Advantageous Effect of Breakthrough Technology in Cybercrime Investigation: A Thoroughgoing Study

Abstract

Advent of Technology and the advancement of the same have aided the human race to enjoy its supremacy in all the aspects of the life. Though the longstanding question of whether technology is boon or bane is not res integra, the collective opinion is that unless it is not a bane, it would be a boon to mankind. One of such unintentional outcome of techno-progressivism is cyber crimes, its catchall definition is that crimes which are conducted under the aegis of technology is called cyber crimes, as it encompasses all the crimes conducted in cyber space or can yield digital evidences. If a crime is reportedly to be taken place, verdict of acquittal or arrest is the culmination of investigation. The traditional crime investigation strives to identify the criminal through clubbing the reports of forensic evidence, DNA evidence, testimonies of witnesses; nevertheless, as in cyber space the crimes are carried out by an anonymous perpetrator, it is impossible for the cyber crime investigation without an adequate knowledge of automation to indentify the criminals hiding behind the keyboard. The primary question pertaining to the subject is evidently Emergent Technologies are walking a tightrope between accentuating cyber crimes and unerring certainty in cybercrime investigation? Cybercrime investigation is not a piece of cake. There are many challenges when it comes to cybercrime investigation be it Loss of data, obstacle pertaining to International Operation, Location detection issues, Jurisdiction issues etc. It requires application of technology more than application of mind. Digital Forensics can take the queen move to keep a checkmate to cybercrimes. This paper discusses about the Innovative Technologies to combat Cybercrime, methods and Frameworks and Obstacles pertaining to it.

Keywords*: Techno – progressivism, Cybercrimes, Cyber Law, Investigation, Cyber Forensics*

1. Introduction

An act would be labeled as cybercrime when it is illegal and conducted through cyberspace by the use of a computer and has an impact on the physical world. Going through the traditional definition of crime, any behavior that violates criminal law and attracts prescribed sanctions is called a crime. It is pertinent to note that the current definition of cybercrime is wider enough to encompass all the activities that the law forbids and deviant behavior in global networks. With the advancement of technology and increased use of the internet, people are becoming more susceptible to being victimized by cybercriminals. The continuous cyber attacks by perpetrators on the internet are the combined consequence of skyrocketing usage of the internet, digitalization of confidential information, and ever-changing strategies and hacking methods of criminals. A research[1] highlights that to be categorized as a cyber crime an act should be the outcome of a modernized criminal method that involves the concealment of identity, intention, and motive of the criminal with heightened intelligence, which impedes the evidence collection and expedient investigation. Substantially, the difference between cyber crimes and traditional crimes is apparent, and the techniques to probe such crimes also vary. The magnitude of cybercrime is wider enough to cover all the shades of cybercrime from common cyber theft to the crime of cyber invasion which unshackles the foundation of a country. Whether it is an individual or country, as both are certainly preyed on by cyber crooks in cyberspace, the investigation requires technical know-how to collect pieces of evidence from the devices enabled by information technology. Nevertheless, as the considerable number of Indian police personnel lacks the technical skills sufficient for clue discovery and detection, the government is seeking the help of agencies.[2] The effective investigation of cybercrime is achieved through an enhanced legal framework and the cyber forensic mechanism that is capable of tracing the network points related to the crime, which could be anywhere in the world.

2. Cyber Crimes and Cyber Criminals

Through the eyes of a layman, cybercriminals can never be easily caught as cyberspace is a boundary-less communication platform, where the high-tech offenders hide behind the

[1]Yanbo Wu et al, *Research on Investigation and Evidence Collection of Cybercrime Cases*, J. Phys Conf. Ser. 1176 (2019), https://iopscience.iop.org/article/10.1088/1742-6596/1176/4/042064/pdf.

[2] Vanathi J, Jayaprasanna S, *A study on cyber crimes in digital world*, International Journal on Recent and Innovation Trends in Computing and Communication, 2(9):1-4 (2014).

keyboards while committing crimes or misdemeanors and leave clues, which need relatively better forensic tools to decipher. Various reports provide that in most cybercrime cases, there is an involvement of organized crime syndicates who conduct or hire hackers to conduct crimes against an individual of high social strata, corporation, or government to make a profit out of technical shortcomings, yet, the fact cannot be evaded that these cyber criminal's target victim selection does not exclude technically sophisticated people. As in today's world, technology deprivation is becoming a serious issue with digitalization and economic inequality whilst such a progression is threatened by cyber theft, online fraud, malware, embezzlement, and so on carried out by black hat hackers. There are different classes and categories of hackers grouped on the basis of their activity, they are as follows

Disgruntled employees: These are ex-employees of the companies, who take revenge by causing economic losses by stealing and disseminating non-physical and most confidential data.

Elite: This class contains highly technically skilled hackers who are frontrunners of this digital world as they code software hacking tools, which the large community of unskilled hackers called script kiddies learns and uses.

Cyber terrorist: These hackers steal information and exchange it for cryptocurrency to the organization, which threats or coerces a government to achieve a political or social objective.

Hacktivists: This is the group of hackers who work with unity to carry out denial of service attacks (DoS) by defacing the domain to satisfy the socio-political cause.

Suicide Hackers: Hackers categorized under this head are the active members of cyber terrorism who hacks for a crucial cause, generally political. Like suicide bombers, these suicide hackers in cyberspace are not afraid to lose anything in the course of satisfying their organization's object.

All the aforementioned classes of hackers fall into the category of black hat hackers. These hackers widely commit the crime of hacking[3], cyber terrorism[4], cyber trespassing, phishing, cyber espionage, e-commerce fraud, trogon horse attacks, cyberstalking, data diddling, cyber forgery[5], data manipulation or theft[6], worm attacks, cyber morphing[7], child pornography[8], etc. As

[3] Information Technology Act, 2000, § 65, No. 21, Parliament of India, 2000 (India).
[4] Information Technology Act, 2000, § 66F, No. 21, Parliament of India, 2000 (India).
[5] Information Technology Act, 2000, § 66D, No. 21, Parliament of India, 2000 (India).

per reports,[9] the Indian Computer Emergency Response has received 12.67 lakh incidents in the year 2022 (till November). The skyrocketing number of cybercrime cases is forewarning the future victimization of the majority of internet users, if the law chooses to be silent on this acute problem and officials continue to obsolete technologies for investigation.

A. Cyber Fraud in 21st Century

Cyber Frauds are increasing in this digital era. We see interesting headline every day in the newspaper. Behind each and every cyber-attack there are combinations of different master minds, impeccable technologies and coding which are not crack able. You set up two-factor authentication for all of these services, nobody should be able to access them without a code sent only to your phone

You spent a wonderful weekend in the woods, taking in the fresh air and lovely weather. You haven't heard your phone ring once, and you're not sure you've missed it. As you enter the driveway, your phone suddenly becomes inundated with messages, emails, and notifications. It appears that the PIN on your bank card has been altered, and several withdrawals from you. When you try to call your bank right away, you discover that you don't have mobile coverage. Only because you home internet was active did you receive these messages? No calls may be placed or answered at all! Your phone number has been taken by someone, along with it, your email, social media accounts, and bank information. You notice messages from a few of your buddies popping up, asking why you've been requesting so much money...our accounts have been made. How did this happen?

B. The Reality

Christine, who runs the Her Money Moves blog[10], experienced just this. She never kept her password on the app, but she thought that hackers had gained access to her funds through her usage of a mobile banking app. Although it's impossible to say for sure how they got their hands

---

[6] Information Technology Act, 2000, § 43, No. 21, Parliament of India, 2000 (India).
[7] Information Technology Act, 2000, § 67, No. 21, Parliament of India, 2000 (India).
[8] Information Technology Act, 2000, § 66E, No. 21, Parliament of India, 2000 (India).
[9] MEDIANAMA, https://www.medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/#:~:text=The%20Indian%20Computer%20Emergency%20Response,Parliament%20on%20December%2014%2C%202022 (last visited Jan. 2, 2023)
[10]ANA DASCALESCU,https://heimdalsecurity.com/blog/12-true-stories-that-will-make-you-care-about-cyber-security/ (Last visited Jan. 3,2023)

on her banking information, they undoubtedly took over her phone number. Theft of this nature is increasing in frequency. One can impersonate you when calling your mobile service provider using just a few basic pieces of information, such as the last four digits of your phone number. They might even mimic you in person at a cell phone store, replete with a bogus driver's licence. Your two-factor authentication is useless once they have your number saved to their phone.

3. Latest Trend

The following are the latest technology tools that detects Cyber Frauds

A. Geolocation[11]

The first detecting fraud technique on our lists is geolocation. Geolocation technology identifies the user due to its physical whereabouts at the moment of purchase when a customer submits a new order. You can determine whether buyer placed the purchase from a suitable location by contrasting this with the data the supplier has on record. The system is not perfect because a customer may make purchases while out of the country. The fraudulent scoring process benefits from the use of geotargeting fraud detection systems as data nodes. For instance, it would be suspicious if a purchaser in Australia used an American account number payment information.

B. 3-D Secure

For buying online, 3-D Secure is a system that functions like a PIN code. The objective is to confirm that customers are valid cardholders. Many retailers were reluctant to use the first iteration of 3-D Secure. The 3DS 2.0 and later generations, on the other hand, fix many of the issues with the older technology. Today, many retailers view 3DS as a crucial tool for reducing fraud and the ensuing charge backs.

C. Fraud Scoring

Each payment is examined by this fraud prevention programme using a variety of suspicious transactions. A cumulative "score" representing the degree of risk associated with the purchase is

[11] FRAUD DETECTION AND PREVENTION TOOLS,https://chargebacks911.com/fraud-detection/ (Last visited Jan. 6,2023).

then produced. You can make fairly straightforward "ups" or "downs" decisions using fraudulent assessment. If a transaction raises too many warning signs, you can either automatically reject it or manually review it. Again, for better result, though, you'll have to incorporate vibrant rules into the procedure.

D. Biometrics

You can use biometric technology in the world of e-commerce, did you realize that? With mobile payment systems like Google Pay and Apple Pay, it is feasible. Two-factor authentication is used by these payment applications. To unlock the phone with a passcode or fingerprint, the user must first present another form of valid identification. Additionally, payments done using digital money are segmented, exactly as a purchase made with an EMV chip.

E. Velocity Checks

The truth is that time isn't on the side of fraudsters. They aim to take as much they can before their behaviour is noticed, thus they want to do it rapidly. As a result, they frequently try to make several quick purchases of items with a high residual value. When a user makes repeated purchases, the programme flags those transactions as suspicious. If you suddenly receive a batch of transactions through one person, velocity checks might help you stop all transaction velocity Checks

F. Open Computer Forensics Architecture

The Dutch National Police Agency may be the author of the forensic analysis framework known as OCFA, or Open Computer Forensics Architecture. In order to achieve their main objective of accelerating their digital evidence investigations, they created this programme, which enables researchers to access information from a uniform and user-friendly interface. The Sleuth Kit, Scalpel, PhotoRec, and many other well-known cybercrime investigation tools have it integrated into them or it makes up part of their fundamental functionality. Although the authorized project was ended a while ago, agencies from all over the world continue to use this tool in conjunction with the best forensic solutions.

4. Investigation and Evidence Collection of Cybercrime Cases

To the common knowledge, if a cybercrime is reported, the investigation begins with questions that why the crime has been committed, what would be the cause and motive of the crime, and how the victim has been victimized. Basic information collection precedes cyber forensics. After collecting the information from the victim's e-device, cyber forensic tools are used to collect shreds of evidence. The steps involved in cybercrime investigation are for searching the criminal by tracking the IP address, and email address, and cracking the password. If the suspect's computer has been seized, the evidence could be collected through recovery and retrieving the deleted data, cracking passwords, and analyzing web server logs.

Cybercrime detection has a sequence for investigation methods; in order to start the cyber investigation the forensic investigator should prepare the First Response of Procedure (FRP), then the investigator should send the information collected at the cybercrime scene to the forensic lab, where the clone bit stream images are prepared for the collected evidence to avoid tampering and then converted into MD5 (message-digit hashing) algorithm. After completing the investigation, the forensic investigator has to prepare the final investigation report.

Before proceeding with the investigation, it is imperative to protect the cybercrime scene, though it is obvious that cybercrime is not confined by any boundary restrictions and destruction of evidence from the computer is an easy task to be carried out, it is the duty of the investigating officer to determine the cybercrime scene through identifying the criminal, his motive, the mean of crime i.e. the device and ascertaining the logs or other relevant records of the device. After determining the crime scene, the investigating officer can investigate the cybercrime scene, where he extracts the magnetic storage of the device, and then the online tracking could be done.

5. Case Study: Live versus Post-mortem

Investigators can gather sensitive information during live investigations that is not often available during a post-mortem probe. Processes that are now executing, event logs, network data, authorized drivers, and licensed services can all be included in this data. Do you know why this is significant to us? Let's examine the situation of running the system and how this might be very relevant to us. The types of programs that may be functioning on a computer are revealed by the running services. Many users are not even aware that all these services exist because they

run at a much top importance than processes. They are a frequent target for hackers due to its higher priority and the usual end user's lack of attention.

We can see the condition of these services by doing a live investigation, which may be essential to our research. For instance, a hacker might disable McShield[12], a McAfee Antivirus service, only to return later and infect the computer with dangerous malware. In the instance of registered drivers, you could counter that a postmortem inquiry could yield a list of the drivers. This is accurate, but if you perform a live investigation at a crime scene, you may even be able to observe the driver of a digital camera.

Thus, you are aware of where to search for that camera in your neighborhood. However, if you left the area and subsequently went back to look for the camera driver, all you could do was pray that the camera was still in place. Along with the process's name, we can view its priority, thread count, handle count, memory utilization, and uptime. You might once more wonder why any of these matters. This information is crucial if you want to judge what someone is doing right now as well as what they having done in the past. Additionally, comprehending the actual process list is crucial in the domain of memory-resident executable.

In a post-mortem investigation, physical memory (RAM) is potentially the most important piece of evidence that is lost. However, this crucial piece of evidence is easily captured using live forensic and investigative tools, allowing the entire contents of RAM to be captured locally and even remotely. We are able to witness the contents of a memory dump and can conduct a search for the word key logger in memory. The raw data contents of the memory provide a vast amount of information that could have been lost if the machine was powered down for a post-mortem investigation. Memory contains evidence ranging from user accounts, passwords, unsaved document content, and malicious software.

Physical memory (RAM) may be the most significant piece of lost evidence in a post-mortem examination. The complete contents of RAM can be remotely and locally captured utilising live forensic and investigational techniques, making it simple to obtain this vital piece of evidence. We have access to a memory dump's contents and may look for the term "keylogger" in memory.

[12] DATA SECURITY COUNCIL OF INDIA, Cybercrime investigation manual, jhpolice_cyber_crime_investigation_manual (Last visited Jan 4. 2023).

If the system had been turned off for a post-mortem inquiry, a tremendous quantity of information might have been destroyed, but the original data elements of the memory preserve that information. User accounts, passwords, unencrypted document data, and dangerous malware are just a few examples of the evidence that is kept in memory

6. Consumer Best Practices

The best practices which the consumers can avail are by protecting themselves. By way of using modern technology, which emerges as a security to online threats? These security measures include Antivirus protection, Protection of Browsers to prevent web attacks, The tools which primarily functions to determine the reputation or trust of a file before downloading the same, Protection against Web- attack toolkits, Unpatched vulnerabilities and socially engineered attacks by way of Intrusion prevention, keeping malicious threats from execution and following URL Reputation and safety ratings for online searches. Consumers must keep up to date which means being updated. Virus security contents must be kept updated on daily or hourly basis to keep the computer protected against the virus.

Using an effective password policy also emerges as one of the security measures. Password policy signifies using a mix of letters and numbers. The best security policy implies not to use words from dictionary, since there are easier to attack. Using complex password with uppercase, lowercase, punctuation, special symbols, etc is recommended. The consumers must be aware of what they are doing. The Read end – user license agreement must be carefully read and understood before agreeing. “Free”, “Cracked” or “Pirated” version can contain malware.

The next step that the consumer can take up as a security measure is by guarding the personal data. The personal information should not be made available in public which can be a tool for cybercriminals. Consumers must avoid using public computers for banking and financial purpose and must not also be disclosed. Consumers must think before clicking any URL or opening any email or attachment etc. Consumers must avoid clicking anonymous posts or catchy links displayed in social media which ends up in Cybercrime attack. Consumers must avoid clicking or installing applications by way of pop ups. These are some of the best practices which should be fulfilled to avoid security threats.

7. Working Model

A. Name

Cyber Guard

(i) Objective

This model is an AI driven mechanism which identifies and detects Phishing attack and Digital Copyright Infringment.This model warns alerts and finds out malicious mails suspicious pop ups etc It also acquires evidence and also has a portal to launch complain. This is a unique software as it identifies detects and warns phishing attack and even after the attack it fosters complaint mechanism and helps find the attacker. It has a portal to register complaint. This is basically a dual software that warns, detects, and helps to mitigate the attack and also after the attack combines with the law enforcing department to crack investigate and identify the attacker.

(ii) Phishing a major Cyber attack

In Phishing Usually, the links received in mails lead to dangerous websites where users' devices are infected with malware or passwords are stolen. Malicious content is stored in the downloads, which are often PDFs, and when the user reads the document, the malware is installed. Nowadays, HTTPS is preferred over HTTP by the majority of trustworthy enterprises since it establishes trust. Cybercriminals are now using HTTPS in the links they include in phishing emails, nevertheless. At times Open-source intelligence (OSINT) is the first tool used by cybercriminals to obtain data from published or publicly accessible sources, such as social media or a business website. Then, to make the receiver believe the email is coming from somebody else inside the company, they target specific people within the business using legitimate names, job titles, or work telephone numbers. In the end, the recipient acts upon the email's directive since they think it is an inside request

The working can be divides into two segments:

- Warning /Detection mechanism before the attack
- Complaint Portal after the attack

B. Warning /Detection Mechanism Before The Attack

(i) Functions of the model /Tool

- This tool assists in detecting things like spelling mistakes or a recipient email address with the incorrect domain, as well as identifying contact details or other real information about the company being faked.
- This also is software that tries to fool Exchange Online Protection (EOP)[13], such as downloads or links with typos.
- As harmful shortened links are often used to trick Secure Email Gateways, this application issues a warning about them.
- This programme checks the signal for any logos that appear to be genuine since they might include bogus or harmful HTML
- This tool alerts users to the possibility of dangerous code being hidden in images in emails with little or no text.
- This tool keeps an eye out for interior request that occur from individuals in other divisions or that seem unusual given the job function.
- Because they may lead to a bogus, dangerous website, this programme detects malicious links to stored information on shared folders like Google Suite, O365, and Dropbox.
- This feature notifies when an unregistered caller asks for personal information that looks out of the ordinary for that caller's style.
- Before replying to a text or doing a suggested action, this tool checks the zip code and compares it to your list of contacts.

- As this programme can force a browser into full-screen mode and detect malicious pop-ups, any automated adjustment in screen size could be a warning sign.
- Even though a hotspot seems trustworthy, this tool still can identify it and cause a "unsecure" alert to appear on a device.
- By using this technology, firewall rules are constantly checked and updated to stop incoming traffic from a hijacked website.

When it comes to Digital Copyright Infringement

[13] Security Score Board, https://securityscorecard.com/blog/types-of-phishing-attacks-and-how-to-identify-them((Last visited Jan. 6,2023)

- This tool detects pirated software and warns or gives signal about illegal downloading
- This tool also detects Linked sites be it Surface Lining or Deep Linking
- This tool detects copyright Infringement on a public forum by connecting with its existing sources
- When it comes to Social Media it generally detects plagiarised or copies content

C. After The Attack

(i) Gather evidence

Collecting intelligence, monitoring, and recognizing significant evidence

(ii) Examine the evidence

Locate and examine evidence such hard drives, file systems, RAM memory, dark web and crypto currency tracks, browsing history, and IP addresses.

(iii) Evidence report

Create a report based on the evidence that can be modified and distributed to a forensic team.

D. Key Features Of The Model

- Checking Records and Processes.
- Prevent using duplicated data.
- Backing for concentrating on important topics.
- Consistently updates data and frameworks.
- Examining Graphics
- Offers the design in accordance with the project's specifications.
- Gives a thorough and understandable overview of the project.
- Offers integration with the project's other components, such as the architectural, civil, traffic, and right-of-way aspects.
- Provides good objectives, compatible guidelines, and preparation practise.
- Verifying computations.
- Examining written correspondence

8. Conclusion

There is a famous quote is saying “Predicting rain does not count, Building Arks does “. Building Arks are the investigative technologies used”. Cybercrime investigation is not an easy task rather requires an outstanding skill and knowledge to perform the digital crime scene productively. With these aspects in the hand, there can be proper analysis of data and investigation. This can be effectively used in tracking the authors behind the different types of cybercrime. As a suggestion, the future research should be focused on improving the protection policies for AI powered cybercrimes. Considering the aspect of compensation, policies must be enhanced for the same for providing compensation to affected organization and individuals. The consequences should be carefully foreseen and the different forecasting methods can be used to predict different outcomes. One such example is the use of face technology to track down criminals by intelligent agencies. This is one of the security measurements and can ensure safety by conducting successful executions. Future research should focus on possible use of these technologies to prevent cyber crimes