Page 1226 - 1237 ***DOI:*** *https://doij.org/10.10000/IJLMH.118121*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 4

2024

A Study on Identifying and Overcoming Key Challenges in Cybercrime Investigations

APARNA C.[1]

ABSTRACT

Cybercrime investigations are a crucial aspect of law enforcement and cybersecurity efforts in the digital age. These investigations focus on identifying, tracking, and prosecuting individuals or groups responsible for various forms of online criminal activities, such as hacking, identity theft, fraud, and more. They often involve skilled investigators, digital forensics experts, and collaboration with international agencies to gather digital evidence, trace the origins of cyberattacks, and bring cybercriminals to justice. The rapid evolution of technology and the sophistication of cyber threats continually challenge investigators to adapt and employ advanced techniques to combat cybercrime effectively. The major objective of this research is to to know the challenges faced by crime investigators when dealing with sophisticated hacking techniques, to analyze current trends and emerging patterns in cybercrime investigation, to analyze the ethical and legal issue in investigating cybercrime. This research follows an empirical type of research and sampling method used in this survey is a convenient sampling method. The independent variables like age, gender, education, occupation and dependent variables like major challenges faced by cybercrime investigators when dealing with sophisticated hacking techniques. Staying updated with evolving cyber threats is a major challenge for investigators. From this research it is found out that technology is the major challenge in investigating cybercrime and the legal issue is that the privacy of individuals is affected while investigating their profile . Balancing the need for investigation with individual privacy rights remained a challenge, prompting the development of protocols for handling personal data. Educating the public about cyber threats, safe online practices, and how to report cybercrimes to law enforcement.

Keywords: *privacy, personal data, technology, digital forensic, threats.*

I. INTRODUCTION

The evolution of cybercrime investigation has seen advancements in technology, techniques, and collaboration among law enforcement agencies. Cybercrime investigations have evolved alongside advancements in technology. Early on, law enforcement agencies focused on basic computer-related offenses, but as the digital landscape expanded, so did the complexity of

[1] Author is a student at Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATS), India.

cybercrimes. The 1980s and 1990s saw the emergence of viruses, hacking, and credit card fraud. In the 2000s, the rise of the internet brought about new challenges like phishing, identity theft, and online scams. Law enforcement agencies developed specialized cybercrime units and digital forensics techniques to gather evidence from digital devices. International cooperation became crucial due to the borderless nature of cybercrimes. Governments enact and update laws specifically addressing cybercrimes, ensuring that legal frameworks keep up with rapidly evolving digital threats. Governments collaborate with other nations to share information, intelligence, and expertise, especially when cybercrimes involve international actors. Rapidly Evolving Technology, Focus on Digital Footprints, Enhanced Training and Skill Development, Ransomware Mitigation, Internet of Things (IoT) and Operational Technology (OT) adoption increased. Digital Forensics Challenges, technological advancements can lead to new types of cybercrimes and require investigators to continually update their skills and tools. AI and machine learning were being applied to analyze large volumes of data, identify patterns, and detect anomalies that might indicate cybercriminal activity. Legal procedures for the collection, preservation, and presentation of electronic evidence in court, ensuring its admissibility. The determination of criminal penalties for cybercrimes, including fines, imprisonment, and other punitive measures. Crime scene investigation challenges in the UK and India can differ due to varying legal systems, resources, and socio-economic factors. In the UK, challenges often revolve around managing large volumes of digital evidence, maintaining the chain of custody, and ensuring proper training for investigators. Additionally, privacy concerns and managing scenes involving international dimensions can be issues. In India, challenges might include limited resources, inadequate training, and a backlog of cases, which can hinder efficient evidence collection and analysis. Coordinating between various law enforcement agencies and dealing with diverse cultural and linguistic factors could also pose difficulties. Digital literacy and forensic technology adoption might vary in different regions of India. The aim of the present study was to investigate the association between cybercrime investigations and challenges.

(A) Objectives:

- To Examine the challenges faced by crime investigators when dealing with sophisticated hacking techniques
- To analyze the current trends and emerging patterns in cybercrime investigation.
- To Understand the ethical and legal issue in investigating cybercrime.
- To Study the procedures in cybercrime investigation

(B) Review of literature:

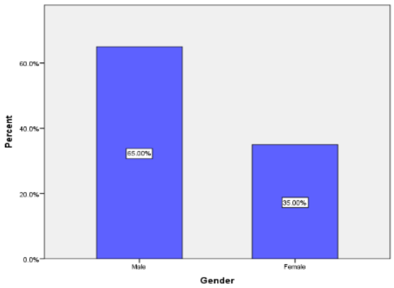
(Ben Brewster. 2016) Cyber crime is a truly global criminal phenomenon which blurs the traditional distinction between threats to internal (criminality and terrorist activity) and external (i.e. military) security and does not respond to single jurisdiction approaches to policing. **(Abiodun Esther Omolara 2022)** The different layers of crime on the Internet can be broken up into three categories: (1) the surface or open web, (2) the deep web and (3) the dark web. These areas of the web contain a host of information that can be valuable to investigations, so it is important to understand the methods that allow investigators to gather and use this information. **(Nouf M. Alzahrani. 2022)** Investigators can also utilize the method of weighting forensic evidence with blockchain technology. This can help with certifying the validity of digital evidence when it is presented in a court. This weighting system first collects evidence in a blockchain that records when the evidence was collected and who was in possession of it at the time. **(Taghreed Justinia. 2022)** FaaS is a cloud-based service where an organization or individual will pay for the forensics services of another company, similar to cloud computing with providers, such as Amazon's AWS. FaaS is changing how forensics is being handled by moving it further into the cloud, which makes cloud forensics more important to understand. **(Antonia Merzon. 2020)** AI can be used by criminals as a tool, but also as a target of their crimes. If criminals can harm a victim's AI systems, it could cause a lot of damage to the victim and their systems. Also, criminals can essentially teach their AI systems to attack the victim's systems, which causes the attack to be faster and more sophisticated than attacks done by individuals. (**Adv Shruti. 2020)** Cyber criminals attack privileged or rich businesses, such as banks, casinos, and investment institutions, where large sums of money are exchanged on a daily basis, and steal critical information. **(Chandra Singh. 2023)** The private sector often holds the keys to provide law enforcement with crucial data to facilitate investigations, and can play a key role in helping to dismantle criminal infrastructures. (**Amarnath Mishra 2023)** Cybercriminals can also use anonymity networks to encrypt (i.e. block access) traffic and hide Internet Protocol address (or IP address), "a unique identifier assigned to a computer [or other Internet-connected digital device] by the Internet service provider when it connects to the Internet". (**Sarbast Moslem. 2023)** The lack of harmonized national cybercrime laws, international standardization of evidentiary requirements (both in terms of admissibility in a court of law, and in terms of international state responsibility), mutual legal assistance on cybercrime matters, and timely collection, preservation, and sharing of digital evidence between countries, also serve as obstacles to cybercrime investigations. (**Tapan Senapati 2017)** Cloud technology is becoming more popular among businesses and individuals. This means that it is a crucial area for investigators to understand. This section discusses the relevant technologies, methods, and frameworks that affect gathering forensic data from cloud sources and using the cloud in forensic investigations. (**Ambareen Siraj. 2021)** breaks cloud forensics into two sections, agent-based solutions and log-based solutions. Log forensics are more popular and widely used. These can be spread into four kinds of investigations: incident driven, provider driven, consumer driven, and resource driven investigations. **(A. Liang. 2013)** discussed eight major information and crime types on the dark web: human trafficking, pornography, child pornography, assassination, drug selling, terrorist activity, cybercrime markets, and cryptocurrency exchange. This information can be used in investigations to determine the identity, motivation, or even location, of the criminal**. (Mangai. 2019)** to communicate and sell stolen identities, credit card numbers and other information, cybercriminals rely heavily on social media platforms such as Facebook, Snapchat, Instagram, WhatsApp, Telegram and other social media platforms". This means that this data, which could be critical to an investigation. (**R. Mills. 2020)** Local law enforcement can view cyber-policing as not their responsibility and be sceptical about calls from scholars and supervisors that more training is needed. This underscores the point that training police officers across the board is likely to present notable challenges. (**James Steele. 2011)** Cyber crime is a truly global criminal phenomenon which blurs the traditional distinction between threats to internal (criminality and terrorist activity) and external (i.e. military) security and does not respond to single jurisdiction approaches to policing. (**Sachi Nandan Mohanty. 2020)** Although information technology has enabled global businesses to flourish, it also becomes one of the major enablers for unscrupulous individuals to commit crime and escape apprehensions by law enforcement agencies. It is often stated that cyber crime investigation & forensics is the largest challenge for law enforcement agencies in this 21st century. (**Michael Cross. 2008)** Cybercrimes, which differ significantly from conventional crimes in many dimensions, are frequently difficult to identify and prosecute. Technology is changing the environment every day, it affects the civilian and military infrastructure in all sectors. (**Robert. 2004)** investigated determinants of patrol officer interest in cybercrime training and investigation in selected United States police agencies. They cite the officers' computer abilities as one element impacting their interest in cybercrime training and investigations. (**Pin-Syuan Jiang 2014)** focused on determining the demands of cyber forensic investigators. They performed a survey of participants from various vocations including cyber forensic students, professors, law enforcement, and practitioners. According to the poll results, participants said that the most pressing requirements are more financing, upgraded tools, improved communication, and amended legislation. (**Douglas J. Dallier. 2021)** Whilst differences in national frameworks present challenges for cooperation amongst European member states, the lack of a common legal framework throughout the world presents significant challenges for international cooperation more generally.

(C) Research Methodology:

This research follows empirical type of research and sampling method used in this survey is convenient sampling method. This study used both primary and secondary data. The secondary data used from government documents, unpublished thesis websites, journals etc.The primary data was collected from the respondents using simple random sampling method with structured questionnaire, occupation etc were also collected. The current paper is based on random method of sampling and the sample size is limited to 200 and most importantly the survey was made in an authenticated way for appropriate result and also tries to reveal the actual truths regarding these issues. This paper also includes various secondary sources to get through the current issues , but the result will be focused mainly on the association of independent variables like age, gender, education, occupation and dependent variables like major challenge faced by cybercrime investigators when dealing with sophisticated hacking techniques, Staying updated with evolving cyber threats is a major challenge for investigators.

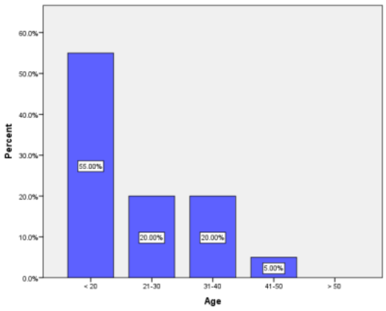
II. ANALYSIS

Figure: 1



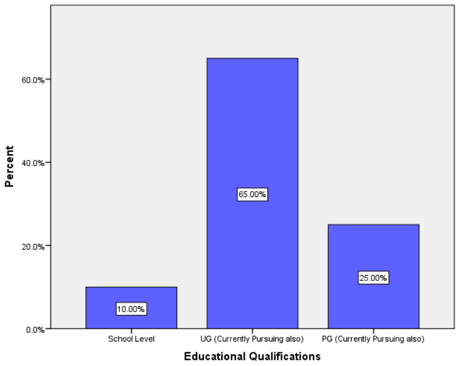
Legend: Figure 1 shows the distribution of gender .

Figure: 2



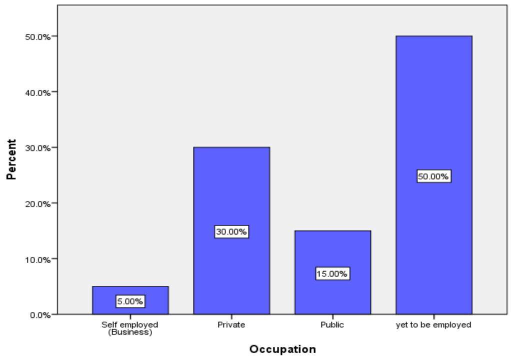
Legend: Figure 2 shows the distribution of age.

Figure: 3



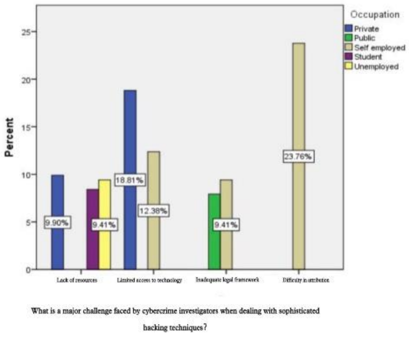
Legend: Figure 3 shows the distribution of occupation .

Figure: 4



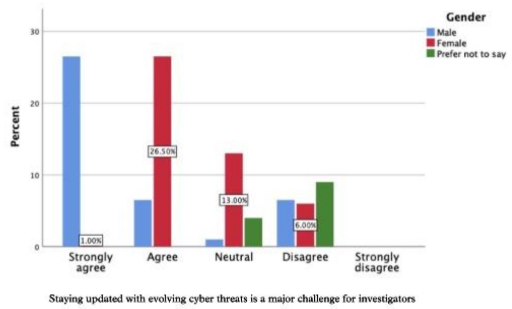
Legend: Figure 3 shows the distribution of educational qualification.

FIGURE 5:



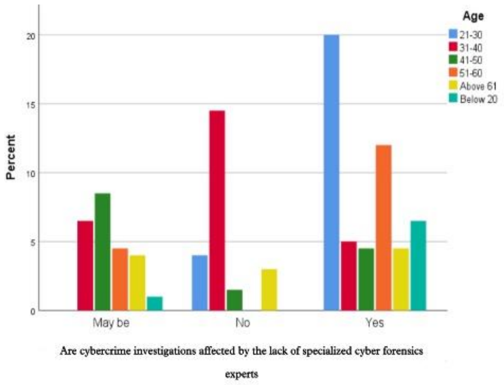
Legend: Figure 5 shows the distribution of occupations with respect to the opinion that a major challenge faced by cybercrime investigators when dealing with sophisticated hacking techniques.

FIGURE 6:



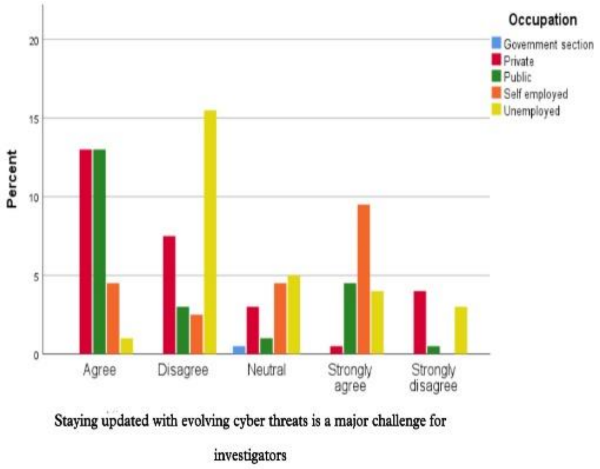
Legend: Figure 6 shows the distribution of gender with respect to the opinion that the Staying updated with evolving cyber threats is a major challenge for investigators.

FIGURE 7



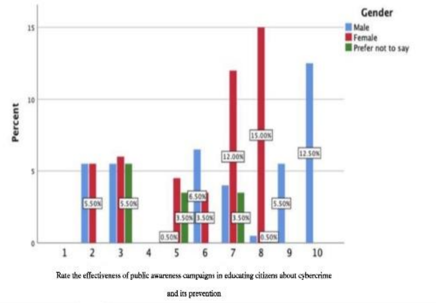
Legend: Figure 7 shows the distribution of age with respect to the cybercrime investigations affected by the lack of specialized cyber forensics experts.

FIGURE 8:



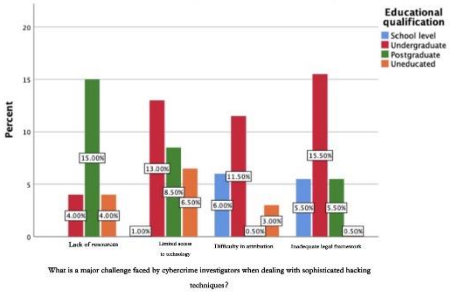
Legend: Figure 8 shows the distribution of occupation with respect to Staying updated with evolving cyber threats is a major challenge for investigators.

FIGURE 9:



Legend: Figure 9 shows the distribution of gender with respect to the effectiveness of public awareness campaigns in educating citizens about cybercrime and its prevention.

Figure 10:



Legend: Figure 10 shows the distribution of educational qualification with respect to the opinion that a major challenge faced by cybercrime investigators when dealing with sophisticated hacking techniques.

III. Results

From **figure 1,2,3 & 4** it is observed that independent variables of gender, age, educational qualification and occupation. From **figure 5** it is observed that self-employed people responded that difficulty in attribution is the major challenge faced by cybercrime investigators when dealing with sophisticated hacking techniques. From **figure 6** it is observed that females strongly agree that the Staying updated with evolving cyber threats is a major challenge for cybercrime investigators. From **Figure 7** it is observed that the age group between 21-30 responded to cybercrime investigations affected by the lack of specialized cyber forensics experts. From **figures 8** it is observed that unemployed people disagreed that Staying updated with evolving cyber threats is a major challenge for investigators and public sector and private sector people responded that cyber threats are a major challenge for investigators. From **figure 9** it is observed that females responded 8 in rating scale 1-10 on effectiveness of public awareness campaigns in educating citizens about cybercrime and its prevention. From **figure**

10 it is observed that undergraduate people responded that inadequate legal framework is the major challenge faced by cybercrime investigators when dealing with sophisticated hacking techniques and postgraduates responded that lack of resources is the major challenge faced by cybercrime investigators when dealing with sophisticated hacking techniques.

IV. Discussion

Figure 1 shows that male respondent 65.00% and female respondent 35.00%. **Figure 2** shows that the age group between 21-30 respondents is 20.00%. **Figure 3** shows the percentage of 65.00% of undergraduate respondents. **Figure 4** shows 50.00% of respondents are yet to be employed. **Figure 5** shows 23.76% of respondents that difficulty in attribution is the major challenge faced by cybercrime investigations when dealing with sophisticated hacking techniques. **Figure 6** shows 26.50% of females agreed that Staying updated with evolving cyber threats is a major challenge for cybercrime investigators, **figure 7** shows the highest response from 21-30 age group stated yes that cybercrime investigations affected by the lack of specialized cyber forensics experts, **figure 8** shows unemployed people disagreed that staying updating with evolving cyber threats is a major challenge for cybercrime investigators, **figure 9** shows 15.00% respondent 8 for rating scale 1-10 on the opinion that effectiveness of public awareness campaigns in educating citizens about cybercrime and its prevention. From **figure 10** it is observed that inadequate legal framework faced by cybercrime investigations when dealing with sophisticated hacking techniques.

V. Limitations

The Major limitation of the study is the sample frame. The restrictive area of sample size is yet another drawback of the research.Collection of data via online platform is limiting the researcher to collect data from the field.Since the data is collected on online platform wherein the respondent is not known, the original opinion of the respondent it is not found. The researcher could only come to an approximate conclusion of what the respondent is feeling to convey.

VI. Suggestions

The legal issue that is present in cyber investigations is the differences between jurisdictions and geographical methodologies. Cybercrime is a global issue and often spans multiple jurisdictions and geographical locations. This means that multiple countries can be affected, which means that law enforcement from these countries must collaborate to investigate the crime properly. The affected countries also often have their own methodologies, tools, and techniques they use in investigations.

VII. Conclusion

Automation and machine learning are advancing the field technology and cyber investigations are also being affected by these technologies. Automation is helping investigators speed up the process of collecting evidence, while machine learning is helping investigators identify and classify this evidence. Automation also presents challenges to this field in regard to legal assumptions and implications. Law enforcement agencies developed specialized cybercrime units and digital forensics techniques to gather evidence from digital devices. International cooperation became crucial due to the borderless nature of cybercrimes. Establishing dedicated cybercrime units within law enforcement agencies to focus on cybercrime investigations, equipped with specialized training and tools. Balancing the need for investigation with individual privacy rights remained a challenge, prompting the development of protocols for handling personal data. Educating the public about cyber threats, safe online practices, and how to report cybercrimes to law enforcement. Establishing mechanisms to provide support to victims of cybercrimes, including resources for recovery and assistance in dealing with the aftermath of attacks. Automation and machine learning provide potential areas of further research as these technologies become more sophisticated. Open-source intelligence techniques were also found to be underrepresented in the research field.

*****

VIII. References

1. Akhgar, Babak, and Ben Brewster. 2016. Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. Springer.
2. Alawida, Moatsum, Abiodun Esther Omolara, Oludare Isaac Abiodun, and Murad Al-Rajab. 2022. “A Deeper Look into Cybersecurity Issues in the Wake of Covid-19: A Survey.” Journal of King Saud University. Computer and Information Sciences 34 (10): 8176–8206.
3. Alfouzan, Faisal Abdulaziz, Kyounggon Kim, and Nouf M. Alzahrani. 2022. “An Efficient Framework for Securing the Smart City Communication Networks.” Sensors 22 (8). https://doi.org/10.3390/s22083053.
4. Aljuraid, Roaa, and Taghreed Justinia. 2022. “Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review.” Studies in Health Technology and Informatics 295 (June): 362–65.
5. Bandler, John, and Antonia Merzon. 2020. Cybercrime Investigations: A Comprehensive Resource for Everyone. CRC Press.
6. Bist, Adv Shruti. 2020. CYBER CRIME AGAINST WOMEN IN INDIA – INVESTIGATIVE AND LEGISLATIVE CHALLENGES. Blue Rose Publishers.
7. Harisha, A., Amarnath Mishra, and Chandra Singh. 2023. Advancements in Cybercrime Investigation and Digital Forensics. CRC Press.
8. Harisha, A., Amarnath Mishra (forensic scientist), and Chandra Singh (Professor of engineering). 2023. Advancements in Cybercrime Investigation and Digital Forensics.
9. Hussain, Abrar, Kifayat Ullah, Tapan Senapati, and Sarbast Moslem. 2023. “Complex Spherical Fuzzy Aczel Alsina Aggregation Operators and Their Application in Assessment of Electric Cars.” Heliyon 9 (7): e18100.
10. International Telecommunication Union. 2017. Understanding Cybercrime: Phenomena, Challenges and Legal Response. United Nations.
11. Lopez, Juan, Jr, Kalyan Perumalla, and Ambareen Siraj. 2021. 16th International Conference on Cyber Warfare and Security. Academic Conferences Limited.
12. Mackey, Tim K., and Bryan A. Liang. 2013. “Pharmaceutical Digital Marketing and Governance: Illicit Actors and Challenges to Global Patient Safety and Public Health.” Globalization and Health 9 (October): 45.

13. Natarajan, Mangai. 2019. International and Transnational Crime and Justice. Cambridge University Press.

14. Payne, K., K. L. Maras, A. J. Russell, M. J. Brosnan, and R. Mills. 2020. “Self-Reported Motivations for Engaging or Declining to Engage in Cyber-Dependent Offending and the Role of Autistic Traits.” Research in Developmental Disabilities 104 (September): 103681.

15. Reyes, Anthony, Richard Brittson, Kevin O’Shea, and James Steele. 2011. Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors. Elsevier.

16. Satpathy, Suneeta, and Sachi Nandan Mohanty. 2020. Big Data Analytics and Computing for Digital Forensic Investigations. CRC Press.

17. Shinder, Debra Littlejohn, and Michael Cross. 2008. Scene of the Cybercrime. Elsevier.

18. Slade, Robert. 2004. Software Forensics: Collecting Evidence from the Scene of a Digital Crime. McGraw Hill Professional.

19. U S Department of Justice. 2014. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. CreateSpace.

20. Wang, Shun-Yung Kevin, Ming-Li Hsieh, Charles Kuang-Ming Chang, Pin-Syuan Jiang, and Douglas J. Dallier. 2021. “Collaboration between Law Enforcement Agencies in Combating Cybercrime: Implications of a Taiwanese Case Study about ATM Hacking.” International Journal of Offender Therapy and Comparative Criminology 65 (4):

*****