A PIONEERING APPROACH TO FORENSIC INSIGHTS: UTILIZATION AI FOR CYBERSECURITY INCIDENT INVESTIGATIONS

VENKATESWARANAIDU KOLLURI

Software Engineer, Department of Information Technology

ABSTRACT—This paper provides an overview on the novel strategies for strengthening the investigations of cybersecurity attacks through targeted usage of Artificial Intelligence (AI). Conventional forensic analysis techniques are still falling behind on the fast-growing scale and frequency of cyberattacks. As a matter of fact, they are not capable of reacting promptly and effectively to identify, isolate, and fingerprint cybercrime [1]. The capability to tap into AI capabilities, specifically machine learning, natural language processing, and anomaly detection, helps to intensify as well as facilitate forensic investigation. Such a transformative approach allows us to minimize response time, gain deeper insights, and develop more accurate threat analysis to arm cybersecurity professionals for fighting the ever-developing cyber-crime landscape. AI-driven forensic analysis speeds up analyses of big data records allowing to detect hidden steps that can be ignored by human analysts. AI-based automated systems can aid cyber security officials to detect real-time suspicious alerts and data breaches automatically which they then can dedicate to strategic threat mitigation efforts and critical decisions [1]. Furthermore, the applications of AI in cybersecurity incident investigations aid in proactive threat hunting and determination of the threat's origin, hence, and allow organizations to thwart cyber threats before they progress into data breaches [1,2]. AI-driven systems would be able to persistently inventory network traffic, system logs and user activity to identify any security anomaly or antisocial behavior that might prove to be a potential threat, thus enabling a preventive approach to preventing the loss of information assets. On the other hand, AI algorithms can also help in the attribution of cyber-attacks through digital fingerprints, code similarities as well as other indicators of malignant behavior, giving significant information.

Keywords— Cyber-attacks, Artificial Intelligence, Cybersecurity, Forensic Investigation, Incident Response, Automated Systems, forensic investigation, Machine Learning

I. INTRODUCTION

In an era of massive digital connectivity, cybersecurity has become a top priority for the security of the data, infrastructure and systems against cyber attacks. With the increasing adoption of digital technologies by organizations to run their business, the impacts of cybercrime have gone deeper to imply losses, brand damage, and security issues in the U.S [1]. Cybercriminals continue discovering new techniques to hack into the systems while cybersecurity measures are strengthened. Such acts of hackers have even led to the further increase in sophistication and frequency. The need for innovative approaches to cybersecurity investigations hence has become a necessity.

Outdated and conventional methods of forensic analysis, while being important in their own regard, tend to be overwhelmed with the dynamic nature of the present day threat landscape. Manual investigation procedures are labor-intensive, time-consuming, and they are prone to human error which impedes fast and appropriate organizations response to cyber security incidents in real time [3]. In addition, the amount and complexity of data created in these digital environments enlarge the gap between rational thinking and high-tech capabilities of human analysts, which can lead to delayed responses and/or inability to attribute cybers threats. Such technology is urgently required to tackle the problem of rising cybercrimes, as forensic systems develop at the pace of constantly changing cyber threats.

AI has nowadays manifested to become a cybersecurity agent carrying the options of revolutionizing today's practice of forensic investigations. Utilizing AI innovations such as machine learning, natural language processing, and anomaly detection, organizations can improve the efficiency, accuracy, and scalability of incident investigations during cybersecurity events [4,5]. Innovations in AI-based forensic analysis give organizations the tools to perform large-scale analysis of data in a very short time, which helps to uncover suspect patterns and anomalies, as well as trigger alarms to the things that traditional methods may not be able to identify. Moreover, AI algorithms are increasingly able to streamline the process of routine procedures such as detecting anomalies in real time and provide an opportunity for cybersecurity professionals to prioritize their decision-making and strategic management skills rather than operational tasks.

Not only does it provide the organizations with the ability to conduct cybersecurity incident investigations through AI, but it also introduces the intelligence-driven approach to threat detection and response. AI-automated systems for online security can always track digital spaces looking for newly emerging threats and weaknesses that can grow into various security breaches. By turning on artificial intelligence capacities like threat intelligence attributes, businesses are boosting their level of intelligence and sensitization, and therefore they are able to preemptively fight cyber threats, hence no big impact from cyber attacks [6]. This evolution of cybersecurity is a significant paradigm shift for organizations to defend themselves from cyber threats in the fast-paced and interconnected nature of the digital world.

II. RESEARCH PROBLEM

The main research problem addressed in this paper revolves on the integrated AI technologies in cybersecurity incident investigation process to achieve higher accuracy as well as their results usability features within reasonable time constraints. Conventional forensic analysis methods that are used often are not so effective in the task of identifying, mitigating, and attributing cyber threats because they are manual and have high labor content. To tackle this problem, the paper will explore how AI-aligned applications can accelerate and enhance FTL processes to make organizations cyber-responding much more rapidly [7]. However, the problem is wider in that it entails exploring the consequences of AI-enabled cyber incidence inquiry on the robustness of the organization, threat mitigation strategies, and the resource allocation as well. With organization’s functioning depended more on digital technologies to perform the operations, the speed of threatening

detection, analyzing, and response has become of the greatest importance. AI technologies such as machine learning, natural language processing, and anomaly detection can empower organizations to achieve much more effective cybersecurity protection through increasing their cyber defense posture and resilience.

III. LITERATURE REVIEW

A. Traditional Forensic Analysis Methods

Traditional forensic analysis methods capture the basics of cybersecurity incident investigations, including a bundle of techniques and procedures which help to locate, reduce and attribute cyber threats. Disk imaging, which is one of the basic and essential techniques of digital forensics, makes a bit-by-bit copy of a digital storage device to preserve its contents and then to examine the items during the digital forensics review [8,9]. This approach enables the team to work with the disk image in a detached way, thus being able to preserve all the original data and subsequently find any malicious files, artifacts, and activities. Another fundamental forensic analysis technique is the RAM analysis that involves the extraction and analysis of volatile memory (RAM) from the living system or memory dumps. Through analyzing memory contents investigators may reveal operating sessions, network contacts and evidence of malware as proof of active hazardous activity and signs of compromise. Besides, memorization will enable us to understand the adversary methods, tactics, procedures (TTPs) which will lead to deducting good ways on how to mitigate or counter only [9].

The log file's analysis is a key issue in forensic analysis, as system and application logs are processed to reconstruct the event sequence preceding the cyber incident and after it. With the help of the Log files, analyzing the investigators may determine the instances in which the suspicious activities, intrusion attempts, and information security breaches occur for the organizations allowing to impact the issue to the scale and influence. Additionally, log file analysis can support the attribution of cyber attacks by using it in the tracing of the origin and course of malicious activities across the network [9].

B. Role of Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) has rapidly become the core of cybersecurity incident investigation tools, which increase the accuracy of incident recognition, identification, and responsiveness. This can be accomplished through AI tools such as machine learning, natural language processing, and anomaly detection that will be advantageous in comparison with the traditional forensic analysis techniques that have their limitations. Machine learning algorithms, especially, have paraded the possibility for an automatic detection of patterns, anomalies and indicators of compromise in the huge volumes of data. Thus, the organizations can pinpoint the emerging threats and vulnerabilities on time.

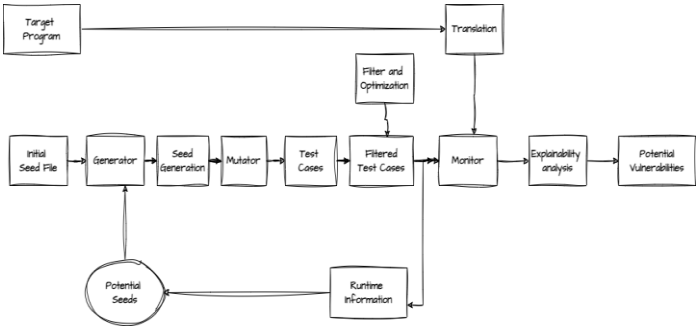

Fig. 1 Vulnerability detection using AI-driven tools

Artificial intelligence and data analyses through Natural language processing (NLP) techniques are empowering to imply threat intelligence feeds, incident reports, and dark web forums. The NLP algorithms are capable of doing an analysis of textual data to find out elements like threat actors, TTPs, tactics and procedures that facilitate sharing and collaboration among organizations [10]. Cybersecurity experts can benefit greatly from NLP as it makes analytical work easier and provides more accurate information to ensure proper threat mitigation as well as response decisions. The AI technologies in this perspective are outstanding in the area of anomaly detection, highlighting deviating behaviors and warning of any suspicious activity in record time [11]. AI-based anomaly detection tools enabled to work with network traffic, system logs, and user's behavior can detect statistics that deviate from norm in pursuit to prevent security problems. AI-empowered systems can flag signs of malicious activity which cyber professionals are informed to act appropriately before the worse impact would be brought by the security breaches.

C. Machine Learning Techniques in Forensic Analysis

The advancements in machine learning have undoubtedly revolutionized the field of forensic analysis in cybersecurity incident investigations, giving this area a new quality of tools allowing investigation officers to detect, analyze, and identify cyber threats more efficiently. While supervised learning algorithms like support vector machines (SVM) and random forests are mostly used to predict data into our predefined categories based on the labeled training examples, we have to find the best method as per our experiment [11,12]. Cybersecurity employs supervised learning for the purposes of malware classification, intrusion detection, and user behavior analysis, allowing organizations to anticipate and promptly react to cyber security risks.

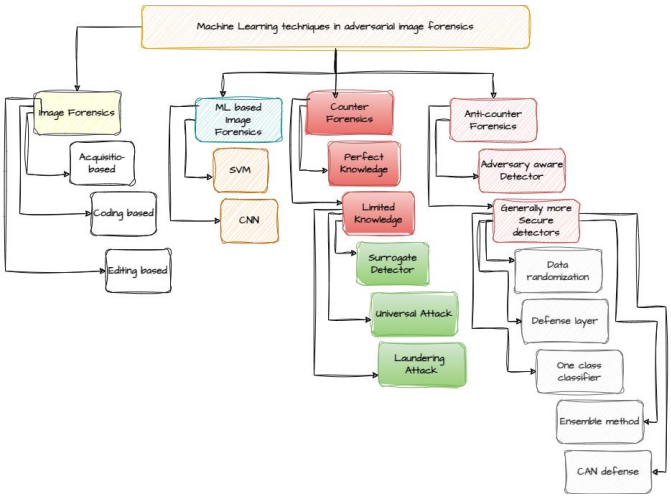

Fig. 2 Machine Learning techniques in adversarial image forensics

One major area where ML algorithms can distinctly outperform human data analysts is in unsupervised learning. Specifically, algorithms like clustering and anomaly detection are self-learning and hence do not require labeled training instances like human data analysts do. Clustering algorithms facilitate grouping of similar data points together based on their attributes, helping investigators to detect similarities between cyberattacks and discover their patterns. While the anomaly detection algorithm is intended to recognise the outliers or the deviations of an ordinary behavior which is suspicious and therefore investigating their more detailed [12]. The implementation of unsupervised learning algorithms into the systems allows companies to identify unheard of threats and vulnerabilities and improve their defense against cyber attacks.

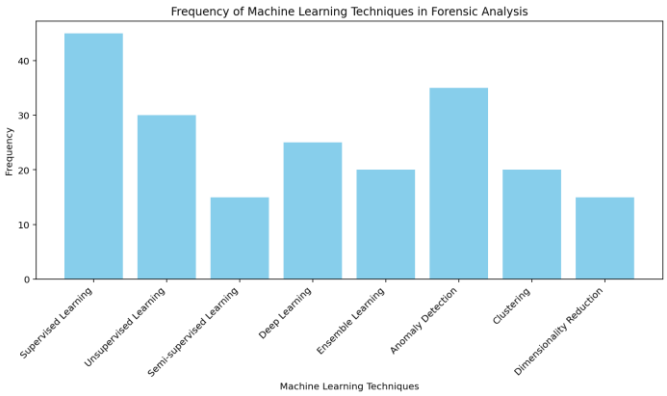

Fig. 3 Frequency of Machine Learning Techniques in Forensic Analysis

Reinforcement learning, which is a subset of machine learning that focuses on learning from failures and correct decisions made by agents during their trials, is starting to make progress towards cybersecurity incident investigations. With the reinforcement learning-based approaches, the agent works together with their environment, doing various actions to maximize their time driven reward. The described strategy is applicable to a number of tasks, for instance, learning to detect multiple malware versions, where the agent's intuition about these malware samples evolves in response to the feedback it receives from the environment [12,13]. This approach makes it possible for reinforcement learning-based systems to continuously learn and adapt to future challenges, helping organizations keep up with cyber adversaries and maintain cyber resilience.

D. NATURAL LANGUAGE PROCESSING FOR THREAT INTELLIGENCE

Natural language processing (NLP) methods are drawing out insights that are actionable from the unorganized data sources which include threat intelligence feeds, incident reports, dark web, and some other sources. NLP algorithms are capable of processing textual data, which can be used to identify the root of threats i.e. actors, TTPs etc; this is shared across the organizations boosting threat intelligence. Cybersecurity professionals can utilize the power of NLP to make a deeper understanding of cyber threats and take more assertive action on the threat mitigation and response strategies through the integration of the NLP in cybersecurity [13]. Another important function of NLP in threat intelligence is sentiment analysis whereby the text will be examined to know the feelings or thoughts of the author. Sentiment analysis can be utilized to estimate the credibility and reliability of various sources of threat intelligence, detect potentially malicious activities, and prioritize the risk data streams depending upon the scale or level of severity. Another aspect is the usage of NLP techniques such as named entity recognition (NER), to identify entities like organizations, individuals, or locations, mentioned in threat intelligence reports. This enables threat analysts to spot threats and their actors [14,15]. Another function of NLP algorithms is topic modeling which is the process of finding the main themes or topics present in a collection of documents. Techniques like latent Dirichlet allocation (LDA) can be used in topic modeling, which can help analysts to discover emerging themes and patterns in cyber threats. In turn, this allows organizations to predict events and formulate measures to neutralize future threats. With the use of NLP in the analysis of large-scale textual data and the extraction of valuable insights, organizations are aided to improve their threat intelligence capabilities and out-wit cyber adversaries.

E. CHALLENGES AND CONSIDERATIONS

The application of AI in cybersecurity incident investigations has taken center-stage offering a lot of opportunities. However, this development has also posed a considerable number of obstacles and issues that must be addressed for AI to serve its purpose and counter any risks that could come up. One of the main difficulties is data privacy and data security, because AI-based forensic analysis always has to deal with the most delicate data, which are, for instance, network logs, user activity records and threat intelligence feeds [16]. Organizations have to implement such measures that can stop unwarranted interference with the data of global commons; at the same time, these measures should comply with relevant regulations and privacy laws.

Another challenge is algorithmic bias, which can occur when AI algorithms do not provide fair or non-discriminatory outcomes for various reasons, including due to the data argument or in the algorithm itself. The problem of algorithmic bias in cyber security investigation is that it leads to an inaccuracy in the threat detection, makes mistakes on the basis of true or false as well as causing a damaging effect for individuals or organizations. Replicating human prejudices in AI technologies has various potential negative impacts which include unfairness, lack of transparency and accountability thus addressing algorithmic bias involves selective data, careful algorithm design and performance evaluation to reduce risks of bias [17].

Besides interpretability and explainability, AI-powered cybersecurity investigations also need to address the decisions made by AI algorithms because their implementation impacts the organizations and individuals extensively. AI systems must be open and obvious, meaning cybersecurity staff should be able to know how decisions are reached and why some of the affected actions were taken [18]. The increased transparency is critical for the proper building of trust in AI-based forensic analysis systems and the ability of the interested parties to interpret and act based on the results obtained from these systems.

Another important limitation comes from the limitations of scalability and resources for the organizations that look at AI-based evidence discovery solutions at scale. AI training systems are frequently very complex on many levels, have strong resource and infrastructure needs as well as frequently resulting in non-sufficient computational resources, data storage and processing power, which might also hinder the success of some organizations. In this regard, the software constantly must be modified as it matches rapidly changing technology and is being based on evolving cyber threats, moreover, makes it necessary to provide more resources and professionals to implement and maintain AI models and algorithms.

IV. SIGNIFICANCE AND BENEFITS TO THE U.S

The role of artificial intelligence (AI) in cybersecurity incident investigations is gaining a lot of value and opportunities for the United States in different fields. Underlining the point, automated forensic analysis indeed ameliorates the nation's cyber-readiness by making the threat detection, analysis, and response much more timely and accurate than the human analysts. AI-equipped solutions enable organizations to hinder hackers by spotting and proactive neutralizing of cyberattacks, with the ultimate goal of protection of the critical infrastructure, public agencies, and businesses from the negative effect of the attacks. Moreover, AI-based investigations of cybersecurity incidents provide a powerful way for threat intelligence sharing and collaboration with government, law enforcement bodies and private entities. Through the implementation of AI's natural language processing (NLP) technologies, AI algorithms are able to derive useful information from a host of unstructured data sources and communicate these relevant and timely threat intelligence to various parties.

Additionally, the use of AI in investigations of cyber incidents is instrumental in not only spurring innovation and development of new technology in the US but also fostering new ways of thinking about cybersecurity. The USA, which is the primary world actor in AI research and implementation, will take the advantage of the constant development and investment of AI-

backed cybersecurity issues [19]. Through the promotion of research and development efforts, the establishment of public-private partnerships, and the facilitation of knowledge exchange and coordination, the USA can not only keep cybersecurity at the top, but also drive economic progress and thus build prosperity. AI-powered cybercrime forensics also has the ability to increase the speed and performance of procedural investigations relative to cyberattacks and incidents of cybercrime. Automating the mundane tasks and increasing the effectiveness of human capabilities, AI-powered systems could be used by law enforcement agencies to find and arrest criminals in cybercrimes, get the evidence and try the offender in court. Strengthening investigative power to stop cybercrime and reform the laws of the Internet is yet another contribution to digital rule of law.

V. FUTURE IN THE U.S

AI-supported cybersecurity incident investigation in the USA will be full of promising prospects for continued discoveries and successes as technology evolves in perfection while battling against cyber threats. With AI technologies being continuously developed and becoming more intelligent, their integration in cyber security operations is foreseeable to be craving for government agencies, critical infrastructure sectors and private enterprise [18]. The future of AI is expected to make it even more powerful with even more specific domains for which AI will be highly fitted and ready to tackle specific cyber-environment incidents and situations. (One of the AI areas of interest in cyber technologies security in the U.S. is the future development of AIs with increasingly sophisticated and domain-specific algorithms. Investigators try to explore the real potential of AI algorithms such as machine learning, deep learning. These developments will allow companies to detect, assess, and respond in an effective way to cyber attacks of various kinds: intruders, hackers, enemy spies, and long-time advanced persistent threats (APTs).

Furthermore, one can anticipate that in the future, the use of AI-empowered cybersecurity in the U.S. is going to get better with more ability of information integration within the systems of AI-powered cybersecurity and existing cybersecurity tools. Organizations are keen on artificially combining AI to overcome those limitations of existing cybersecurity capabilities, having AI provide them with threat detection, incident response, and threat intelligence sharing mechanisms into their cybersecurity system. The interconnection of AI with available cybersecurity technologies and structure helps the organization to achieve the goal. In this way they can use AI to the full extent, underpinned with their existing security investments. Moreover, the future of AI-enabled cybersecurity in the US will mean the growing collaboration and information exchange among governmental departments, businesses, academia and foreign partners in mutual security protection. Public-private collaborations and cross-sector collaborations will be central in realizing these capabilities not only but also they will help in information exchange, technology exchange, and joint research endeavors. Stakeholders can unite their talents and assets and as a result form the basis of a common platform that can contribute in tackling similar challenges and increase the nation's resilience to cyber threats.

VI. CONCLUSION

This paper has discussed how AI can be used in a cybersecurity investigation, mainly through the use of AI-based forensics for detection, response, and analysis of the cyber threats. The paper has shown that by using a wide range of emerging AI technologies including machine learning, natural language processing, and anomaly detection, the role of the traditional processes of forensic analysis can be greatly enhanced and the current cyber-crime problems solved. Additionally, AI-driven cybersecurity for the United States is discussed with an emphasis on its role in building cyber resilience, enabling sharing of threat information, facilitating innovation, and strengthening its law enforcement agencies. Applying the AI technique, the U.S. should be prepared to successfully defend its critical infrastructure, to develop a nationalistic security, and to be at the leading edge in global cybersecurity. Finally, it is possible to conclude that the AI for cybersecurity in the U.S. will certainly continue to invent, to collaborate, and be adaptive to emerging cyber threats. Harnessing AI advances in their full potential as well as promoting collaboration among different sectors of society will lead to greater United States cyber resilience and adaptation to the emerging cyber threats as well.

REFERENCES

[1] B. Carrier, File system forensic analysis. Boston, Mass. ; London: Addison-Wesley, 2005.

[2] H. Carvey and E. Casey, Windows forensic analysis DVD toolkit. Burlington, Ma Syngress Publ, 2009.

[3] H. Carvey, Windows forensic analysis toolkit : advanced analysis techniques for Windows 8; [4E]. Waltham, Ma: Syngress, 2014.

[4] H. A. Carvey, D. Kleiman, and J. Faircloth, Perl scripting for windows security : live response, forensic analysis, and monitoring. Burlington, Ma: Syngress, 2007.

[5] J. Dykstra, Essential Cybersecurity Science. "O'Reilly Media, Inc.," 2015.

[6] M. Gregg, The network security test lab : a step-by-step guide. Indianapolis, In: Wiley, 2015.

[7] D. Watson and A. Jones, Digital Forensics Processing and Procedures : Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements. Waltham, Massachusetts: Elsevier Science, 2013.

[8] A. Jones and C. Valli, Building a digital forensic laboratory : establishing and managing a successful facility. Burlington, Mass: Butterworth-Heinemann/Syngress Pub, 2009.

[9] C. Altheide and H. A. Carvey, Digital forensics with open source tools : using open source platform tools for performing computer forensics on target systems : Windows, Mac, Linux, UNIX, etc. Rockland, Mass.: Syngress ; Oxford, 2011.

[10] K. J. Jones, R. Bejtlich, and C. W. Rose, Real digital forensics : computer security and incident response. Upper Saddle River, Nj: Addison-Wesley, 2006.

[11] H. Jahankhani, Handbook of electronic security and digital forensics. Singapore ; Hackensack, Nj: World Scientific, 2010.

[12] E. Huebner and Stefano Zanero, Open source software for digital forensics. New York: Springer, 2010.

[13] J. Sammons, The basics of digital forensics : the primer for getting started in digital forensics. Waltham, Ma: Syngress, 2015.

[14] J. Sammons, Digital forensics : threatscape and best practices. Waltham, Ma: Syngress Is An Imprint Of Elsevier, 2015.

[15] R. Slade, Software forensics : collecting evidence from the scene of a digital crime. New York: Mcgraw-Hill, 2004.

[16] B. Nelson, A. Phillips, and C. Steuart, Lab Manual for Nelson/Phillips/Steuart's Guide to Computer Forensics and Investigations, 5th, 5th Ed. Course Technology Ptr, 2015.

[17] B. Nelson, A. Phillips, and C. Steuart, Guide to Computer Forensics and Investigations + Lms Integrated for Labconnection 2.0, 2-term Access. Course Technology Ptr, 2015.

[18] C.H. Wei and Chih-Ying Gwo, Modern library technologies for data storage, retrieval, and use. Hershey: Information Science Reference, 2013.