Cyber Investigation Portal

[1]**Submitted By-** Aasthashree Mudgal, Manas Patil (Students of VPPCOE, Mumbai)
[2]**Under the guidance of-** Prof Manjiri Pathak(Computer Engineering, VPPCOE)

Abstract – Cyber security has been really important for organizations for a long time, notwithstanding, even with interests in security cycles and innovation, cyberattacks are ordinary across all enterprises. Assessing occurrences throughout the long term, cybercriminals have been keeping occupied with sharpening their art, bringing about online protection episodes expanding no matter how you look at it.

As we know, Cybercrimes are difficult to investigate and prosecute because it often crosses legal jurisdictions and even international boundaries.

Our Cybsec- investigation portal will help investigators to monitor the activities using our tools that give investigators access to criminals' devices. The script he runs, the attack he performs the webpages he visits – all the logs are collected through keyboard strokes. The tool is installed on a criminal's computer and records everything he types. It also collects sensitive information like IP addresses, System Configuration. Then it sends this log file and a screenshot of the Device to an Investigator's email, where the cyber cell makes use of all this sensitive information. Tools are hidden so deep that even some antivirus programs can't detect them. Designed tools get embedded with the operating system kernel which makes it too difficult to detect by antiviruses.

Key Words: Cybersecurity, Security, Technology, Infosec, Cybercrime, Cyberattack, Privacy, Data security

1. INTRODUCTION

All through the present web-empowered networks, the expanding accessibility of organization access improves digital-related infringement. This ascent is boosting associations, which are attempting to forestall criminal operations, to determine network security concerns.

Cyberthreats are continually developing to exploit online conduct and patterns. The COVID-19 episode is no exemption. Cybercriminals are assaulting the PC organizations and frameworks of people, organizations, and, surprisingly, worldwide associations when digital guards may be brought due down to the shift of concentration to the wellbeing emergency. Cybercrime is turning into a worldwide peculiarity and an overall concern. As cybercriminals face no limits, the customary regulation authorization approach is becoming old. If the borders and artificial boundaries set up by countries are becoming a big obstacle to investigating and prosecuting traditional crime, the concerns are even bigger in regards to identifying, investigating, prosecuting, and bringing cybercriminals before justice. Our Investigation portal investigates digital and cyber-enabled crimes such as hacking incidents, data

1.1 Aims & Objectives

The main objectives behind the Cyber Investigation Portal are:

- To detect cybercrimes and receive complaints about cybercrimes.
- To collect cyber-crime threat intelligence about the cybercriminals and criminal infrastructure.
- To investigate cybercrime cases.
- To do analytical as well as information investigation connected with cybercrime cases.
- To prepare and launch public awareness campaigns to prevent cybercrimes.
- To work with researchers, academia, and the private sector to improve cyberspace security.

1.2 Motivation

The motivation behind creating Cyber Investigation Portal is the problem statement given by the Bureau of Police Research & Development (Smart India Hackathon 2020) Criminal Navigation using Email-based Tracking System, which gives the facility to report Cyberbullying incidents to authority.)

2. SYSTEM ARCHITECTURE

Cybercrimes are difficult to investigate and prosecute because it often crosses legal jurisdictions and even international boundaries. The investigation portal will help investigators to monitor the activities using our tools that give investigators access to criminals' devices.

2.1 Current Scenario

Several potholes exist within the system due to which a gap continues between reporting of crime, arresting Search for Legal Articles a criminal, and finally ensuring successful prosecution of the accused in Cyber Cases.

Emerging trends of cyber-crimes include hacking, identity theft, spamming, phishing, and cyberstalking. With these arising patterns in wrongdoing, it is about time for the

Indian police to patch up and change the exploring system for the effective indictment of such digital cases.

2.2 Proposed System

The recent report gives us a clear picture of how much cyber has increased. To find out defaulters, we want Cyber Forensics innovation. We want digital warriors who can secure and restrict these assaults. These crimes are dangerous not only to organizations but it is becoming a threat to human life also.

The proposed system is user-friendly and easy to use. We have divided the portal into four parts. Cyber Attacks, Cyber News, Cyber Tools, and anti-phishing portal. This Portal will be investigating, analyzing, and recovering critical forensic digital data from the networks involved in the attack—this could be the Internet and/or a local network—to identify the authors of the digital crime

We will implement the system using MySQL for storing the data. We have used Python scripts to create the tools. We are going to use AI/ML to implement Incident Response & Threat Intelligence. The required items are fetched from the database such as incident details along with victim name and attack-related information etc. The admin can have the authority to access the database.

When the client is signed in, they are given sure honours. We can connect the various structures utilizing MySQL to utilize the framework.

2.3 System Backend

The proposed system comprises three layers: information assortment, pre-processing, and application. The application layer incorporates two sub-layers: one for forecast and one for assessment. The exploratory examinations obtain real data from sensors. The information collection layer involves the gathered sensor information as data sources. Different clean-up cycles of information and investigation techniques are applied in the pre-processing layer to eliminate abnormalities from the genuine information.

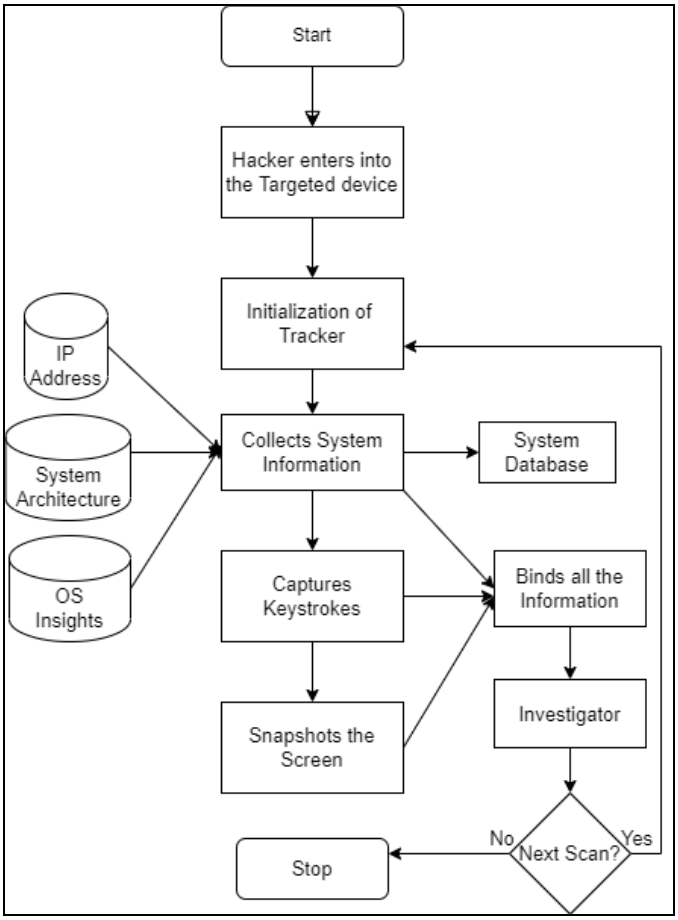
The system which can learn from a security database is suitable for dynamic decisions. Subsequently, in this exploration, we limit security issues and propose an effective information-driven interruption location structure in the field of network protection. This structure thinks about a laid-out signature and has seen inescapable acknowledgment and business achievement as of late. Its system screens network action and distinguishes conduct patterns for gambles by inspecting the connected security data.

This strategy isn't just effective in estimating accuracy for obscure datasets by wiping out overt repetitiveness in recreation yet, in addition, mitigates the system's computational intricacy by restricting the elements of the element while building the comparing structure.

Our moment backing to such cases, our reports, and discoveries empower regulation implementation to quick track their examination We will utilize instruments are (ML-based) to the salvage in network protection. Composite AI misrepresentation recognition motors are showing exceptional outcomes in perceiving confounded trick designs. Extortion identification frameworks' high-level investigation dashboards give exhaustive insights concerning episodes.

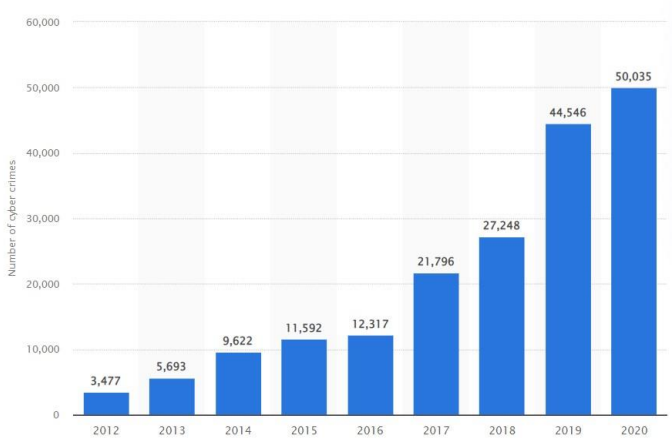
This entryway helps us in exploring, investigating, and recuperating basic legal advanced information from the organizations associated with the assault this could be the Internet as well as a nearby organization to recognize the creators of the computerized wrongdoing and their actual expectations.

Workflow:



Flowchart of Cyber-Tracker(Tool)

Data Insights of Cybercrimes (2012-2020)



3. CONCLUSIONS

3.1 Summary

Our Investigation portal investigates digital and cyber-enabled crimes such as hacking incidents, data breaches, phishing attacks, email fraud, financial crimes, online scams, and cyber-attacks. Our instant support to such cases, our reports, and our findings enable law enforcement to fast-track their investigation. Our portal helps Corporations, Small Businesses, and Individuals address unwanted cyber issues impacting their lives. Crimes range from Cyber Harassment, Unlawful computer Intrusions, Invasion of Privacy, Internet Fraud, Trademark Infringement, Defamation, Copyright Infringement, and Intellectual Property Theft.

3.2 Future Scope

This project can be further enhanced to provide greater flexibility and performance with certain modifications whenever necessary. This portal can be easily implemented under various situations. We can add new features as and when we require such as integration with IoT and cloud facilities. Portal can be converted into a mobile application.

ACKNOWLEDGEMENT

1)Prof Manjiri Pathak, Department of Computer Engineering, VPPCOE.

2)Dr. Mahavir Devmane, HOD, Department of Computer Engineering, VPPCOE.

3) Dr. Alam Shaikh, Principal, Department of Computer Engineering, VPPCOE.

REFERENCES

1] Cyber Forensics and Comparative Analysis of Digital Forensic Investigation Frameworks (IEEE Paper)

2] An Investigation on Cyber Security Threats and Security Models (IEEE Paper).

3] Cybercrime investigations in the era of big data (IEEE Paper)