"Current Obstacles and the Prospective of Cyber Attack Investigation"

Rekha, Dept. of Law, Research Scholar, SunRise University, Alwar (Rajasthan)
Dr. Vinod Kumar Sharma (Law), Professor (Dept. of Law), SunRise University, Alwar (Rajasthan)

ABSTRACT

Because technology is so integral to modern life, it is also increasingly used by criminals. Criminals are adept at using cutting-edge technologies, so forensics teams must keep up. Many people have been and will be victims of cyber Attack, so it's crucial that investigators are familiar with the latest techniques used in cyber investigations. Investigating computer crimes can be broken down into two broad categories: digital forensics and open-source intelligence. More than just the investigators themselves are feeling the effects of cyber investigations. Based on the data collected and the efficiency of the available tools and methods, they must choose the appropriate instrumentation. Investigatory tools include anything from software to hardware, while investigatory methods refer to the steps taken to make use of those tools. This study analyses and contrasts the most popular investigation techniques to ascertain the evidence they yield and which ones are most reliable. In order to achieve this goal, the survey compares and analyses the tools used in mobile digital forensic and open-source intelligence investigations, establishing a standard by which to judge their efficacy. We discovered that no one piece of software or set of procedures exists to compile all the data that investigators need. In order to maximise the effectiveness of many of the tools, they must be used in tandem. Of course, some instruments are more practical than others. Logical extraction and hex dumps are the two most reliable and least risky methods used in mobile digital forensics. When it comes to open-source intelligence tools, natural language processing far outstrips the competition.

Keywords: Intelligence Tools, cyber Attack, Digital Forensic, Criminals, Open-Source Intelligence

INTRODUCTION

In recent years, the frequency and severity of cyber-attacks have increased dramatically, posing a significant threat to organizations and individuals worldwide. As a result, cyber-attack investigation has become a critical area of concern for cybersecurity professionals and law enforcement agencies.

One of the biggest obstacles in cyber-attack investigation is the rapid evolution of technology and the corresponding changes in attack methodologies. Attackers are constantly finding new and innovative ways to bypass security measures and exploit vulnerabilities, making it challenging for investigators to keep up with the latest threats.

Moreover, cyber-attacks are often highly sophisticated, with attackers leaving little to no trace of their actions. This makes it difficult for investigators to determine the source of the attack and identify the perpetrators. Cyber-attacks can also occur from anywhere in the world, adding a layer of complexity to the investigation process as investigators must coordinate with international authorities and navigate various legal frameworks.

However, despite these challenges, there are several prospects for cyber-attack investigation. Advancements in technology, such as artificial intelligence and

Machine learning, are making it easier to identify and respond to cyber threats in real-time. Additionally, the growing demand for cybersecurity professionals has led to an increase in the number of trained investigators available to tackle these issues. Moreover, collaboration and information sharing between organizations and authorities have also improved in recent years. Many organizations have established partnerships with law enforcement agencies and other stakeholders to share threat intelligence and develop proactive approaches to cyber security.

In conclusion, while cyber-attack investigation remains a challenging and rapidly evolving field, advances in technology, increased collaboration, and the growing pool of trained cybersecurity professionals offer promising prospects for the future of cyber security.

REVIEW OF RELATED LITERATURE

Year 2019: Author: Yavuz, G., & Bayram, İ.

Title: Cybercrime investigation methods and challenges: A review of literature

This article presents a comprehensive review of the literature on the methods and challenges of cybercrime investigation. It covers the different types of cybercrime, the methods and tools used in cybercrime investigation, and the challenges faced by investigators.

Author: Khan, M., & Shaikh, F.

Title: Digital forensics investigation framework for cloud security breaches

This paper proposes a digital forensics investigation framework for cloud security breaches. The framework consists of four phases: evidence collection, evidence analysis, evidence presentation, and post-incident activity.

Year 2020: Author: Baggili, I.

Title: Cyber-attacks investigation: An overview of current practices and emerging issues. This article provides an overview of current practices in cyber-attacks investigation, including the use of digital forensics tools, the legal and ethical issues involved in cyber-attacks investigations, and the challenges posed by emerging technologies.

Author: Li, J., Li, Y., & Li, S.

Title: A comprehensive survey of cybercrime investigations

This paper presents a comprehensive survey of cyber-attacks investigations, including the different types of cyber-attacks, the legal framework for cybercrime investigations, and the techniques and tools used in cyber-attacks investigations. It also discusses the challenges and future directions of cyber-attacks investigations.

Year 2018: Author: Alzahrani, A. I., Alsufyani, N. A., & Alqurashi, T. S.

Title: The digital forensics challenges in investigating cyber attacks

This paper discusses the challenges faced by digital forensic investigators in investigating cyber-attacks, including the volume and variety of data, the rapid evolution of technology, and the complexity of digital networks.

Author: Kumar, R., & Kumar, A.

Title: A systematic review of digital forensics investigation frameworks for cybercrime

This paper presents a systematic review of digital forensics investigation frameworks for cybercrime. The review covers 22 frameworks and identifies the common features and components of these frameworks. It also highlights the gaps in the existing frameworks and suggests future research directions.

STATEMENT OF THE PROBLEM

The problem of Cyber Attack Investigation: Landscape, Challenges, and Future Research Directions is that the field of cybercrime investigation is rapidly evolving and becoming increasingly complex. Law enforcement agencies and other stakeholders face numerous challenges in investigating and responding to cybercrimes, including the lack of standardization in investigation methodologies, the rapid pace of technological change, and the increasing sophistication of cybercriminals.

Additionally, the legal and ethical issues surrounding cyber Attack investigation can be complex, with questions around privacy, data protection, and human rights frequently arising. The lack of cooperation and coordination between different stakeholders can also hinder effective investigation and response to cyber Attack.

To address these challenges, there is a need for research that can help to identify the most pressing issues facing cybercrime investigation, and provide recommendations for improving investigation methodologies, enhancing collaboration and communication between stakeholders, and ensuring that investigations are conducted in a manner that is ethical and legally compliant. Without such research, law enforcement agencies and other stakeholders may struggle to keep pace with the evolving nature of cyber Attack and may be unable to effectively investigate and respond to this growing threat.

NEED FOR THE STUDY

Understanding the Current State of Cyber Attack Investigation: As cybercrime becomes more prevalent, it is important to have a clear understanding of the current landscape of cyber Attack investigation. This study can help to identify the current challenges and limitations of the current investigation methodologies, and to identify areas where improvements are needed.

Addressing the Challenges of Cyber Attack Investigation: Cybercrime investigation can be complex and challenging, and there is a need to develop new approaches and tools to improve the effectiveness and efficiency of digital forensics. This study can help to identify the most pressing challenges and provide recommendations for addressing these challenges.

Staying Ahead of Emerging Threats: cyber Attack is constantly evolving, and new threats and challenges are emerging all the time. This study can help to identify emerging trends and threats in cybercrime, and to provide insights into new forms of cybercrime that may be on the horizon.

DIGITAL FORENSICS

Mobile Forensics

The prevalence of mobile devices has increased as technology has advanced. This means that everybody working in the sector should be aware of the importance of mobile forensics as a component of investigations. Because of the differences in "technology, software, power consumption, and total mobility," mobile forensics is different from all other types of forensics. Also, it is assumed that mobile devices include personal information that may be crucial to an investigation.

Phases of an Investigation

Mobile forensics investigations include four stages: preservation, acquisition, inspection, analysis, and reporting. Figure 1 illustrates these stages.

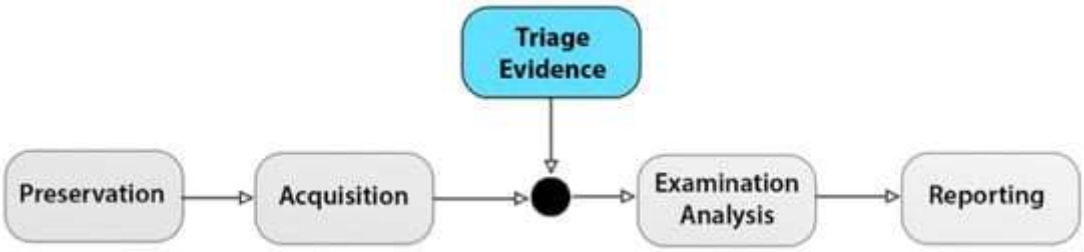

Fig. 1. Mobile forensic investigative phases

Investigators seize mobile devices during the preservation phase and follow them to make sure the data on them hasn't been altered. The data on the mobile device is copied to another device during the acquisition phase in preparation for analysis during the examination analysis phase. The reporting phase is the last step, where all the data the investigators uncovered during the examination and analysis phase is recorded. To maintain the integrity of any investigation using mobile devices, each of these steps must be correctly followed.

Extraction of Data

In mobile forensics, there are standard ways of gathering that are also known as data extraction. During investigations, data from mobile devices must be extracted. Data extraction can be done at five different levels: manual, logical, hex dumps, chip-offs, and micro readings. Each of these options enables researchers to collect various data from various regions of the gadget with varied levels of complexity. Based on the criteria listed in Section 1, Table 1 compares various techniques.

The least challenging extractions are those that require manual labour since they involve regular device interaction, like touching a touch screen, from the investigator.

Table 1. Comparison of the methods of mobile data extraction

The risk with this strategy is that the data on the device may be accidently damaged or altered by the investigators. This strategy should not be used since it exposes the evidence to the possibility of being destroyed or altered, which may render the evidence inadmissible in the case if it got to court.

Investigators will use technology like Bluetooth or a USB to logically extract data from the gadget and transfer it to an external workstation. Moreover, this approach runs the danger of unintentionally changing data. Because it enables investigators to examine data from a different device, logical extraction is a suitable technique to start with throughout an investigation. It is important to keep in mind that logical extraction may require a pin or password to access the data, which could result in hassles or legal issues.

Table 1 demonstrates that although manual extraction is simple, it is not advised due to the potential danger to the accuracy of the data. Hex dumps and logical extraction are the best techniques. They examine data from several sources, providing investigators with a way to compile new kinds of evidence that the other technique is unable to access. Hex dumps and logical extraction have medium or low complexity, which makes them easier to use and faster. Due to the utilisation of a separate workstation for data manipulation, both of these solutions represent a low risk to data integrity.

Forensics of networks

Analyzing data from a host or a network as a whole is the practise of network forensics.

Logs or traffic captures can provide the forensic information.

Investigators may find relevant information in three of the TCP/IP Model's levels. These layers are the network, transport, and application layers. The only layer not covered by this is the network interface layer, which is responsible for managing a network's physical connections and ethernet transmissions. Using the logs that hosts collect, forensic data can be collected from the application layer. This information, which can be crucial in an inquiry, can include timestamps or details on unsuccessful logon attempts. Firewalls are categorised as being at the transport and network layers. If firewalls are set up correctly, they can store logs of network traffic that has been dropped. This can provide information to investigators about potentially harmful traffic that the firewall has seen. Figure 2 depicts the relationship between the layers and the data that may be gathered by investigators by displaying the traffic flow across the network model and the devices it affects.

The volume of traffic and log data that can be present during an investigation is the biggest problem that network forensics investigators must deal with. Although it is theoretically conceivable, it is not practical for investigators to gather and examine each and every packet in a network capture. The amount of data will not only need too much time to examine, but it may also result in high prices that are frequently unaffordable.

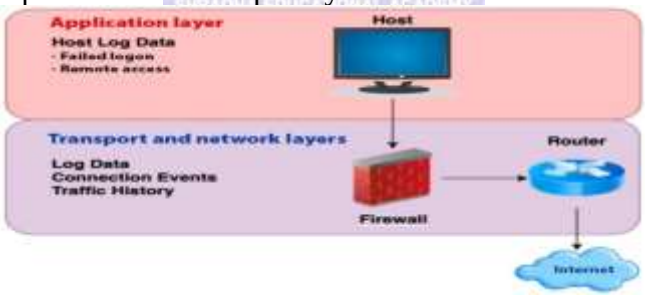

Fig.2. Evidence gathered from network layers.

The expanding Internet of Things trend presents investigators with another difficulty when using network forensics (IoT). Since these devices are network dependent, there are more end hosts on networks, which increases the amount of logs and traffic they generate. In addition to making log and capture size challenges more difficult, this makes establishing the scope of investigations more difficult.

INVESTIGATING ONLINE

The process of obtaining, organising, and using information that can be found online is known as an online inquiry. Any person, including members of law enforcement or security personnel, may carry out these. Open-source intelligence is the primary technique for obtaining information in online investigations (OSINT). The information acquired using other methods that are mentioned in the sections below is combined and used in this manner. Relationships, names, or events that are pertinent to the cyber investigation are revealed by the information obtained for this kind of research.

The Information Sources

Investigators conduct internet investigations using a variety of information sources. The open, deep, and black web are the three primary sources. Each of these sites has information that investigators might use. The web's layers are depicted in Figure 4 along with an example of how the information overlaps. It is crucial to remember that the dark web is a part of the deep web and not a stand-alone information source.

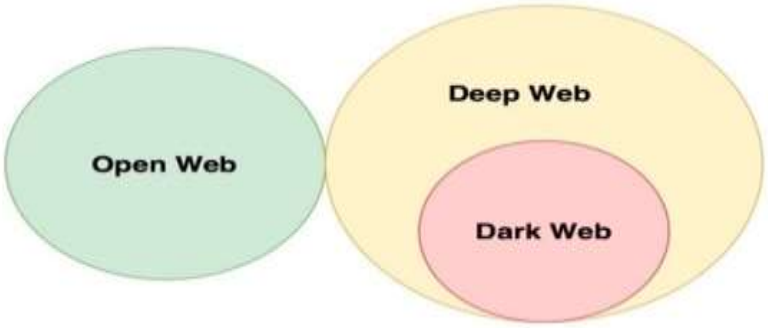

Fig. 3. Layers of the web

Open Web: The open web is the part of the Internet that is open to all users and indexed by normal search engines, such as Google.

Deep Web: The deep web is the part of the Internet that is not indexed by search engines. This is the area of the Internet is not necessarily illegal, but it can be.

Dark Web: The dark web is the subset of the deep web where illegal activity occurs. It can be accessed using specialized software, such as Tor, that allows users to access servers, forums, and blogs that would be otherwise unavailable to users.

Specialized Sources of Information

Social Media, Cryptocurrency Flow, *Data Mining*

DATA MINING

Data mining is the practice of searching the web for information, organizing this information into a report, and using it in an investigation

The techniques used for data mining must adhere to a number of requirements, as stated in Section 1. They must, first and foremost, be more effective for use by investigators. The first criterion, that they must be quicker than manual searching, is satisfied by all four of the techniques shown in Table 2. Table 2 compares them based on the sources of the methods' data, the number of cases they are relevant to, and the number of distinct techniques discovered.

Table 2. Comparison of data mining methods.

Even though there is only one source of information, natural language processing is the most widely employed technique, with 85 techniques and 18 distinct case types at investigators' disposal. This results mostly from the subcategories of this strategy, which can be employed on the same kinds of cases yet produce various kinds of information that investigators can use. Authorship profiling, for instance, can be used to identify the author's characteristics, such as militancy, which informs investigators as to whether the author poses a threat, in situations of terrorism and extremism. The capacity to recognise the feelings that a text's author is experiencing and determine whether or not they are a member of the criminal organisation allows investigators to employ sentiment analysis in cases of terrorism and extremism. The number of applications for natural language processing grows since two subcategories might be utilised on the same situation.

Automatic Language Recognition

The interaction between human languages and computers is known as natural language processing. It only examines text-based information. Natural language processing is divided into four key subfields: authorship analysis, author profiling, sentiment analysis, and text classification. Identification of the author of a certain text is done through the method of authorship analysis. Author profiling is the practise of examining a text to identify the writing style and traits of the author. Sentiment analysis is the process of figuring out what drives a piece of writing. Lastly, text classification involves figuring out where a piece of text fits into several pre-established categories. Out of the techniques examined in this survey, natural language processing is by far the most popular. It just has one information source, which is text, however there are numerous ways it can be used in situations.

Cases involving terrorism, extremism, and harassment can all benefit from sentiment analysis. This technique is used to identify emotion, the direction of that emotion, and the strength of that emotion in both of these case categories. This is accomplished by classifying the text's lexicon and figuring out the writing style.

In cases of crimes against children, text classification can be used. Investigators are able to identify and then categorise the main traits of child abuse media. They will then be able to categorise material based on these definitions. Commonly used keywords are one of the most frequent ways to recognise and define certain media kinds.

Study of Social Networks

The use of technology to study the network between criminal groups and platforms is known as social network analysis. This technique makes use of tools to extract data from an online source concerning a criminal or terrorist group's links. Social network analysis is one of the most useful methods for open-source intelligence investigations even if it simply uses text as the information source.

In order to analyse social networks, investigators might employ a variety of tools and techniques. Scraping information from blog posts and forums that are known to be used for illegal behaviour is one of the most effective techniques. Researchers also use data mining, which involves extracting information from graphical sources like the social graph of YouTube. The relationships between extremist videos and communities are seen in this graph.

Using NLP techniques, such as emotion detection, might be crucial when conducting social network analysis. This can assist investigators in establishing the connection between people and groups by letting them know who is connected to the group and what its actions are.

Extraction of Information

Automatically gathering and organising information is known as information extraction. Using the previously discussed techniques, this compiles the data that was taken from the web into a report. Because it collects information and produces a report, information extraction is intended to reduce the amount of time required by investigators. URLs, technical sophistication, language, and webpages are the four key sources used to get this data.

This strategy requires tools that can take into account various interfaces, such as online databases. Web crawlers, which look for any page connected to a site and report on the popular subjects there, are one of the frequently utilised tools for this technique. Investigators will be able to find out about prospective new targets and criminal activities thanks to this. URLs, degrees of technical sophistication, language, and webpages are the four basic categories of data that information extraction analyses. These sources can provide data on the connections and skills between people and groups.

In situations involving terrorism and extremism, information extraction is frequently used. Investigators frequently get their information from forums and websites related to these activities. The forums and webpages can be scraped by investigators to discover the common themes among these groupings.

Machine Learning

Using online photos and videos to learn more about a subject or a crime is a process known as computer vision. This applies to text, audio, and images all found in a video. This

technique can offer data that can be used in investigations, such as the names and connections of users online. The three primary sources of data for computer vision are audio, video, and pictures.The application of numerous distinct methodologies is possible in the field of computer vision. Identification of people using various information sources is one of the most popular applications of computer vision. There are numerous techniques investigators might use to identify people. Using facial recognition software on avatars created from photographs is one way to achieve this. This method is found to be accurate, but only when the user creates the avatar using their own photo.

Computer vision is frequently used for phishing attacks and spam screening. To get past spam filters, many spam emails disguise their messages as graphics. In order to deceive the recipient into believing the email is authentic, phishing emails often largely rely on pictures.

CURRENT OBSTACLES OF CYBER ATTACK INVESTIGATION

Rapidly changing attack methods and techniques: Cyber attackers are constantly evolving their methods and techniques, which can make it difficult for investigators to keep up with the latest attack vectors and vulnerabilities.

Limited technical expertise: Conducting a thorough cyber-attack investigation requires technical expertise in areas such as network forensics, malware analysis, and digital evidence collection. Many law enforcement agencies and organizations lack the necessary technical expertise to conduct such investigations effectively.

Insufficient funding and resources: Cyber-attack investigations can be time-consuming and resource-intensive. Many organizations lack the funding and resources to conduct comprehensive investigations or to invest in the latest cybersecurity technologies.

Complexity of the attack surface: With the proliferation of Internet of Things (IoT) devices, cloud services, and other technologies, the attack surface has become increasingly complex. This can make it challenging to identify and mitigate vulnerabilities, or to attribute attacks to a specific actor.

Jurisdictional challenges: Cyber-attacks can originate from anywhere in the world, making it difficult to identify the responsible party or to coordinate investigations across different jurisdictions.

Privacy and data protection concerns: Cyber-attack investigations often involve the collection and processing of sensitive personal data, which can raise privacy and data protection concerns. Investigators must ensure that they are complying with relevant data protection laws and regulations.

Lack of cooperation and information sharing: Effective cyber-attack investigations often require cooperation and information sharing between multiple organizations, including law enforcement agencies, security vendors, and victim organizations. However, there can be challenges in obtaining and sharing information due to legal, policy, and other barriers.

Time-sensitive nature of investigations: In many cases, cyber-attack investigations must be conducted quickly to prevent further damage or to identify the responsible party. This can place pressure on investigators to make quick decisions and can make it difficult to conduct a thorough investigation.

Rapidly evolving threat landscape: The threat landscape is constantly evolving, with new types of attacks and vulnerabilities emerging all the time. This can make it challenging for investigators to keep up with the latest threats and to develop effective countermeasures.

Complexity of digital evidence: Digital evidence can be complex and difficult to collect, analyze, and present in court. Investigators must ensure that they are collecting and preserving evidence in a forensically sound manner and that the evidence is admissible in court. This can require specialized technical expertise and tools.

OPEN ISSUES AND RESEARCH DIRECTIONS

Based on our research, the open issues can be organized into three categories:

Technical Issues

Any issue relating to the technology, tools, or approach employed in the field of cyber investigations is characterised as a technical issue. There are many different technological problems that can arise in this area. One is the approach to using open-source intelligence's

tools and methods. This is due to the fact that each instrument offers information in a unique way, and there is no established "best practise" methodology that investigators can apply. Although investigators have access to a variety of helpful tools, there isn't much study on how to use them. Making sure an entity's identity is accurate and using the right framework to do this are two more technical issues.

Legal Issues

Any issue that investigators might have about the law or presenting the investigation in court is characterised as a legal issue. The topic of upholding and demonstrating the integrity of digital evidence is one concern in this category. Investigators will need to present the evidence and demonstrate that it was gathered legally once the forensic evidence has been gathered and the case may potentially go to court. Inability to do so could make the evidence inadmissible.

Ethical Issues

Every moral or ethical conundrum that investigators can encounter during a cyber investigation is classed as an ethical issue. For instance, one of the methods used by investigators in open-source intelligence investigations is profiling based on the data discovered about a person or group online. A procedure known as criminal profiling is one "in which the nature of a crime is exploited to create assumptions about the personality and other traits of the likely culprit."

Open Issues' Directions for Research

These unresolved problems may inspire worthwhile research initiatives. One of these is how to more effectively use open-source intelligence technology as a whole programme, rather than just as separate tools. The instruments mentioned do not give investigators information that fully defines the situation.

Research on bias handling and fair treatment in open-source intelligence investigations may also result from this poll. It is crucial that these investigations may be conducted appropriately and fairly because they play a significant role in the whole investigating process. If there are no prejudices or presumptions ingrained in the techniques or resources an investigator uses, this can also aid them in discovering the truth more quickly.Finally, research on the aforementioned legal difficulties can aid security professionals in doing a better job of their jobs. It is crucial to comprehend how laws impact the gathering and preservation of evidence since criminal investigations may lead to court proceedings. Even though technical personnel may not have conducted this study, it is crucial for them to comprehend the non-technical legal challenges.

FUTURE SCOPE OF THE STUDY

Future directions for the research could focus on:

- The improvement of the efficacy and efficiency of digital forensics necessitates the creation of new tools and techniques for the investigation of cybercrime.
- By analysing case studies of similar cybercrimes, we can determine which investigation methods work best and where improvements can be made.
- Cybercrimes involving advanced technologies like social media, the cloud, and IoT require novel data sources and analysis methods, which are currently under investigation (IoT).
- Ethical, legal, and social implications of cybercrime investigation are examined with a focus on sensitive topics like personal information protection and human rights.
- The role of law enforcement in preventing and investigating cybercrime, as well as an analysis of the efficacy of existing cybercrime legislation.
- New trends and types of cybercrime are being identified and analysed, including those associated with AI, cryptocurrencies, and deep fakes.
- The creation of innovative methods for investigating and responding to cybercrime requires the joint efforts of experts from the academic and law enforcement communities, as well as the private sector.
- Law enforcement agencies and other relevant stakeholders need specialised cybercrime investigation training, so new courses are being developed.

Future research in these areas may shed light on developing problems and trends in the ever-evolving field of cybercrime investigation, which is currently fraught with difficulties.

CONCLUSIONS

As criminal investigations try to keep up with increasingly sophisticated threat actors, technology has become increasingly important. Investigators have access to a wide variety of resources and techniques that can help them do their jobs more effectively. There isn't a single one of these gadgets that can do everything detectives need. Therefore, it is important for investigators to learn about various tools, their purposes, and the data they can yield.

Even though digital forensics has been around for a while, the discipline is constantly developing. Even as new techniques are developed, the four primary areas of host, mobile, network, and cloud forensics remain essential to digital investigations. When it comes to mobile forensics, there is more than one way to get at the data you need. Logical extraction and hex dumps are the most efficient approaches. Since more and more services are moving to the cloud, cloud forensics has emerged as a promising new field in digital forensics.

Even though online and open-source intelligence investigations have been around for a while, investigators are always finding new ways to improve upon them. Online investigations can use a variety of these techniques to learn as much as possible about potential danger actors. There is some information to be gleaned from each of these approaches, but collectively they fall short of what is required to conduct a thorough investigation. While there are many tools at an investigator's disposal, natural language processing (NLP) stands out as the one with the widest range of potential uses. This approach can be used for a wide variety of investigations and provides investigators with multiple data points to work with.

Cyber investigations are being impacted by the rise of automation and machine learning in the field. In addition to speeding up the evidence-gathering process, automation and machine learning are also aiding in the identification and categorization of the evidence gathered. The legal assumptions and implications of automation also pose difficulties in this area .

The potential for new discoveries in this area is high. As AI and ML continue to improve, new research questions are opening up. It was also discovered that open-source intelligence techniques were under-researched, creating a new avenue for study.

REFERENCES

1. Baggili, I. (2020). Cybercrime investigation: An overview of current practices and emerging issues. Digital Investigation, 31, S56-S62.
2. Li, J., Li, Y., & Li, S. (2020). A comprehensive survey of cybercrime investigations. Digital Investigation, 31, S43-S49.
3. Yavuz, G., & Bayram, İ. S. (2019). Cybercrime investigation methods and challenges: A review of literature. Journal of Financial Crime, 26(1), 186-200.
4. Khan, M., & Shaikh, F. (2019). Digital forensics investigation framework for cloud security breaches. Journal of Cloud Computing, 8(1), 1-21.
5. Alzahrani, A. I., Alsufyani, N. A., & Alqurashi, T. S. (2018). The digital forensics challenges in investigating cybercrimes. Journal of Digital Forensics, Security and Law, 16(1), 11-32.
6. Kumar, R., & Kumar, A. (2018). A systematic review of digital forensics investigation frameworks for cybercrime. International Journal of Cyber-Security and Digital Forensics, 10(2), 109-124.
7. Ghosh, D., Dube, A., & Saini, S. (2019). Cyber crime investigation: An overview. International Journal of Innovative Technology and Exploring Engineering, 8(10S), 92-95.
8. Mousavi, S. S., & Saghafi, F. (2020). Cybercrime investigation using fuzzy decision-making approach. Journal of Risk and Financial Management, 13(10), 222.
9. Shabut, A. M., Kyriakakis, C., & Akhgar, B. (2019). Investigating cybercrime using big data analytics: A review of challenges, methods, and tools. Journal of Big Data, 6(1), 1-24.
10. Bertino, E., & Islam, N. (2019). Cybercrime and digital forensics: An overview. IEEE Security & Privacy, 17(1), 13-20.

11. Fattah, S. A., & Huang, K. (2019). Investigating cybercrime: A systematic review of the literature. Digital Investigation, 28, 1-14.
12. Taqvi, S. H., Qaisar, S., & Hamid, M. A. (2019). Digital forensics challenges in cloud environment. Journal of Telecommunication, Electronic and Computer Engineering, 11(2-6), 141-146.
13. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.
14. Kwon, J., & Goel, S. (2017). Cybercrime investigations: Challenges and issues. In Information Science and Applications (pp. 1195-1202). Springer.
15. Zawoad, S., Hasan, R., & Hasan, M. Z. (2020). Digital forensics and cybercrime investigation: A review of literature. Journal of Digital Forensics, Security and Law, 15(3), 41-56.