IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 13, No. 4, August, 2023, pp. 701-707
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Cyber Forensics with AI and Machine Learning: A Study on Automated Threat Analysis and Classification

Bandr Fakiha

Faculty of Health Sciences, Medical Health Services Department, Umm Al-Qura University, Al-Qunfudah 28821, Saudi Arabia

Corresponding Author Email: bsfakiha@uqu.edu.sa

https://doi.org/10.18280/ijsse.130412

Received: 25 May 2023
Revised: 15 July 20223
Accepted: 2 August 2023
Available online: 28 September 2023

Keywords:
artificial intelligence, machine learning, cyber threats, cyber forensics, automated analysis, digital forensic investigation, case studies, survey research, threat detection

ABSTRACT

The escalating frequency and complexity of cyber-attacks have necessitated the development of effective cyber forensic investigation techniques. This research investigates the utilization of machine learning and artificial intelligence (AI) in automated analysis and classification of cyber threats, aiming to enhance the understanding of their role in cyber forensics. Employing case studies, observations, and surveys, information was gathered from forensic investigators and cybersecurity experts. The case studies comprehensively examine organizations that have implemented AI and machine learning in cyber forensics. Observational methods involve attending conferences and closely observing investigators during forensic analysis. Survey data from forensic investigators and cybersecurity experts were collected to gain insights into the application of these novel investigation methods in cyber forensics. The findings demonstrate that AI and machine learning are emerging as powerful tools for augmenting cyber forensic investigations, particularly in the realms of threat detection and classification. The case studies reveal that businesses adopting these technologies have experienced notable improvements in the efficiency and precision of forensic investigations. This study underscores the potential advantages of integrating artificial intelligence and machine learning in advancing digital forensic investigations and provides valuable insights into their roles in cyber forensics. Accelerated analytical procedures and enhanced threat detection capabilities are evident outcomes of incorporating these technologies. By leveraging AI and machine learning, investigations can be expedited, enabling prompt responses to cyber threats and reducing overall risk exposure for businesses. As the cybersecurity landscape continues to evolve, the successful integration of AI and machine learning in the industry holds the promise of ushering in a new era of proactive threat detection, bolstering organizations' capacity to safeguard digital assets.

1. INTRODUCTION

The increasing dependence on computer systems and related technologies has led to a surge in cyberattacks, necessitating effective cyber forensic investigations. According to a study by Sharif and Mohammed [1], cybercrime damages are projected to reach staggering levels, with an estimated cost of at least $10.5 trillion to the global economy annually in the next two years. As organizations grapple with the escalating hazards posed by cyberattacks, navigating the intricate web of digital evidence left behind becomes crucial. While traditional forensic techniques remain vital, they often struggle to cope with the sheer volume and complexity of data. Manual categorization and evaluation of cyber threats are time-consuming, laborious, and prone to errors. As a result, there is a growing demand for cutting-edge technologies that can assist forensic investigators in more effectively and reliably identifying and classifying cyber hazards. Artificial intelligence (AI) and machine learning (ML) are two such technologies.

The potential of machine learning and artificial intelligence in augmenting digital forensic investigations through automated analysis and classification of cyber threats has been widely recognized. The sheer magnitude of data can overwhelm human investigators, making it challenging to manually detect, analyze, and categorize information. However, these technologies offer the capability to accomplish these tasks in significantly reduced time [2]. Furthermore, machine learning algorithms can identify anomalies and learn from patterns to anticipate future cyber threats [3]. By introducing AI and machine learning, the industry can address the limitations of traditional approaches, enhancing the efficiency and accuracy of threat detection [2]. Notably, the inherent automation of AI and ML has the potential to expedite investigations and enable more rapid incident response strategies. In a field where agility and precision are paramount, the integration of AI and ML presents transformative potential that extends well beyond conventional investigation approaches.

1.1 Research aim

The present study aims to investigate the role of machine learning (ML) and artificial intelligence (AI) in cyber forensic investigations. Employing a mixed-methods approach, this research combines case studies, observation, and surveys to gather data from forensic investigators and cybersecurity experts. The analysis focuses on organizations that have implemented ML and AI in cyber forensics, comparing their effectiveness with traditional investigation methods. The observational component entails attending conferences and closely observing investigators from both groups as they conduct forensic analysis. Additionally, surveys will be administered to forensic investigators and cybersecurity experts to gain insights into the utilization of these novel investigation methods in cyber forensics.

The primary objective of this study is to evaluate the efficacy of AI and ML approaches in bolstering cyber forensic investigations, particularly in terms of expediting data processing and enhancing the accuracy of threat detection. Extensive comparisons will be conducted between these technologies and traditional methods to identify disparities in efficiency, accuracy, and overall investigative outcomes. Furthermore, this study aims to explore the intricate adoption of AI and ML within the realm of cyber forensics, examining the facilitating and inhibiting factors that shape their integration. This comprehensive assessment will provide a thorough understanding of the dynamics influencing the influence of AI and ML in this critical domain.

In addition to its practical implications for investigators, this paper contributes to the expanding scientific literature on the application of ML and AI in cyber forensics. The research findings will offer valuable insights into the advantages of these emerging technologies in enhancing digital forensic investigations, particularly in the domains of threat detection and classification. Through an examination of their practical implementation in cyber forensics, this study contributes to the development of effective strategies for combating cybercrime and fortifying digital security.

1.2 Research questions

The researchers developed four research questions to guide the study:

- How effective are artificial intelligence and machine learning in detecting and categorizing cyber threats during forensic investigations?
- What are the benefits and drawbacks of using artificial intelligence and machine learning in cyber forensic investigations, as perceived by forensic investigators and cybersecurity experts?
- To what extent do organizations currently incorporate artificial intelligence and machine learning into their cyber forensic investigations, and what factors influence their adoption of these technologies?
- What are potential limitations and challenges in implementing AI and ML in cyber forensic investigations?

2. LITERATURE REVIEW

The integration of machine learning (ML) and artificial intelligence (AI) has significantly advanced cyber forensics, fostering effective data security and cybercrime investigation over recent decades [4]. To address the escalating frequency of cyberattacks, organizations and companies have made substantial investments in these transformative technologies, recognizing the crucial need for robust digital forensic investigation methods. Notably, the cyber security industry presently faces an unprecedented surge in cyberattacks, impacting millions of individuals annually [5]. Projections indicate that this number will increase by over 40% in the next five years. Moreover, a report by Sharif and Mohammed [1] predicts that global losses attributable to cybercrime will amount to $10.5 trillion per year by 2025, a significant surge from approximately $3 trillion in 2015. Consequently, there exists an urgent requirement for advanced technologies to aid forensic investigators in efficiently and accurately detecting and categorizing cyber risks, thereby facilitating expedient implementation of legal procedures and protective strategies.

In the realm of cyber forensic investigations, artificial intelligence has emerged as an invaluable tool, leveraging its capacity to analyze vast volumes of data and discern patterns [6]. AI-enabled systems possess the capability to automatically collect, process, and analyze digital data, encompassing network traffic and log files, enabling real-time identification of potential cyber threats and prompt investigation of incidents. For instance, such systems facilitate the automation of data correlation and analysis from multiple sources, enhancing the ability to trace the origins of attacks [7]. Fundamentally, artificial intelligence empowers investigators to scrutinize extensive data sets and derive more informed conclusions, thereby augmenting the efficacy of investigations.

On the other hand, Machine learning, a subset of AI, entails the utilization of algorithms that can autonomously learn from data and enhance their performance without explicit programming [8]. In the domain of cyber forensics, ML exhibits the capability to automatically classify and analyze digital data [9]. For instance, through the training of machine learning algorithms, network traffic can be scrutinized to discern trends indicative of cyberattacks. Moreover, machine learning facilitates the automation of malware investigation by identifying patterns within code that correspond to suspicious operations. Consequently, the integration of ML expedites and enhances the accuracy of analysis in cyber forensic investigations, empowering investigators to swiftly detect and mitigate cyber risks.

The significance of artificial intelligence and ML in analyzing vast data volumes and uncovering potential cyber risks cannot be overstated. These technologies find utility across various stages of the investigation process, encompassing evidence gathering, processing, and threat detection. Acquiring a comprehensive understanding of these stages and the transformative potential of these technologies is paramount.

The initial phase of any digital forensic investigation necessitates evidence collection [10]. This undertaking entails the aggregation of data from diverse sources, such as mobile devices and cloud storage. Conventional evidence collection methods rely on manual search and analysis of digital devices, which are susceptible to errors and time-consuming. However, AI and ML can automate the evidence collection process, mitigating the associated time and effort. Notably, digital forensic triage tools represent a prominent approach to automating evidence collection. These tools leverage machine learning algorithms to scan devices for potentially relevant data, including file types and timestamps. Consequently, investigators can expedite the identification of potentially pertinent data and diminish the volume of data necessitating manual analysis [11]. By fostering the development of automated systems proficient in collecting and analyzing vast data quantities, AI-driven technologies have revolutionized the evidence gathering process. This transformation stems from the remarkable pattern recognition capabilities inherent in machine learning algorithms, enabling the identification of subtle irregularities indicative of cyberattacks. Moreover, AI systems proficiently identify pertinent digital traces, thereby streamlining investigations and enhancing the precision with which digital evidence is interpreted. An illustrative example lies in the ability of machine learning systems to discern intricate connections amidst seemingly disparate data elements, facilitating the reconstruction of breach events and substantially augmenting investigation outcomes.

The incorporation of ML and AI in data collection yields two significant advantages. Firstly, the automated nature of these technologies enables a substantial reduction in the time required for evidence gathering and processing. This expeditiousness empowers investigators to swiftly and efficiently respond to cyber incidents, a critical capability in combating rapidly spreading and evolving cyber-attacks. Secondly, the integration of ML enhances the accuracy of evidence collection, mitigating the potential for human errors that could compromise the integrity of the investigation. Additionally, the extensive pattern recognition capabilities of ML algorithms contribute to the identification of concealed digital footprints that may elude conventional methods.

Post evidence collection, digital forensic investigators proceed to data analysis, a stage entailing the examination of the gathered data to identify potential evidence relevant to the investigation's objectives. Numerous investigative organizations, particularly government legal bodies, have leveraged ML and AI technologies to significantly enhance their research capabilities [12]. Clustering algorithms represent a common approach employed by these investigative bodies to automate data analysis. Such algorithms facilitate the grouping of similar data, aiding investigators in identifying potential patterns and unusual trends within the analyzed data [13]. Similarly, natural language processing (NLP) algorithms are utilized to analyze written or spoken language, facilitating the identification of potential evidence in text-based communication.

Following successful data analysis, investigators move on to the detection of additional threats, a crucial step in preventing future attacks. AI plays a vital role in this stage by automating the threat detection process through various detection tools and methods. Sophisticated intrusion detection systems (IDS) contribute to the automation of data detection by analyzing network traffic and identifying potential threats based on patterns and anomalies within the data [14]. Similarly, machine learning-based malware detection systems analyze code to identify potential malware by examining patterns, trends, and features within the code. Research by Tayyab et al. [15] demonstrates that these malware detection systems exhibit tenfold greater accuracy compared to traditional intrusion detection methods.

Undoubtedly, the integration of machine learning in cyber forensics enhances digital forensic investigations by automating and expediting evidence collection, data analysis, and threat detection processes [16]. However, the effectiveness of these technologies relies on other equally significant factors, including data quality, investigation complexity, and the capabilities of the machine learning algorithms employed [17]. It is important to note that despite the recognized benefits over traditional methods, further research is necessary to comprehensively comprehend the potential and limitations of these technologies in the realm of cyber forensics. Furthermore, the conclusions drawn from these studies not only illuminate the expeditiousness of evidence identification and analysis facilitated by ML and AI but also shed light on the intricate relationship between technological advancements and the broader investigative landscape.

Building upon this foundation, the present research aims to thoroughly evaluate the application of these technologies in a field setting. Our study questions seek to explore diverse applications of machine learning and AI, assessing their advantages and disadvantages. Additionally, these questions will investigate adoption rates, influencing factors, and potential obstacles.

3. METHODOLOGY

3.1 Research model framework

The researchers in this study chose a mixed-method data collection technique consisting of observation, case study, and survey as the primary data collection methods. The mixed-method strategy allows for diverse data collection [18]. A typical scientific data collection process, specifically in the information technology field, involves the researcher developing a hypothesis for a tested explanation for an observation in the industry. They then formulate a research strategy that supports or refutes the hypothesis [19]. The purpose of the research is to test the theory [20]. One needs to identify the independent and dependent variables and implement control measures to guarantee that the process is free of confounding variables that could alter the results [21]. The researcher then uses the analyzed findings to form a conclusion. If the hypothesis is confirmed, the researcher might present a theory in light of the data. This research is by no means an exception; the researchers seek to ensure that the results are legitimate and dependable. It aims to provide a comprehensive understanding of the role of artificial intelligence and machine learning in enhancing cyber forensic investigations.

3.2 Participants

The 426 participants for the survey were selected through purposive sampling, which involves selecting individuals who meet specific criteria for inclusion in the study of Ritchie et al. [22]. The sampling frame consisted of forensic investigators and cybersecurity experts actively engaged in cyber forensic investigations and had experience using artificial intelligence and machine learning. Participants were recruited through professional organizations, conferences, and online forums related to cyber forensic investigations and cybersecurity.

3.2.1 Selection criteria

The participants in this study were forensic investigators and cybersecurity experts with experience in cyber forensic investigations. The selection criteria for participants were based on the following conditions:

- The level of experience, expertise, and involvement in cyber forensic investigations.
- Participants must have at least two years of experience in cyber forensic investigations or cybersecurity.
- The participant must have had a certification in cyber

forensic investigations, such as the Certified Information Systems Security Professional or the Certified Forensic Computer Examiner (CFCE).

- The participant also had to be willing to participate in the survey.

The main reason we employed purposive sampling to recruit 426 participants was to guarantee that participants had the needed knowledge and experience necessary to fully respond to the research questions. Specifically, we needed expertise with artificial intelligence and machine learning technology. On the other hand, 426 participants were an appropriate number for this study because of the targeted approach and conformity to the study's goals. Moreover, by concentrating on participants who match strict selection criteria, which is crucial in a specialized and difficult topic like cyber forensics, the researchers needed to obtain a higher level of data quality and understanding depth.

3.3 Data collection procedures

3.3.1 Case study

Regarding the case study, we chose an international corporation, J.S. Held. This global consulting firm provides scientific and technical expertise in several fields, including forensic cyber security. We chose this organization because it is one of the most preferred companies in cyber forensics. The company management assigned one of their cybersecurity experts who assisted us in studying one of their cases involving a large-scale data breach at a major retail corporation in 2013. In this case, J.S. Held was engaged to conduct a forensic investigation of the breach and identify the root cause of the security vulnerability the attackers had exploited. The research involved a comprehensive analysis of the company's systems and network infrastructure and a review of the security policies and procedures in place at the time of the breach.

3.3.2 Survey

After obtaining approval from the necessary authorities, the survey was conducted through the google form online platform. The researchers formulated a list of cyber security experts from different organizations in Sichuan, China, who were invited to participate in the survey. We sent them an email featuring a brief introduction to the study, a statement formal agreement and a hyperlink directing them to the questionnaire. The participants were assured of the confidentiality and anonymity of their responses. The survey questions were designed to obtain information about the use of machine learning and artificial intelligence in cyber forensic investigations. The data collected from the survey were stored securely on a hard drive and analyzed using appropriate statistical tools.

In the online survey, the participants answered the following questions:

i. How effective are artificial intelligence and machine learning in detecting and categorizing cyber threats during forensic investigations?

ii. On a scale of 1 to 10, how do you think artificial intelligence benefits cyber forensic investigation? 1 represent extremely insignificant, while 10 represents highly beneficial.

iii. What do you think are the benefits of using artificial intelligence and machine learning in cyber forensic investigation?

iv. What do you think are the drawbacks of using A.I. in your field?

v. To what extent does your organization incorporate artificial intelligence and machine learning into its cyber forensic investigations?

vi. What factors influence the adoption of these technologies?

vii. What are the ethical considerations of using artificial intelligence and machine learning in cyber forensic investigations, and how can these be addressed?

viii. What are the limitations of AI in cyber forensic investigations?

ix. What do you think is the future of artificial intelligence? Kindly explain your answer.

3.3.3 Observation

In the observation phase of the study, we booked an appointment with the same cybersecurity expert from J.S. Held Company to observe one of their cyber forensic investigations using one of the traditional methods of investigation. This case involved a similar breach in which a retail company was hacked, and its financial data was deleted from the server. The forensic cyber security expert used the memory analysis method to analyze one of the hard drives presented to the company as evidence. The expert used autopsy, an open-source digital forensics platform that provides a graphical interface to access and analyze data from digital devices [23]. Using this tool, we conducted a file system analysis, registry analysis, keyword search, and timeline analysis. The researchers observed each process while taking notes and keeping track of the time taken to complete the procedure. We then compared the results from the two groups. Comparing the traditional investigation methods with those that involve artificial intelligence was a strategy for the researchers to gain insight into the potential benefits and limitations of using machine learning and A.I. technologies in this field.

3.4 Data analysis plan

We analyzed the data collected through the observation qualitatively through thematic analysis. Thereafter, the notes taken during the observation were reviewed and then analyzed to help identify key themes. This analysis helped us to identify limitations and inefficiencies in memory analysis, which were then compared to the results of the case study where artificial intelligence was involved. We then developed a comparative bar graph using the data. On the other hand, the data collected through the case study were analyzed quantitatively through statistical analysis. Specifically, we analyzed the data we gathered from the J.S. Held organization through descriptive statistics. We used percentages to determine the effectiveness of artificial intelligence in enhancing cyber forensic investigations. The data collected through the survey were used to create a pie chart showing the distribution of respondents' answers. This approach offers helpful insights into the intricate nature of memory analysis by enabling a comprehensive investigation of limitations and weaknesses. We created a comparative bar graph to visually illustrate the disparities and highlight the possible benefits of AI integration by comparing these findings with the results of the case study. Similarly, a quantitative analysis of the case study data was carried out using descriptive statistics, specifically percentages in order to statistically evaluate the efficacy of artificial intelligence in cyber forensic investigations, this approach offers a thorough evaluation of the contribution of AI in improving investigation.

3.5 Ethical considerations

To ensure the participants' confidentiality and anonymity, each was assigned a unique identifier code in place of their actual names or positions. The participants' identities were kept confidential, and only the researchers had access to their data. Additionally, participants received a request to sign a formal agreement form before taking part in the study. The study provided detailed information about the study and their rights as participants.

4. RESULTS

The results of the observation phase showed that conventional cyber forensic investigation techniques were time- and resource-intensive. The cybersecurity expert's method of memory analysis involved laborious, time-consuming, and error-prone manual data collecting and analysis. However, the expert could execute a file system analysis, registry analysis, keyword search, and timeline analysis thanks to the graphical interface of the autopsy. The observation phase's notes also showed the significance of professional knowledge when conducting cyber forensic investigations. Utilizing machine learning technologies, i.e., clustering and anomaly detection, it was possible to quickly spot unusual data flows that pointed to the assault vector by analyzing network traffic patterns. In addition, text-based communication logs were examined using natural language processing techniques, which revealed strange linguistic patterns that suggested the extent of the breach. The AI-driven analysis made it possible to identify sophisticated attack paths and provided a thorough picture of the scope of the breach, providing useful information that sped up reaction plans and supported accurate mitigation measures.

After the case study conducted with J.S. Held, we found that their approach to cyber forensic investigation involves a comprehensive analysis of a compromised organization's systems and network infrastructure. This approach allowed the expert to conduct a thorough identification of the root cause of a security vulnerability that attackers had exploited. The researchers realized that J.S. Held's team of forensic experts utilized advanced AI techniques, i.e., network and system analysis, to identify the attack vector and to determine the extent of the breach. They also used machine learning algorithms to analyze the large volumes of data collected during the investigation to identify patterns and anomalies that may have indicated the presence of malicious activity. As a result of their AI-based investigation, J.S. Held provided the retail corporation with a detailed digital track of the breach in less than two hours of intervention.

Using the notes gathered during observation and case study, the researchers developed a comparative bar graph showing the difference in the time taken when performing different tasks using AI-based methods and when using autopsy, a traditional memory analysis method. The bar graph appears as shown in Figure 1 below. It compares the memory analysis methods with-AI-based methods, i.e., their efficiency in file system analysis, registry analysis, keyword search, and timeline analysis. The y-axis represents the time taken in minutes.

The data collected through survey methods revealed that 70% of the respondents responded in favor of machine learning methods. 25% of the participants were entirely against the use of artificial intelligence methods. They preferred traditional methods of data analysis due to various reasons. Most argued that A.I. and machine learning techniques gradually took over human jobs. 4% of the respondents were undecided about the topic, while 1% failed to respond to the survey. Figure 2 below shows the distribution of the respondents according to the survey findings.

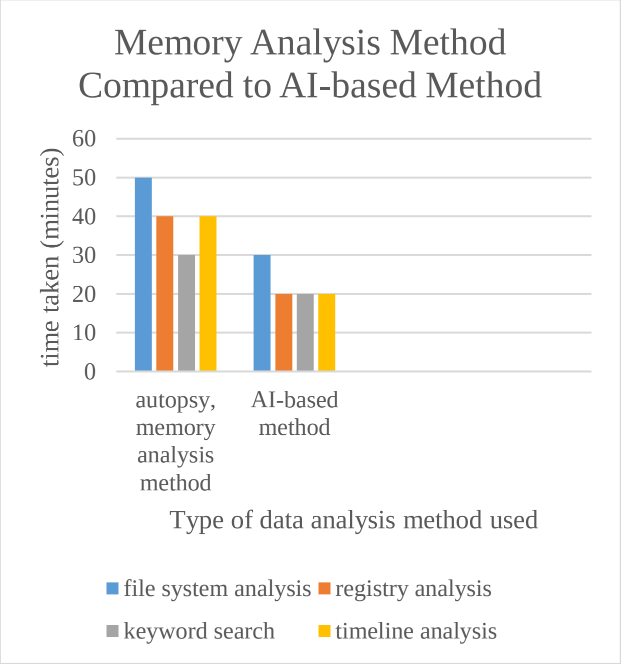

Figure 1. Compares the memory analysis method to the AI-based method

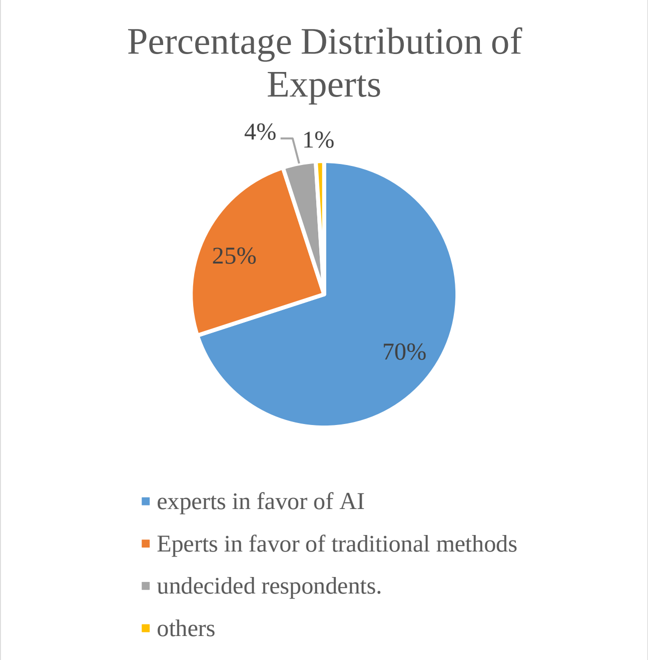

Figure 2. Distribution of experts according to their responses

The effective use of machine learning algorithms, in particular, showed a significant decrease in investigation time while retaining a high degree of accuracy. The AI-driven research proved the concept that AI can considerably improve the efficiency and precision of cyber forensic investigations. this was achieved by demonstrating its capacity of these technologies to quickly identify cyber threats and estimate breach extents.

5. DISCUSSION

This case study highlights the effectiveness of combining traditional forensic investigation methods with machine learning to enhance cyber forensic investigations and mitigate cyber threats. Comparing the time taken using traditional analysis with AI-based methods provides a better understanding of the potential benefits of machine learning and A.I. technologies in cyber forensic investigations. Evidently, investigations can be completed more quickly, accurately, and effectively with machine learning [24], thus leading to faster resolutions of security breaches. It is also essential to note that incorporating A.I. and machine learning in cyber forensic investigations could lead to improved identification of patterns, trends, and anomalies [25], which could aid in predicting and preventing future cyber threats. These findings suggest that integrating machine learning technologies could enhance the effectiveness of cyber forensic investigations, as indicated by Koroniotis et al. [26].

According to the online survey, most of Sichuan, China's cyber security specialists, know the potential advantages of utilizing artificial intelligence in cyber forensic investigations. Most respondents, more than 70%, agreed that A.I. could significantly increase the effectiveness and precision of cyber forensic investigations. Unfortunately, only a tiny portion of the specialists have actually conducted their investigations using AI-based techniques. This implies that despite the benefits of A.I. being recognized, there is still a gap in its use in cyber forensic investigations.

However, it is equally crucial to note that Traditional techniques play a significant role and provide a vital counterbalance to the advancements brought by AI and machine learning. While these state-of-the-art technologies speed up operations, conventional approaches offer a contextual depth that is beneficial in certain circumstances. For instance, traditional techniques aided by human experience may reveal hidden trends that algorithms can miss in situations involving specialized attacks. The rigorous record-keeping and chain of custody assurance, a feature of most traditional methods, guarantee the admissibility and reliability of the evidence in court.

The results of this study contribute to the body of knowledge already known in the field by empirically proving the effectiveness of artificial intelligence and machine learning in boosting investigation procedures. The distinction between conventional and AI-driven approaches provides significant insights into the advantages and drawbacks of each strategy. It illuminates the practical implications for forensic practitioners. The adoption of the proposed technology in the modern forensic investigation world shows a great potential in transforming the industry. However, there are obstacles that accompany this process. These obstacles include a lack of resources and necessary expertise. The adoption of AI may be limited by the significant investments required in terms of technology infrastructure and qualified individuals, especially by enterprises with limited resources. Additionally, cyber forensic investigators who lack expertise in these fields may face difficulties due to the particular understanding needed to use AI tools appropriately. One possibly effective strategy to close this gap will involve giving cyber forensic investigators thorough training in AI and machine learning. This will help in proper handling of the tools and systems. Governments should also facilitate funding of such beneficial technologies to improve the overall data security.

6. CONCLUSION AND CONTRIBUTION

In conclusion, this study sought to examine the advantages and disadvantages of applying machine learning and artificial intelligence to cyber forensic investigations. We conducted a case study with J.S. Held, one of the top businesses in the forensic cybersecurity industry. We watched a conventional cyber forensic investigation utilizing memory analysis and autopsy, comparing it with AI-based tools. We also conducted an online poll among cyber security specialists from various Sichuan, China, firms.

Our research findings imply that using AI-based technologies in cyber forensic investigations can drastically save the time needed to evaluate and uncover potential security breaches. Yet it also proved the significance of professional human judgment when interpreting the information produced by these instruments. Through the observation process, we were able to comprehend the advantages and limitations of the various cyber forensic analysis techniques. We concluded that while the use of AI-based tools in cyber forensic investigations can offer significant benefits, it is crucial to balance the use of these technologies and the expertise of human investigators.

Cyber forensic investigations that combine AI technology and human knowledge require a synergistic strategy that draws on the advantages of both fields. One effective tactic is to use AI as tool to speed up data processing and provide warnings for human investigators after identifying specific abnormalities. The results produced by AI can then be tailored and evaluated by human specialists, who can provide crucial domain expertise and judgment. The accuracy and effectiveness of cyber forensic investigations could be improved by this symbiotic partnership, which is defined by the complementing merging of human intuition and AI's computational capability. Ultimately, this would strengthen the cybersecurity landscape. However, further research is essential to fully understand their potential applications and limitations.

Our research has several implications for forensic investigators. The empirical validation for AI's effectiveness highlights the technology's potential to revolutionize evidence gathering and threat detection. These results support the strategic integration of AI technologies into investigative workflows, enabling cyber forensic investigators to take advantage of AI's benefits while maintaining the contextual expertise of human investigators, fostering a flexible strategy for dealing with evolving cyber threats.

REFERENCES

[1] Sharif, M.H.U., Mohammed, M.A. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews, 15(1): 138-156.

https://doi.org/10.30574/wjarr.2022.15.1.0573

[2] Lo Piano, S. (2020). Ethical principles in machine learning and artificial intelligence: Cases from the field and possible ways forward. Humanities and Social Sciences Communications, 7(1): 1-7. https://doi.org/10.1057/s41599-020-0501-9

[3] Aldweesh, A., Derhab, A., Emam, A.Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 189: 105124. https://doi.org/10.1016/j.knosys.2019.105124

[4] Iqbal, S., Alharbi, S.A. (2019). Advancing automation in digital forensic investigations using machine learning forensics. In Digital Forensic Science. Intech Open. https://doi.org/10.5772/intechopen.90233

[5] Yigitcanlar, T., Desouza, K.C., Butler, L., Roozkhosh, F. (2020). Contributions and risks of artificial intelligence (A.I.) in building smarter cities: Insights from a systematic literature review. Energies, 13(6): 1473. https://doi.org/10.3390/en13061473

[6] Poppensieker, T., Riemenschnitter, R. (2018). A new posture for cybersecurity in a networked world. McKinsey. March. https://www.cybersecitalia.it/wp-content/uploads/2018/05/a-new-posture-for-cybersecurity-in-a-networked-world.pdf.

[7] Nisha, S.S., Patil, H., Bag, A., Singh, A., Kumar, Y., Kumar, J.S. (2022). Critical information framework against cyber-attacks using artificial intelligence and big data analytics. In 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 533-537. https://doi.org/10.1109/ICACITE53722.2022.9823779

[8] Salkuti, S.R. (2020). A survey of big data and machine learning. International Journal of Electrical & Computer Engineering, 10(1). http://doi.org/10.11591/ijece.v10i1.pp575-580

[9] Karie, N.M., Kebande, V.R., Venter, H.S. (2019). Diverging deep learning cognitive computing techniques into cyber forensics. Forensic Science International: Synergy, 1: 61-67. https://doi.org/10.1016/j.fsisyn.2019.03.006

[10] Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C. (2011). Systematic digital forensic investigation model. International Journal of Computer Science and Security (IJCSS), 5(1): 118-131.

[11] Mohammed, H., Clarke, N., Li, F. (2016). An automated approach for digital forensic analysis of big heterogeneous data. Journal of Digital Forensics, Security and Law, 11(2): 9. https://doi.org/10.15394/jdfsl.2016.1384 https://commons.erau.edu/jdfsl/vol11/iss2/9/

[12] Mikalef, P., Gupta, M. (2021). Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance. Information & Management, 58(3): 103434. https://doi.org/10.1016/j.im.2021.103434

[13] Xia, J., Mandal, R., Sinelnikov, I.V., Broadhurst, D., Wishart, D.S. (2012). MetaboAnalyst 2.0 - a comprehensive server for metabolomic data analysis. Nucleic Acids Research, 40(W1): W127-W133. https://doi.org/10.1093/nar/gks374

[14] Bridges, R.A., Glass-Vanderlan, T.R., Iannacone, M.D., Vincent, M.S., Chen, Q. (2019). A survey of intrusion detection systems leveraging host data. A.C.M. Computing Surveys (CSUR), 52(6): 1-35. https://doi.org/10.1145/3344382

[15] Tayyab, U.E.H., Khan, F.B., Durad, M.H., Khan, A., Lee, Y.S. (2022). A survey of the recent trends in deep learning-based malware detection. Journal of Cybersecurity and Privacy, 2(4): 800-829. https://doi.org/10.3390/jcp2040041

[16] Baig, Z.A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., Johnstone, M., Kerai, P., Ibrahim, A., Sansurooah, K., Syed, N., Peacock, M. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22: 3-13. https://doi.org/10.1016/j.diin.2017.06.015

[17] Sharif, M.H.U., Mohammed, M.A. (2022). A literature review of financial losses statistics for cyber security and future trend. World Journal of Advanced Research and Reviews, 15(1): 138-156. https://doi.org/10.30574/wjarr.2022.15.1.0573

[18] Palinkas, L.A., Horwitz, S.M., Green, C.A., Wisdom, J.P., Duan, N., Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. Administration and Policy in Mental Health and Mental Health Services Research, 42: 533-544. https://doi.org/10.1007/s10488-013-0528-y

[19] Maxwell, S.E., Delaney, H.D., Kelley, K. (2017). Designing Experiments and Analyzing Data: A Model Comparison Perspective. Routledge. https://doi.org/10.4324/9781315642956

[20] Toledo, A.H., Flikkema, R., Toledo-Pereyra, L.H. (2011). Developing the research hypothesis. Journal of Investigative Surgery, 24(5): 191-194. https://doi.org/10.3109/08941939.2011.609449

[21] Lipton, P. (2017). Inference to the best explanation. A Companion to the Philosophy of Science, 184-193. https://doi.org/10.1002/9781405164481.ch29

[22] Ritchie, J., Lewis, J., Elam, G. (2003). Designing and selecting samples. Qualitative Research Methods, 5(3): 77-108. https://doi.org/10.4236/ojbm.2017.53040

[23] Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., Treichelt, J. (2007). Is the open way a better way? Digital forensics using open-source tools. 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), pp. 266b-266b. https://doi.org/10.1109/HICSS.2007.301

[24] Yan, J.N., Gu, Z., Lin, H., Rzeszotarski, J.M. (2020). Silva: Interactively assessing machine learning fairness using causality. In Proceedings of the 2020 chi Conference on Human Factors in Computing Systems, pp. 1-13. https://doi.org/10.1145/3313831.3376447

[25] Jarrett, A., Choo, K.K.R. (2021). The impact of automation and artificial intelligence on digital forensics. Wiley Interdisciplinary Reviews: Forensic Science, 3(6): e1418. https://doi.org/10.1002/wfs2.1418

[26] Koroniotis, N., Moustafa, N., Sitnikova, E. (2019). Forensics and deep learning mechanisms for botnets in the internet of things: A survey of challenges and solutions. IEEE Access, 7: 61764-61785. https://doi.org/10.1109/ACCESS.2019.2916717