Establishing The Role of Cyber Forensic for Determining Cybercrime in India: A Study

Surbhi Choudhary

ABSTRACT

Cybercrime has become a pervasive threat in India, with a wide range of activities, including financial fraud, data theft, and intellectual property infringement.

Cyber forensic investigations play a crucial role in identifying, collecting, preserving, and analyzing digital evidence to determine the perpetrators of cybercrimes. This study aims to explore the significance of cyber forensic techniques in establishing the role of individuals or groups involved in cybercriminal activities within the Indian context. By examining various case studies and analyzing the effectiveness of existing cyber forensic frameworks, the research seeks to identify challenges and opportunities for enhancing cyber forensic capabilities in India to combat cybercrime effectively.

Cybercrime has emerged as a significant threat to individuals, businesses, and nations worldwide. India, with its rapidly growing digital landscape, is particularly vulnerable to cyberattacks. To effectively combat cybercrime, robust investigation techniques are essential. Cyber forensics, a specialized field that applies scientific and investigation techniques to digital evidence, plays a crucial role in this regard.

Cybercrime is a serious problem in India. People use computers to do bad things like stealing money, stealing information, and copying things that don't belong to them. To catch these bad people, we need to look at their computers. This is called "cyber forensics." We can find clues on their computers that show who did the bad things. Moreover, cyber forensics aids in the reconstruction of cyberattacks . By analyzing the digital footprints left behind by the attacker, experts can determine the techniques employed, the extent of the damage caused, and the potential vulnerabilities exploited.

Key Words: Cyber forensics, cybercrime, digital evidence , cyberattacks.

INTRODUCTION

In today's world, technology has become an essential part of our lives. We use computers, smartphones, and the Internet for almost everything , from shopping to banking to socializing. While technology has brought many benefits, it has also created new challenges, one of the most significant being cybercrime.

History reveals that cybercrime originated even in the year 1820. That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan, and China. The era of modern computers, however, began with the analytical engine of Charles Babbage.[1]

In addition to physically committing crime using a computer, cybercrimes are largely done in the network area. William Gibson coined the word cyberspace in his literary work Neuromancer (1984).

For the first time, I described electronic activities in the virtual world. To explain the causes of crimes in the network area, Jaishankar (2008) suggested the principle of the room crossing. The principle of 7 states how a person's behavior varies in physical and network areas that can give birth to the crime commission in the network area. Cybercrime refers to any illegal activity that involves computers or networks. It can range from simple hacking to complex attacks on critical infrastructure. India , with its growing digital landscape, has unfortunately become a target for cybercriminals.

In recent years, India has witnessed a significant rise in the utilization of technology and the Internet, leading to a corresponding increase in various forms of cybercrimes, including hacking, identity theft, online fraud, and data breaches. The significance of cyber forensics in combating these threats cannot be overstated. It plays a vital role in assisting law enforcement agencies, organizations, and cybersecurity professionals in understanding the intricacies of how cybercrimes are perpetrated , identifying the individuals involved, and gathering substantial evidence that can be presented in legal proceedings.

[1] Cyber forensics encompasses a range of methodologies and techniques designed to recover lost or deleted data, analyze digital devices, and trace the online activities of potential offenders. By shedding light on these aspects, the research seeks to enhance our understanding of how to effectively protect individuals and organizations from the growing threat of cybercrimes , ultimately contributing to a more secure digital environment in India.

Cyber Forensics : Concept and Analysis

Cyberforensics is the process of checking digital devices to find evidence of cyber offenses. Experts collect and analyze data from computers, phones, and networks to resolve issues such as hacking, fraud, or identity theft. They use special equipment to restore deleted files, track activities online, and find out who is responsible. Cyber forensic police help companies and individuals protect against digital dangers.

Why is cyber forensics important?

Today's modern generation greatly values cyber forensics. Faster investigations and more accurate outcomes are made possible by the combination of technology and forensic science.

The points that show the significance of cyber forensics are as follows: Cyber forensics helps in collecting important digital evidence for criminal tracking. Electronic devices retain huge amounts of data that are invisible to the average person. For instance, every word we say in a smart home causes smart gadgets to gather vast amounts of data that are essential to cyber forensics. Using the evidence gathered online, innocent persons can also use it to defend their innocence. In addition to solving digital crimes, it also solves real-world crimes like murder and theft.

Strategies used by cyber forensic investigators

Cyber forensic investigators analyze the data using a variety of styles and instruments. Some of the styles they constantly employ are

Reverse steganography: Steganography is a technique for hiding sensitive information within digital files, images, etc. Reverse steganography is therefore used by cyber forensic specialists to examine the data and determine how it relates to the case.

Dynamic forensics : In this field, professionals examine and recreate online activity without the use of digital objects. Unintentional changes to data performed by digital processes are related to proof in this environment.

Cross-drive analysis : In this procedure, data from several computer drives is compared and cross-referenced in order to save and break down data that's useful to the inquiry.

Live analysis: In this fashion, the computer of criminals is broken down from within the OS in running mode. It aims at the changeable data of RAM to get some precious information.

Deleted file recovery: This includes searching for memory to find pieces of an incompletely deleted file in order to recover it for proof purposes.

Advantages

- The quality of the computer is guaranteed by cyber forensics.
- Many individuals, businesses, etc. learn about these crimes through cyber forensics and take necessary precautions to prevent them.
- Cyber forensics gathers evidence from digital devices and presents it in court, where it may result in the offender being punished.
- Anywhere in the world, they effectively find the offender.
- They support individuals or groups in safeguarding their funds and time.
- The public can be made aware of the correct information by making it trending.

[1] *See* article by Justice K.N. Basha, Judge, Madras High Court, Chennai.

Cyber Forensic Challenges

1. Challenges with Hardware

The variety and wide range of contemporary digital devices create hardware challenges in cyber forensics. A constantly expanding variety of gadgets, including smartphones, tablets, Internet of Things devices, and encrypted storage units, are encountered by forensic investigators. Collecting data is challenging without specialized tools because many of these devices use exclusive parts and interfaces. Crucial forensic evidence retrieval may also be hampered by data damage caused by physical harm or regular use.

2. Challenges with Software

Software problems include a variety of file systems, operating systems, and applications, many of which may be purposefully changed to obstruct forensic investigation. Malware, encryption technologies, and anti-forensic tools can all be used to conceal or alter digital evidence. Furthermore, forensic tools find it challenging to keep up with the rapid updates and obfuscation techniques in software development, necessitating constant adaptation and expertise to accurately analyze digital environments.

3. Challenges in Cloud Forensics

Because cloud environments are distributed and virtual, cloud forensics presents special difficulties. The spread of data in the cloud across several jurisdictions, geographical areas, and service providers can make it more difficult to gather and preserve evidence. Serious concerns in forensic investigations arise from the dynamic nature of cloud resources (such as virtual machines and containers), multi-tenancy, and lack of physical access, which make it challenging to guarantee the authenticity and integrity of data collected.

2.1. Introduction to Cyber Forensics

Cyber forensics, also known as digital forensics, is the use of computer testing and analysis techniques, which is a blow to identify, collect, preserve, and analyze data from digital devices acceptable in court. This is really a scientific study of digital media for legal purposes. The goal is to highlight the facts and evidence related to cyber offenses or other events related to digital devices.

What is the required set of skills needed to be a cyber forensic expert?

Being an expert in cyber forensics requires the following abilities:

- ➢ One must be knowledgeable about a variety of technologies, including computers, smartphones, network hacking, security breaches, etc.
- ➢ The expert must pay close attention when analyzing a lot of data in order to find proof or evidence.
- ➢ The expert needs to know about criminal investigations, criminal laws, etc.
- ➢ The most recent technology must be taught to the experts.
- ➢ Cyber forensic specialists need to be able to analyze data, draw conclusions, and interpret it correctly.
- ➢ The expert must have strong communication skills so that everyone in the courtroom can clearly understand every detail when the expert presents evidence.
- ➢ The specialist must possess a solid understanding of fundamental cybersecurity.

Digital Evidence and Forensics

Digital evidence is information that can be used in court that has been stored or transmitted in binary form. It can be found, among other places, on a mobile phone and the hard drive of a computer. Digital evidence is frequently linked to electronic crime, or e-crime, which includes credit card fraud and child pornography. But now, digital evidence is used to prosecute not just e-crime but all kinds of crimes. For instance, important information about a suspect's intentions, whereabouts at the time of a crime, and relationships with other suspects may be found in their email or mobile phone records.

Internet fraud: what is it?

Internet fraud is the practice of defrauding or exploiting victims by using software and online services that have internet access. The phrase "internet fraud" generally refers to any cybercrime activity that occurs via email or the internet, such as identity theft, phishing, and other hacking schemes intended to defraud people of their money. Every year, online scams that use online services to target victims generate millions of dollars in fraudulent activity. Additionally, as internet usage rises and cybercriminals' tactics advance, the numbers keep rising. State and federal law both prosecute offenses related to internet fraud.

Types of Fraud Online

- To perpetrate online fraud, cybercriminals employ a range of attack methods and tactics.
- This covers malicious software, spoof websites that steal user information, phishing scams that are complex and widespread, and email and instant messaging services that spread malware.

Internet attacks can be broken down into several key types of attacks, including:

1. Phishing and Spoofing: The use of email and online messaging services to dupe victims into sharing personal data, login credentials, and financial details.
2. Data breach: Stealing confidential, protected, or sensitive data from a secure location and moving it into an untrusted environment. This includes data being stolen from users and organizations.
3. Denial of service (DoS): Interrupting access of traffic to an online service, system, or network to cause malicious intent.
4. Malware: The use of malicious software to damage or disable users' devices or steal personal and sensitive data.
5. Ransomware: A type of malware that prevents users from accessing critical data and then demands payment in the promise of restoring access. Ransomware is typically delivered via phishing attacks.
6. Business email compromise (BEC): A sophisticated form of attack targeting businesses that frequently make wire payments. It compromises legitimate email accounts through social engineering techniques to submit unauthorized payments.

Legal and Institutional

I. **Challenges Complicated Regulations:** Complying with different legal frameworks can be difficult.
II. **Bureaucratic Delays:** Decision-making and implementation are slowed down by institutional inefficiencies.
III. **Corruption and Poor Management: Weak governance** results in resource mismanagement and a lack of accountability.
IV. **Inconsistent Policies:** Businesses and individuals are left in the dark by frequent policy changes.
V. **Judicial inefficiency:** Justice and law enforcement are delayed by slow court proceedings.
VI. Limited Public Participation-The effectiveness of policies is impacted by a lack of stakeholder engagement.
VII. **Enforcement Gaps:** Lack of oversight and enforcement systems lessen the effect of legislation.
VIII. **Institutional Overlaps**: Ineffective governance is caused by disputes between agencies.
IX. **Lack of Transparency:** Public trust and accountability are hampered by limited access to information.
X. **Resource Constraints:** Institutional capacity is weakened by a lack of funds and staff.

CONCLUSION

In India, digital forensics has become an essential tool in routine criminal investigations. These case studies demonstrate the importance of digital forensics in uncovering digital evidence, reconstructing timelines and communication networks, and establishing links between suspects and criminal activity. However, challenges in digital investigations persist,

including data encryption, privacy issues, and the need for specialized training to keep up with rapidly evolving digital platforms and cyber threats. Because digital technologies are constantly evolving, it is critical to continue improving digital forensic techniques in order to protect the integrity of evidence and the rule of law. Given the ongoing evolution of digital crimes, the importance of digital forensics in India's law enforcement and judicial systems cannot be overstated. Cyber forensics is critical in managing India's growing cybercrime problem. However, current systems face several challenges, including technological, educational, and procedural restrictions. As cyber threats become more complex, India's ability to detect, investigate, and prosecute these crimes must evolve. Without considerable advances in infrastructure, people, policy, and awareness, the gap between cybercrime complexity and forensic skills will continue to grow, threatening national security, data privacy, and public trust in digital systems.

REFERENCES

- Boddington, Richard. (2016). A Case Study of the Challenges of Cyber Forensics Analysis of Digital Evidence in a Child Pornography
- European Network of Forensic Science Institutions. (2015). Best practice manual for the forensic examination of digital technology. ENFSI-BPM-FIT-01
- Marcella, Albert, 2008 Marcella Jr., Albert J., "Cyber Forensic : A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes." 2008. Taylor & Francis Group , LLC. Auerbach Publications. pp. 27-48, pp. 77-85, pp. 87.
- Nishesh Sharma, 'Cyber Forensics in India - A Legal Perspective,' Universal Law Publishing.

BIBLIOGRAPHY

Books

1. Rommel Rodrigues' book Kasab: The Face of 26/11 (2010) focuses on Ajmal Kasab, the only terrorist apprehended. It serves as the foundation for the aforementioned film The Attacks of September 11th.
2. Cathy Scott-Clark and Adrian Levy's nonfiction book The Siege: The Attack on the Taj Mahal. It recounts the 2008 attacks on the Taj Mahal Palace Hotel in Mumbai, India, on the night of November 26. Penguin Books originally released the book in 2013.
3. Computer Forensics: Computer Crime Scene Investigation, by John R. Vacca, Cengage Learning, 2nd ed., 2005. (Chapters 1–18). (UNIT I–IV)
4. Marjie T. Britz, "An Introduction to Computer Forensics and Cybercrime," Pearson Education, 2nd Ed., 2008. (Chapters 3–13). (UNIT IV–V)
5. Computer Forensics: Cybercriminals, Laws, and Evidence, MariE-Helen Maras, Jones & Bartlett Learning, 2nd Ed., 2014.

Articles & Journals

- Agarwal , S., & Mishra, P. (2022). The evolving role of cyber forensics in combating cybercrime in India. Indian Journal of Cyber Law and Policy, 8(1), 24-36.
- Bansal, A., & Mehra, T. (2021). Challenges in digital evidence collection in India: A cyber forensic perspective. Journal of Forensic Science and Criminology, 10(2), 50-63.
- Das, R., & Singh , S. (2023). Investigating Cyber Fraud: Insights from Forensic Science in India. Journal of Cybercrime Research, 7(4), 95-107.
- Khan, M., & Thomas, P. (2022). An analysis of cyber forensic tools used in Indian law enforcement. Journal of Digital Investigations, 18(1), 15-30.

Reports

Ministry of Electronics and Information Technology (MeitY) (2023). Cybercrime in India: A statistical and forensic overview. Government of India. Retrieved from https://www.meity.gov.in

National Crime Records Bureau (NCRB). (2022). Cybercrime statistics in India: Trends and analysis. Government of India. Retrieved from https://www.ncrb.gov.in

NASSCOM (2021). Enhancing India's cyber forensic capabilities. Retrieved from https://www.nasscom.in

World Economic Forum. (2022). Cybersecurity and forensic readiness: Global perspective with a focus on India. Retrieved from https://www.weforum.org/reports.in