everyday lifestyles all across the world. Online criminality, on the other hand, has risen in tandem with the growth of Internet activity. Cyber security has advanced greatly in recent years in order to keep up with the rapid changes that occur in cyberspace. Cyber security refers to the methods that a country or organization can use to safeguard its products and information in cyberspace. Two decades ago, the term "cyber security" was barely recognized by the general public. Cyber security isn't just a problem that affects individuals but it also applies to an organization or a government. Everything has recently been digitized, with cybernetics employing a variety of technologies such as cloud computing, smart phones, and Internet of Things techniques, among others.

L. A. Gordon Martin et.al, the Computer Security Institute has started a joint survey on Computer Crime and Security Survey with San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The survey is in its 11th year and is the longest-running continuous survey in the information security field. The 2006 survey addresses the issues considered in earlier CSI/FBI surveys such as unauthorized use of computer systems, the number of incidents in an organization, types of detected misuse or attacks and response actions. Other issues include the techniques organizations use to evaluate the performance of computer security investments, security training needs and the use of security audits and external insurance. The survey has found that virus attacks are the source of greatest financial loss. Unauthorized use of computer systems and the total financial loss due to security breaches has decreased this year. Use of cyber insurance remains low, but may increase in coming years.

Taufik Hidyat et.al, cloud computing is one revolution in information technology (IT) that can share resources, services and data through a network among users. Because users have same rights on the network to transfer data, data are vulnerable to be attacked by unauthorized person. Lately, data security in a system only concentrates on data storage on cloud by utilizing internet security, but a little concentration is found during data transfer. By considering security as a serious problem, an encryption-based proposed system is presented to secure during data transfer. Authors propose an approach to boost system security during data transfer in order to prevent data theft by unauthorized person. To prevent an attack by unauthorized person, Advanced Encryption Standard (AES) will be proposed to secure data transfer and storage in cloud computing. For better future, authors will propose Systematic Literature Review (SLR) to generate suggestions and opportunities in AES cloud computing.

3. EXISTING SYSTEM

A repository that collects and stores information about adversary tactics, techniques, and procedures (TTPs) can provide numerous benefits. By gathering threat intelligence information for each TTP, it is not possible to provide better result to optimize data.

3.1 Technique

Disclose Framework.

3.2 Disadvantage

The calculation of various hash function algorithms can be time-consuming.

4. PROPOSED SYSTEM

Concept

The analysis of data will be conducted to streamline the process. The result of the data will be optimized to take decision over the data.

Technique

EM (Expectation-Maximization) and AES (Advanced Encryption Standard) algorithm

Advantage

It gives the better optimization during the data processing.

4.1 Architecture Diagram

Modules

FBI (Federal Bureau of Investigation)

Court

Sheriff

Module Definition

FBI (Federal bureau of investigation)

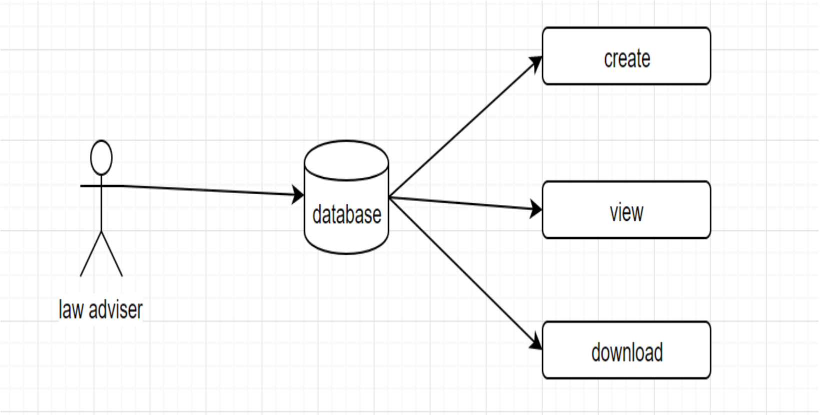
The Federal Bureau of Investigation (FBI) is a national security and law enforcement agency of the United States Department of Justice. The FBI's mission is to protect the American people and defend the Constitution of the United States. It investigates federal crimes, including terrorism, cybercrime, organized crime, white-collar crime, and public corruption, and provides support and assistance to other law enforcement agencies across the country. The FBI also operates a number of national security programs, including the Terrorist Screening Center and the National Cyber-Investigative Joint Task Force.

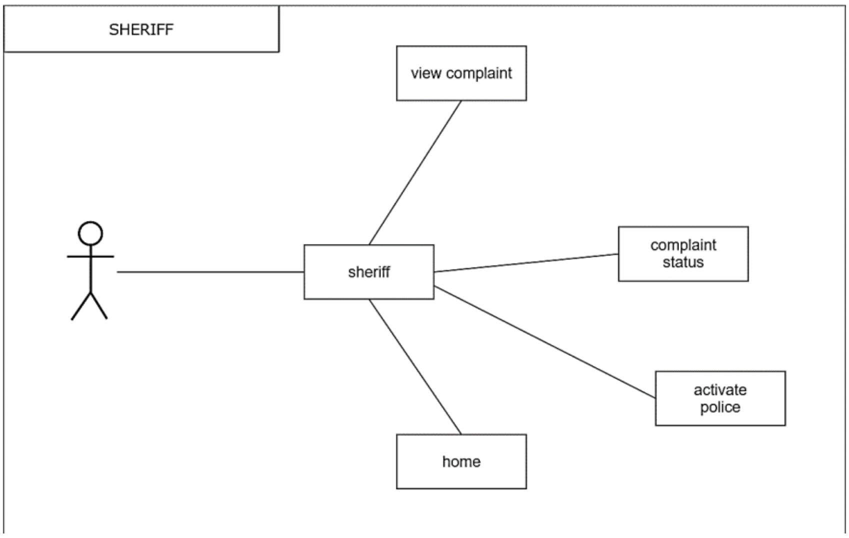
Court

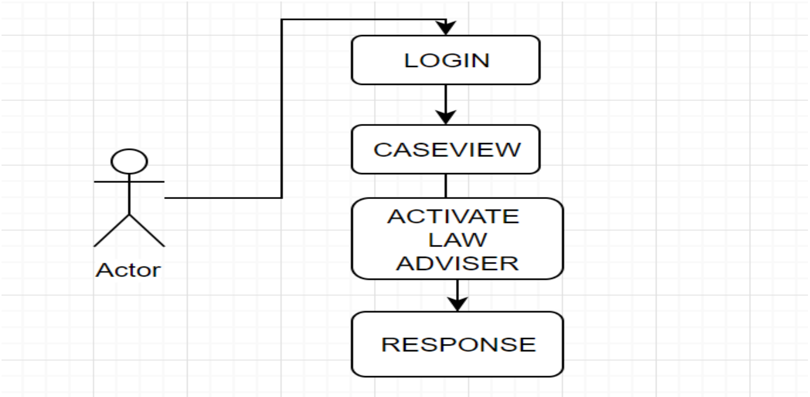
A law adviser for cybercrime is a professional with specialized knowledge and expertise in the laws and regulations related to cybercrime. The role of a law adviser in the context of a cybercrime module would be to provide guidance and support to individuals and organizations that are affected by cybercrime. the role of a law adviser in a cybercrime module is to provide individuals and organizations with the legal support and guidance that they need to effectively respond to cybercrime incidents and to protect their rights and interests

Sheriff

A sheriff in the context of a cybercrime module would be responsible for investigating and enforcing laws related to cybercrime in their jurisdiction. Investigating cybercrime incidents: The sheriff would be responsible for conducting investigations into cybercrime incidents, including gathering evidence and interviewing witnesses. Enforcing cybercrime laws: The sheriff would be responsible for enforcing the laws related to cybercrime, including making arrests and pursuing charges against individuals who have committed cybercrimes.

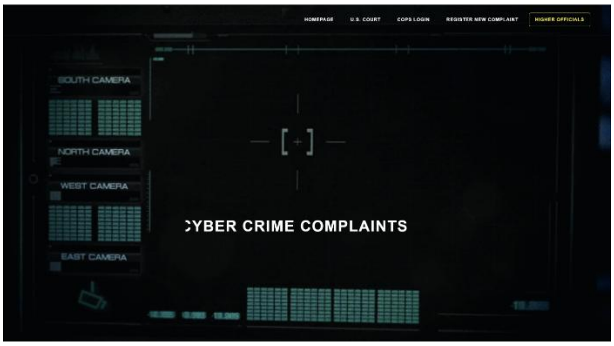






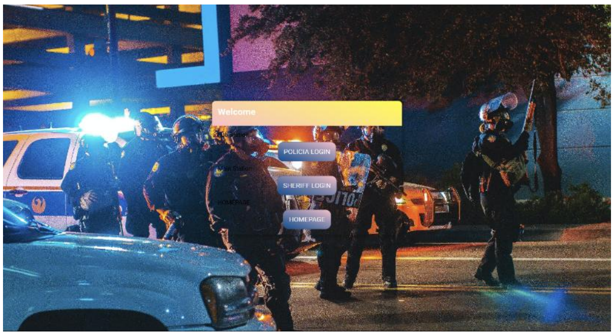
Screen Shots

Home page

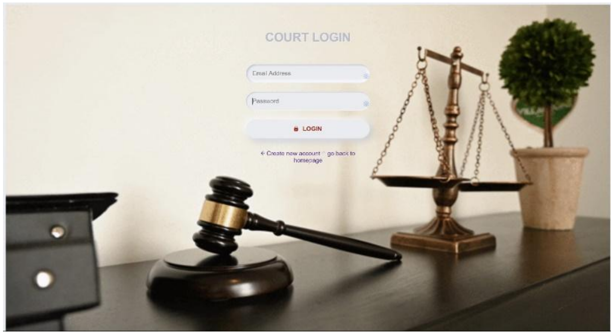


CYBER CRIME COMPLAINTS

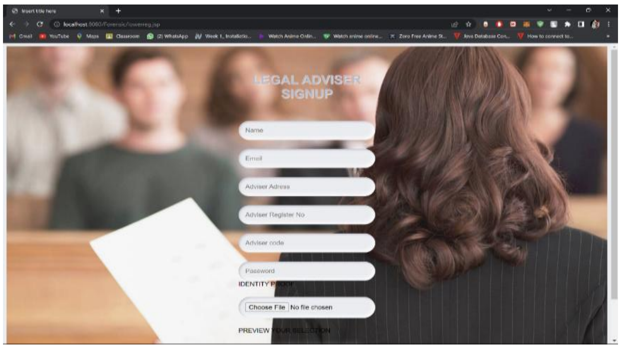
COP Choosing Page



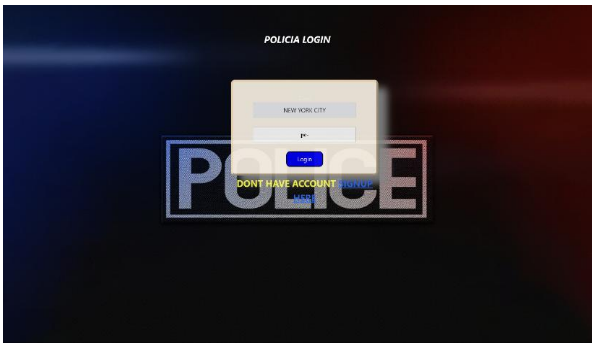
COURT Login Page



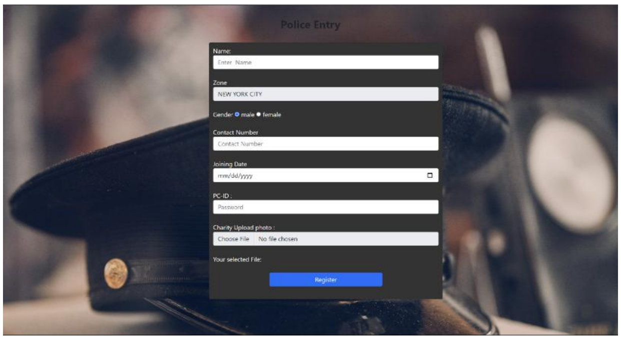
LAW Adviser Register Page



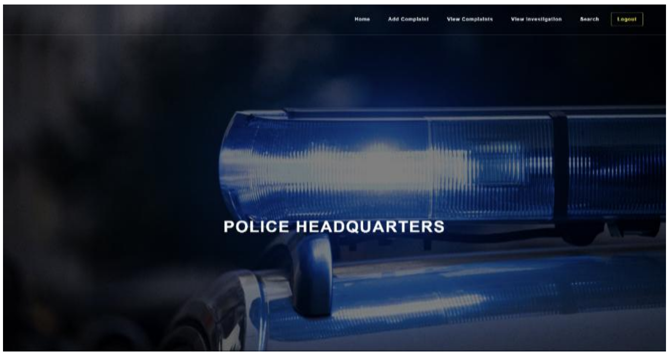
POLICIA Login Page



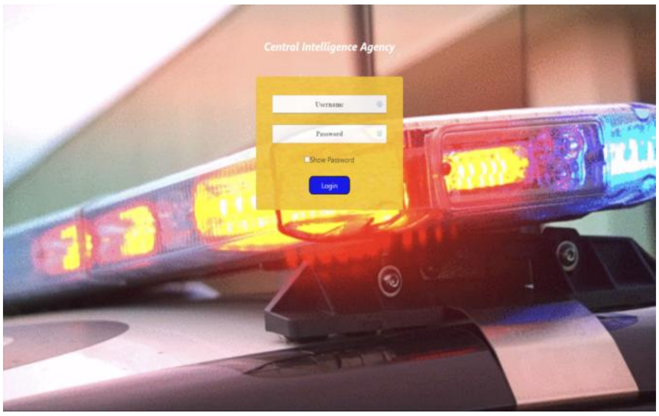
POLICIA Register Page



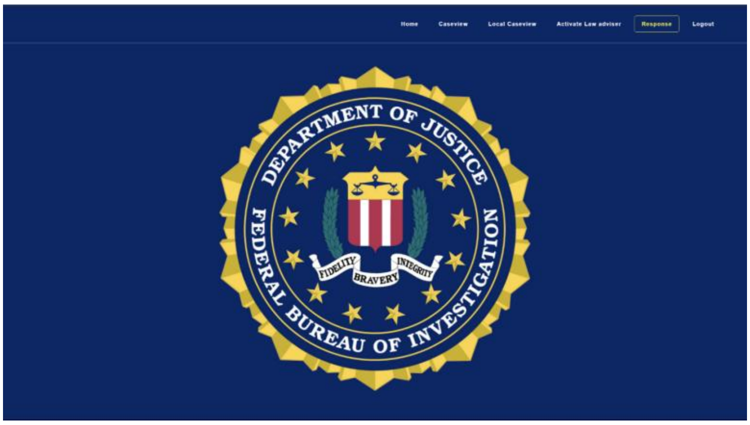
SHERIFF Manage Page



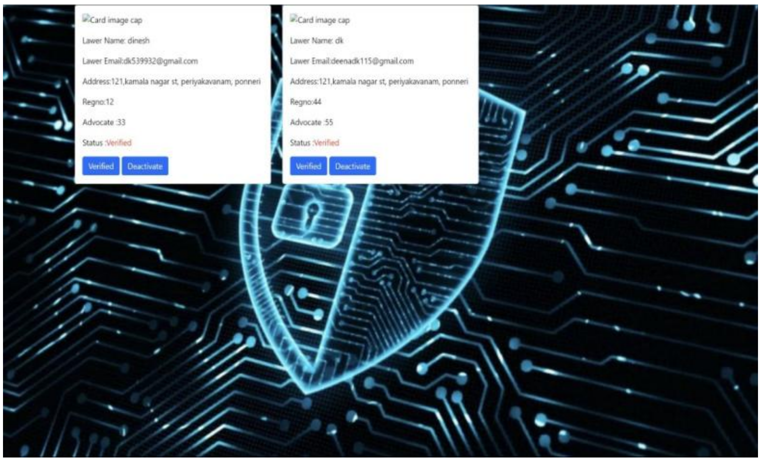
CIA Login Page



FBI Manage Page



LAW Adviser Verification Page



Card image cap

Lawer Name: dinesh

Lawer Email:dk539932@gmail.com

Address:121,kamala nagar st, periyakavanam, ponneri

Regno:12

Advocate :33

Status :Verified

Card image cap

Lawer Name: dk

Lawer Email:deenadk115@gmail.com

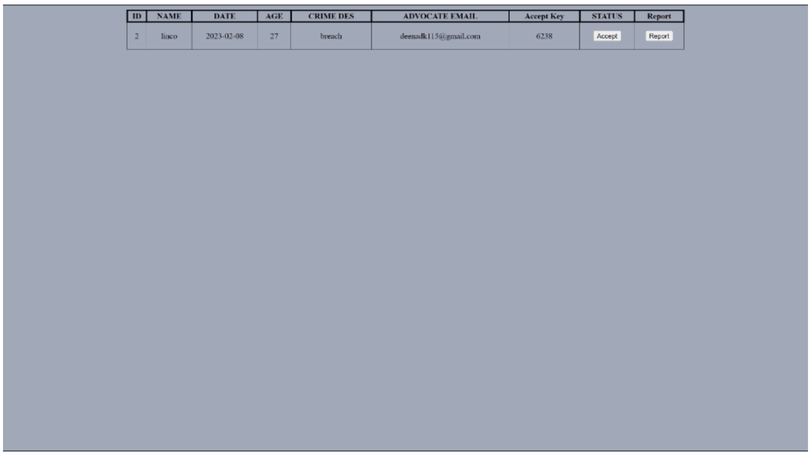
Address:121,kamala nagar st, periyakavanam, ponneri

Regno:44

Advocate :55

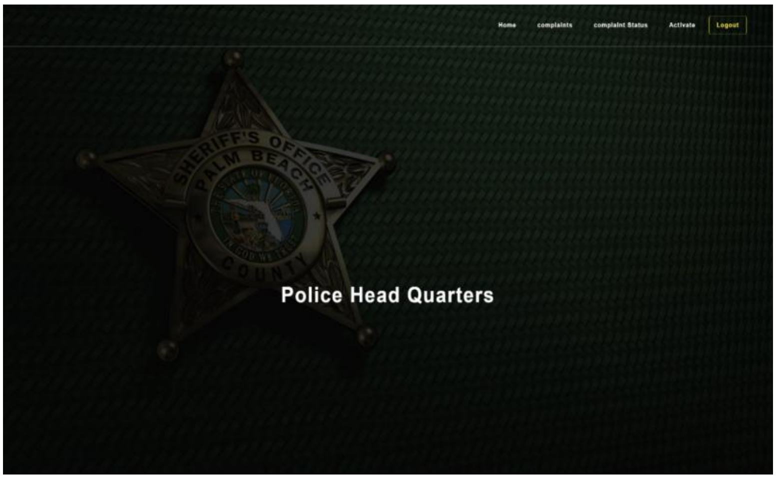
Status :Verified

FBI Response Page

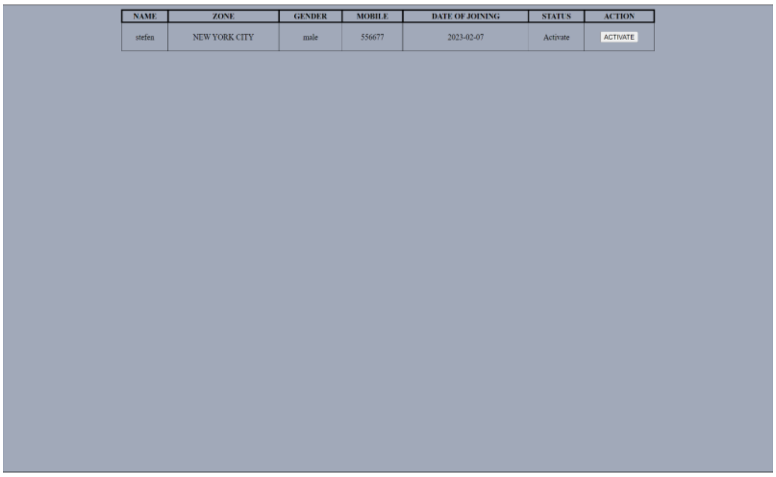


ID	NAME	DATE	AGE	CRIME DES	ADVOCATE EMAIL	Accept Key	STATUS	Report
2	linco	2023-02-08	27	breach	deenadk115@gmail.com	6238	Accept	Report

Sheriff Page



POLICIA Activation Page



NAME	ZONE	GENDER	MOBILE	DATE OF JOINING	STATUS	ACTION
stefen	NEW YORK CITY	male	556677	2023-02-07	Activate	ACTIVATE

5. CONCLUSION

Cybercrime involves the process of identifying, collecting, acquiring, and preserving. Analysing, and presenting of digital evidence. Digital evidence must be authenticated to ensure its admissibility in a court of law. Ultimately, the forensic artefacts and forensic methods used to static or live acquisition depend on the cases and its section. Real evidence must be competent (authenticated), relevant, and material. This software is developed with modular approach. All module in this system have been tested with valid data and everything worked successfully. Acquiring digital evidence involves the process of obtaining and preserving digital data for the purpose of forensic analysis. The digital evidence can be acquired from various sources such as computers, mobile devices, servers, cloud storage, or other digital storage media. The process of acquiring digital evidence must be performed in a manner that maintains the integrity and authenticity of the data. This includes taking proper steps to prevent modification or corruption of the data, and documenting the chain of custody of the evidence. The method of acquiring digital evidence depends on the type of data and the source, and can range from live acquisition techniques such as memory imaging to static techniques such as disk imaging. It is important to follow best practices and industry standards for digital evidence acquisition to ensure the admissibility of the evidence in a court of law.

6. REFERENCES

[1] "Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001, and Best Practice Requirements" by David Watson and Eoghan Casey.

[2] "A Survey of Cybersecurity and Privacy Research" by Y. Al-Turjman, published in the Journal of Information Security and Applications in 2021.

[3] "The State of Industrial Cybersecurity: 2020 Report" by Kaspersky, published in 2020.

[4] "A Systematic Review of Multistep Attack Detection in Cybersecurity" by X. Chen, Y. Li, and X. Lu, published in the Journal of Network and Computer Applications in 2019.

[5] "Standardizing Cyber Threat Intelligence Information with the Structured Threat Information Expression (STIX)" by S. Shackleford and J. Hoelzle, published in the Journal of Information Security and Applications in 2016.

[6] "A Cyber Forensics Needs Analysis Survey: Revisiting the Domain's Needs a Decade Later" by H. Alshammari, A. Alshammari, and M. Al-Turjman, published in the Journal of Digital Forensics, Security and Law in 2020.

[7] "Internet Crime Report 2020" - published by the FBI's Internet Crime Complaint Center (IC3).

[8] "A Guide to Integrating Forensic Techniques into Incident Response" by C. Sanders, published in the Journal of Digital Forensics, Security and Law in 2013.

[9] "The Evolution of U.S. Cyber Crime: A Historical Review and Future Projections" by M. Cloppert, published in the Journal of Digital Forensics, Security and Law in 2011.

[10] "U.S. Cyber Crime: Challenges and Strategies for Investigation and Prosecution" by M. Cloppert and J. Tyworth, published in the Journal of Digital Forensics, Security and Law in 2015.