Khurram *et al. (IJECI)* 2023

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0702154

Research Article

Vol. 7 issue 2 Year 2023

The role of Artificial Intelligence in Cyber Security and Incident Response

Syed Khurram Hassan[1] and Asif Ibrahim[2]

[1] Institute of Quality and Technology Management, University of the Punjab, Lahore, Pakistan.

[2] Department of Mathematics, FC College University, Lahore.

Corresponding author: khuramshah6515@gmail.com

Received: March 10, 2023; **Accepted**: March 25, 2023; **Published**: June 15, 2023

Abstract:

The escalating number and intricacy of cyber attacks have underscored the urgent requirement for innovative solutions to bolster the security of digital infrastructure. Among these solutions, Artificial Intelligence (AI) emerges as a promising technology with the potential to significantly enhance cyber security and incident response. It has the aptitude to improve the speed and accuracy of threat detection, response and mitigation while also reducing the workload on security professionals. This research paper focuses on the role of AI in key areas of cyber security and incident response, specifically vulnerability assessment, intrusion detection and prevention, and digital forensics analysis. It elucidates how AI, with its innate capabilities, can be a game-changer by empowering organizations to detect, respond to, and mitigate threats more effectively. However, AI is not a silver bullet for Cyber Security. Like any technology, it possesses its limitations and potential vulnerabilities. Consequently, this paper also addresses the need for ongoing development in the field of AI to overcome these limitations and challenges. By recognizing the need for continuous advancements, the research paper emphasizes the importance of future research and development efforts to maximize the potential benefits of AI in the realm of cyber security.

Keywords: Innovative solutions, artificial intelligence, cybersecurity, incident response, machine learning, sophisticated attacks, vulnerabilities

1. Introduction

Cyber security is the safety of records/statistics, property, services, and systems of cost to reduce the possibility of loss, damage/corruption, compromise, or misuse to a stage commensurate with the cost assigned. As time-sharing structures emerged within the mid to past-due 1960s and more than one job and users have been capable of running on equal time, controlling the get admission to the facts in the system became a primary point of the subject. One answer that

turned into used become to manner categorized statistics one degree at a time and "sanitize" the device after the jobs from one stage have been run and earlier than the jobs for the subsequent stage were run. This approach to pc protection became referred to as durations processing because the jobs for every level had been all run over their particular length of the day. This becomes an inefficient manner to use the device, and an effort changed into made to locate greater green software solutions to the multilevel security problem. Another approach is including extra functions or mechanisms in a laptop gadget another manner of enhancing laptop security. The mechanisms offered in this phase are grouped into authentication mechanisms, get admission to control and inference manipulation. The other approach to improving the safety of a system is to difficulty the system to rigorous warranty strategies on the way to increase one's self-belief that the system will perform as preferred. Among those strategies are penetration analysis, formal specification and verification, and covert channel evaluation. None of these techniques assure a stable system. The best boom is one's self-belief inside the protection of the gadget [1].

During the Initial Response, the gathering of data regarding the incident that began inside the previous section maintains. The goal is to accumulate enough data to allow the formula of an adequate response method in the next step. Typically, the data this is amassed in this step includes interviews of any individuals concerned in reporting the suspected incident, and available network surveillance logs or IDS reviews, which can suggest that an incident took place. The aim of the formulation of the response strategy is "thinking about the totality of the occasions" that surround the incident. These occasions include the criticality of the affected systems or statistics, what sort of attacker is suspected, and what the overall harm would possibly amount to. A business enterprise's response posture, which defines its coverage concerning the response to pc protection incidents, might also have a big effect on the choice of a reaction method. During the research of the incident, exceptional varieties of proof relevant to the incident, e.g. Host- or network-based proof, are accumulated with the purpose to reconstruct the occasions that comprise the computer protection incident. This reconstruction ought to provide reasons for what came about, when, how, or why it occurred, and who is accountable. To gain this, an investigation is usually divided into two steps: Data Collection and Data Analysis. The cause of the Resolution section is to take the right measures to contain an incident, remedy the underlying troubles that brought on the incident, and take care that a similar incident will now not occur once more. All the important steps completed must be taken and their progress supervised to verify that they may be powerful. Adjustments to the affected systems must be best completed after amassing viable evidence, otherwise, that evidence is probably lost. After the resolution of the incident is entire, it may be necessary to update protection rules or the IR techniques, if the reaction to the incident uncovered a weak spot in contemporary exercise [2].

Artificial intelligence in cyber security is beneficial as it improves how safety professionals examine, look at, and understand cybercrime. It complements the cyber protection technology that businesses use to fight cybercriminals and assist keep groups and customers secure. On the opposite hand, artificial intelligence can be very aid extensive. It may not be sensible in all applications. More importantly, it can also serve as a new weapon inside the arsenal of cybercriminals who use the generation to hone and enhance their cyber attacks. Synthetic intelligence in cyber security is beneficial as it improves how safety professionals examine, look at, and understand cybercrime. It complements the cyber protection technology that businesses use to fight cybercriminals and assist keep groups and customers secure. On the opposite hand, artificial intelligence can be very aid extensive. It may not be sensible in all applications. More importantly, it can also serve as a new weapon inside the arsenal of cybercriminals who use the generation to hone and enhance their cyber attacks. Artificial intelligence is a developing area of interest and investment in the cyber protection community. Let's hash it out. How artificial intelligence cyber security features improve digital safety ideally, if you're like many modern-day corporations, you have more than one tier of protection in location — perimeter, community, endpoint, software, and statistics security measures. For example, you could have hardware or software firewalls and network security answers that track and determine which network connections are allowed and block others. If hackers make it past these defenses, then they'll be up against your antivirus and antimalware solutions. Then possibly they'll face your intrusion detection/intrusion prevention answers (IDS/IPS), and many others [3].

Not a lot of scarce literary resources describing attempts to apply Artificial Intelligence strategies in Incident Handling, however, based on our enjoyment of the introduction of Artificial Intelligence strategies in Tactical, and particularly, Operational Cyber Intelligence, we've got come to the conclusion that gift the primary characteristic of Artificial Intelligence in Incident Handling can be fixing a category challenge, i.e. The unambiguous reference of the modern-day incident to one of the elements of the Classification Scheme, where for every element applicable techniques and workflows have been developed [4].

For the long term, the IR technique has been driven and completed with the aid of people. Automation in the execution of cyber attacks has significantly expanded the tempo with which assaults are now carried out, making it difficult for human analysts to follow. Alert fatigue is a commonplace problem among safety teams that are overwhelmed with the aid quantity and pace of in recent times automated cyber assaults. AI rises as a method to address this problem, being already gifted within the discipline of cyber security, both in literature and security products. AI is also used as an offensive device for carrying out cyber assaults, leading to the necessity of leveraging AI for protection as a way of tackling the speed and volume of such assaults. It is equally important, even though, to not forget the AI it

as a goal for the cyber attack. For the long term, the IR technique has been driven and completed with the aid of people. Automation in the execution of cyber attacks has significantly expanded the tempo with which assaults are now carried out, making it difficult for human analysts to follow. Alert fatigue is a commonplace problem among safety teams that are overwhelmed with the aid quantity and pace of in recent times automated cyber assaults. AI rises as a method to address this problem, being already gifted within the discipline of cyber security, both in literature and security products. AI is also used as an offensive device for carrying out cyber assaults, leading to the necessity of leveraging AI for protection as a way of tackling the speed and volume of such assaults. It is equally important, even though, to not forget the AI as a goal for cyber attack [5].

2. Vulnerability Assessment

In the contemporary interconnected and digitized world, the cybersecurity landscape has grown increasingly intricate and sophisticated. Organizations now confront a myriad of perils posed by cyber criminals who exploit vulnerabilities in their systems and networks, aiming to illicitly access sensitive information, disrupt operations, or inflict financial losses. To confront and mitigate these risks, organizations employ a range of security measures, among which vulnerability assessment emerges as a pivotal component of their comprehensive cybersecurity and incident response strategies. Undoubtedly, vulnerability assessment assumes paramount importance within the realm of cybersecurity administration. It entails the meticulous identification of vulnerabilities present in software and systems, constituting a proactive process of scanning and scrutinizing potential targets and emerging threats with the aim of averting malicious attacks [6]. The domain of Vulnerability Assessment has reached a considerable level of maturity; however, keeping up with the wide range of computing and digital devices requiring scrutiny poses a significant challenge [7]. This practice revolves around a methodical approach to pinpointing and assessing vulnerabilities existing within an organization's IT infrastructure, applications, and systems. It encompasses proactive scanning, testing, and analysis of potential weaknesses that may be exploited by malicious individuals. Conventional approaches to vulnerability assessment have predominantly relied on manual techniques and static rule-based systems, which frequently struggle to match the pace of the evolving threat landscape and the relentless growth in both the volume and intricacy of vulnerabilities [8]. The advent of artificial intelligence (AI) has brought about a transformative shift in the realm of cybersecurity, encompassing vital aspects such as vulnerability assessment and incident response. AI introduces fresh capabilities and efficiencies that hold the potential to greatly enhance the effectiveness and efficiency of these pivotal security processes. Through harnessing machine learning algorithms, natural language processing (NLP), and deep learning methodologies, AI-powered vulnerability assessment empowers organizations to identify, analyze, and address vulnerabilities in a more proactive,

precise, and timely manner. As highlighted by Cybersecurity Ventures, a staggering 111 billion lines of new software code are generated worldwide on an annual basis (Ventures, 2017). By employing automated mechanisms to aid in vulnerability detection prior to system deployment, product teams can dedicate more attention to feature development and performance enhancement. The proliferation of devices and applications being deployed presently not only amplifies the risks associated with networked systems but also furnishes a rich trove of training data for utilization in conjunction with artificial intelligence techniques [9]. The role of AI in vulnerability assessment assumes a multifaceted nature [10].

a) Artificial intelligence (AI) possesses the ability to automate and streamline the entire vulnerability assessment process, mitigating the need for manual efforts and empowering security teams to focus on tasks of greater value. Through the utilization of machine learning algorithms, AI can analyze extensive datasets comprising system logs, network traffic, and historical vulnerability information. This analysis facilitates the identification of patterns and anomalies that may signify potential vulnerabilities. Furthermore, AI can continuously learn and adapt to emerging threats and attack techniques, thereby bolstering the overall resilience of the vulnerability assessment process.

b) AI serves as a catalyst for more advanced and sophisticated vulnerability detection and analysis. Leveraging deep learning techniques, such as Convolution Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Generative Adversarial Networks (GANs), AI models can extract insightful information from complex datasets, including unstructured sources like security reports, blogs, and research papers. This capability empowers organizations to identify previously unknown vulnerabilities and effectively detect emerging threats.

c) AI-based vulnerability assessment significantly contributes to incident response by expediting the identification of vulnerabilities with greater accuracy. Consequently, security teams can allocate resources and prioritize tasks accordingly. By reducing the time between vulnerability detection and remediation, organizations can substantially diminish their exposure to potential attacks and minimize the impact of security incidents.

Below is a diagram illustrating the vulnerability management life cycle, outlining the optimal steps to assess vulnerabilities within a system:

1. Identify and Uncover Neglected Devices and Assets: Thoroughly examine the network to identify any devices or assets that may have been overlooked or forgotten.

2. Prioritize and Sequence Assets: Evaluate the importance and value that each asset contributes to the company, and prioritize them accordingly.

3. Comprehensive Scanning: Even after

prioritization, leave no stone unturned. Conduct a meticulous scan of every component within the system.

4. Effective Reporting: Establish a streamlined reporting mechanism to promptly communicate any ambiguities or concerns to higher-level staff.

5. Vulnerability Assessment and Ticket Assignment: Assess the vulnerabilities discovered and assign tickets based on the level of risk acceptance and urgency.

6. Solution Verification and Remediation: Verify the effectiveness of applied solutions and ensure they successfully mitigate the identified vulnerabilities.

7. Continuous Improvement: Embrace an iterative approach by repeating the improvement cycle to enhance the assessment process continually.

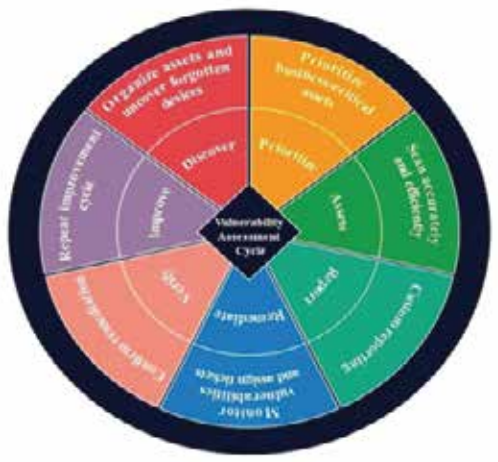

Figure 1: Vulnerability Assessment Cycle

2.1 How AI can be used for Vulnerability

Security vulnerabilities encompass various flaws and weaknesses found within information technology and its associated products, spanning across different levels and components of an information system. These deficiencies directly impact the smooth operation of the entire information system. When maliciously exploited, they can gravely compromise the integrity, confidentiality, and availability of the system. Consequently, the study of security vulnerabilities stands as a fundamental aspect within the realm of information security research [11]. In light of the escalating complexity of cyber threats, traditional security techniques are no longer sufficient to safeguard against these ever-evolving risks. Consequently, businesses are turning to artificial intelligence (AI) to bolster their cybersecurity strategies. AI offers enhanced capabilities for detecting and responding to threats, bolstering vulnerability management, and improving compliance and governance practices. By leveraging AI technologies such as machine learning, natural language processing, behavioral analytics, and deep learning, organizations can fortify their cyber defenses and shield themselves against a wide array of cyber threats, including malware, phishing attacks, and insider threats. AI has numerous applications in the cyber security industry, including [10].

2.1.1. Threat Detection and Response

AI plays a pivotal role in cyber security by enabling efficient threat detection and response. By leveraging machine learning techniques and natural language processing, organizations can analyze vast amounts of data to identify patterns and anomalies indicative of cyber threats. Intrusion detection systems

powered by AI algorithms monitor network traffic, detecting trends and abnormalities that may signify a security breach. Additionally, AI-driven cyber threat hunting helps uncover and track advanced persistent threats (APTs) lurking within networks. Predictive analytics further empowers organizations to proactively identify and address potential threats before they materialize, bolstering proactive defense strategies [10].

2.1.2. Vulnerability Management

AI is instrumental in effective vulnerability management, offering robust solutions for vulnerability scanning and prioritization. AI-enabled tools assist businesses in identifying and prioritizing issues that require remediation. Vulnerability management encompasses automating tasks such as penetration testing, security policy enforcement, and patch administration. Through AI, penetration testing can be automated, simulating attempts to exploit vulnerabilities and assessing the efficacy of existing security measures [10].

2.1.3. Compliance and Governance

AI finds valuable applications in ensuring compliance and governance within organizations. It aids in risk detection, monitoring adherence to regulations and policies, and enforcing compliance. For instance, AI automates compliance reporting and monitoring, ensuring companies adhere to regulations like HIPAA and GDPR. By analyzing extensive data sets, AI can assess risks, identify potential threats and weaknesses, and provide recommendations for suitable mitigation strategies. Furthermore, AI can automatically detect and prevent policy violations, ensuring policy compliance across the organization [11].

2.2. Identifying Vulnerabilities

There are a lot of ways that we can use in order to automate the process of identifying the vulnerabilities. Some of these ways are listed and explained below:

2.2.1. Automated Code Analysis

Utilizing AI algorithms, software code can undergo comprehensive analysis to unveil potential vulnerabilities. This approach facilitates the early identification of vulnerabilities. Static analysis techniques examine code without executing it, seeking out known code patterns, unsafe practices, or insecure coding methodologies that may give rise to vulnerabilities. Dynamic analysis techniques, on the other hand, involve executing the code in controlled environments, closely monitoring its behavior, and uncovering any security weaknesses. It's worth noting that dynamic analysis, in contrast to static analysis, conducts its evaluation during runtime on a live system. This entails executing the code with specific test cases to fulfill defined coverage criteria, albeit this process tends to be time-intensive [12].

2.2.2. *Network Traffic Analysis*

AI plays a pivotal role in scrutinizing network traffic data to discern anomalies or patterns that may indicate potential vulnerabilities. By monitoring the flow of network traffic, AI algorithms can identify suspicious activities like port scanning, atypical packet behaviors,

or attempted network intrusions. The surge in network traffic coupled with the evolution of artificial intelligence necessitates novel approaches to intrusion detection, malware behavior analysis, and the categorization of internet traffic and other security aspects. Machine learning (ML) exhibits impressive capabilities in addressing these network-related challenges [13].

2.2.3. *Vulnerability Scanning*

vulnerability scanners can autonomously conduct comprehensive scans of systems, networks, or applications to unveil known vulnerabilities. These scanners harness AI techniques to compare the gathered data against established vulnerability databases, exploit frameworks, or attack signatures, discerning the presence of any vulnerabilities [14].

1.1.4. *Behavior Monitoring and Anomaly Detection*

AI algorithms possess the ability to learn and understand typical system or user behaviors, allowing them to identify deviations that could potentially indicate vulnerabilities. Through the analysis of system logs, user activities, or system behaviors, AI systems have the capacity to detect anomalies that may serve as red flags for unauthorized access attempts, privilege escalation, or other security breaches [10].

1.1.5. *Natural Language Processing (NLP)*

Leveraging the power of NLP techniques, textual sources such as security advisories, vulnerability reports, or user feedback can undergo thorough analysis. AI algorithms excel at extracting and scrutinizing pertinent information, recognizing vulnerability-specific keywords, and comprehending the contextual nuances surrounding reported vulnerabilities [10].

3. Machine Learning-based Classification

Through the application of machine learning algorithms, datasets labeled with vulnerability information can serve as training material for code, network traffic, or system log classification. These algorithms acquire the ability to discern whether a given instance is vulnerable or non-vulnerable by assimilating patterns and indicators extracted from historical data. This knowledge empowers them to effectively identify new instances of vulnerabilities based on their learned expertise [10].

4. DEEP LEARNING

Harnessing the potential of deep learning techniques, including convolutional neural networks (CNNs) and recurrent neural networks (RNNs), proves valuable in scrutinizing intricate and unstructured data to uncover vulnerabilities. For instance, CNNs excel at processing images depicting software interfaces or network diagrams, while RNNs excel at analyzing sequences of events or logs, enabling the detection of vulnerability-related patterns [10].

5. DATA FUSION

AI systems excel at merging data from diverse sources, such as vulnerability databases, security feeds, or system logs, to construct a comprehensive and holistic perspective of potential vulnerabilities. By correlating information gleaned from these distinct sources, AI algorithms bolster the accuracy and dependability of vulnerability identification, enabling more robust cyber security measures.

6. Intrusion Detection And Prevention

Intrusion detection and prevention involve the continuous monitoring of system logs and also the network traffic to identify potential security breaches. A crucial role in this process by collecting and analyzing large amounts of data in real-time is played by automated security tool. These tools employ various techniques such as signature-based detection, anomaly detection, and behavior-based analysis to identify suspicious activities or patterns that may indicate unauthorized access attempts or other security threats. However, despite the automation provided by these tools, the expertise and judgment of human analysts remain essential. Human analysts are responsible for reviewing the findings and analysis generated by the automated systems. They assess the severity and context of the detected threats, investigate any false positives or false negatives, and determine the appropriate response strategy. Human analysts bring their knowledge, experience, and critical thinking skills to interpret the data, validate the findings, and make informed decisions about how to respond effectively to the detected threats [15].

While automation streamlines the detection process and provides initial insights, human analysts add a layer of intelligence and contextual understanding that cannot be replicated by machines alone. Their involvement ensures that the response to detected threats is tailored to the specific circumstances, aligns with organizational policies and priorities, and minimizes the risk of false positives or unnecessary disruptions to legitimate network activities. Human analysts also play a crucial role in adapting the intrusion detection and prevention systems to evolving threats by continuously learning from new attack techniques and adjusting the system configurations accordingly [15].

In this topic, we will explore the initial three subtopics: Network-based Intrusion Detection and Prevention (NIDP), Host-based Intrusion Detection and Prevention (HIDP), and Intrusion Detection and Prevention Systems (IDPS).

6.1 Network-based Intrusion Detection and Prevention (NIDP)

Network-based Intrusion Detection and Prevention (NIDP) entails the surveillance of network traffic to identify and respond to potential intrusions. NIDP utilizes various techniques to analyze packet-level data and identify abnormal or malicious behavior. A fundamental approach in NIDP is packet analysis, which involves scrutinizing network

packet headers and contents to identify patterns or anomalies indicating potential intrusions. Common techniques employed in packet analysis include deep packet inspection (DPI) and protocol analysis [16].

Anomaly detection is another crucial aspect of NIDP, involving the establishment of baseline behavior for comparison against current network activity to identify deviations. Statistical methods, machine learning algorithms, and behavioral analysis are frequently employed in anomaly detection to identify anomalies. By comparing present network traffic patterns to historical data or predefined thresholds, NIDP systems can generate alerts or implement preventive measures [17].

Signature-based detection is a well-established technique in NIDP, which entails comparing network traffic against a database of known attack signatures. If a match is found, the system raises an alert. Although signature-based detection efficiently identifies known attacks, it may struggle with detecting novel or previously unseen attack patterns. To overcome this limitation, intrusion detection and prevention systems often combine signature-based detection with anomaly-based approaches for heightened security [18].

Network traffic monitoring is an integral part of NIDP, encompassing the collection and analysis of network flow data, including source and destination IP addresses, ports, protocols, and session duration. Through network flow analysis, security administrators can identify suspicious patterns such as abnormal data volumes or unusual communication patterns. Network flow data can also be utilized to visualize network activity and detect patterns that may not be discernible through other analysis techniques [19].

6.2 Host-based Intrusion Detection and Prevention (HIDP)

Host-based Intrusion Detection and Prevention (HIDP) focuses on monitoring activities and events on individual hosts or endpoints to protect against internal network-based attacks. HIDP techniques provide detailed visibility into host-level activities, playing a vital role in safeguarding systems. Log analysis is a key component of HIDP, as system logs contain valuable information regarding host activities, including login attempts, file accesses, system calls, and configuration changes. Analyzing log files enables security analysts to identify suspicious or unauthorized activities. Automated log analysis tools aid in detecting patterns or events of interest, facilitating efficient intrusion detection [20].

System call monitoring is another important HIDP technique that involves capturing and analyzing system calls made by programs or processes running on a host. By monitoring system calls, HIDP systems can detect malicious or abnormal behavior, such as unauthorized access attempts, privilege escalation, or file manipulation. Anomalies detected through system call monitoring can trigger alerts or proactive measures to mitigate potential risks. File integrity checking is a mechanism employed to ensure the integrity of critical system files. HIDP systems often main-

tain hash or checksum values for each file and periodically verify their integrity by recalculating the hash and comparing it with the stored value. The detection of discrepancies indicates potential file modifications or tampering, which could signify a security breach [21].

Behavior-based detection techniques in HIDP involve the continuous monitoring and analysis of process and application behavior running on hosts. This approach focuses on identifying deviations from expected behavior patterns, allowing for the detection of abnormal or potentially malicious activities. In conclusion, NIDP, HIDP, and IDPS form essential subtopics in intrusion detection and prevention. By utilizing techniques such as packet analysis, anomaly detection, signature-based detection, log analysis, system call monitoring, and behavior-based detection, organizations can enhance their ability to identify and prevent intrusions, safeguarding their networks and systems from malicious activities [22].

6.3 Intrusion Detection and Prevention Systems (IDPS)

Intrusion Detection and Prevention Systems (IDPS) play a vital role in the identification and response to intrusions in computer networks and systems. These systems are designed to continuously monitor network traffic, host activities, and system logs, offering real-time capabilities for detecting and preventing threats. IDPS can operate in different modes, including network-based, host-based, or a combination of both, to provide comprehensive security coverage. IDPS are built on a combination of technologies, methodologies, and algorithms to recognize and mitigate security threats. To find malicious actions and potential vulnerabilities, they use cutting-edge detection techniques like signature-based detection, anomaly detection, and behavior-based analysis. [23].

Signature-based detection in IDPS involves comparing network traffic, host data, or system logs against known attack signatures or patterns. These signatures are derived from previously identified and documented malicious activities. If a match is found, the IDPS generates an alert, enabling security personnel to take appropriate actions. Signature-based detection is effective in identifying known attacks but may face challenges in detecting new or unknown attacks that lack pre-existing signatures. Anomaly detection is another essential component of IDPS. This technique involves establishing a baseline of normal behavior for the network or host and comparing ongoing activities against this baseline. Any deviation or anomaly from the established norm may indicate a potential intrusion. Anomaly detection algorithms utilize statistical methods, machine learning, and behavioral analysis to identify unusual patterns, network traffic spikes, or abnormal system behavior. By generating alerts based on detected anomalies, IDPS can aid in the detection of previously unseen or evolving threats. Behavior-based analysis is a proactive approach employed in IDPS to identify malicious activities based on the observed behavior of network traffic, applications, or system processes. By analyzing the sequence of actions, resource access patterns, or commu-

nication behavior, IDPS can detect deviations from expected behavior and raise alerts. Behavior-based analysis is particularly effective in detecting sophisticated attacks that may evade signature-based detection [24].

Apart from detection, IDPS also prioritize prevention and response. When a potential intrusion or suspicious activity is detected, IDPS can take various actions to prevent further harm or reduce the impact. These actions may involve blocking network traffic, isolating compromised hosts, resetting user sessions, or notifying security personnel for further investigation. IDPS can also integrate with other security systems, such as firewalls, to automatically enforce access control policies or update rule sets to enhance overall security.

6.4. *AI and Intrusion Detection and Prevention*

AI can augment the capabilities of human analysts and traditional security tools in several ways. Here are some examples:

6.4.1. Real-time monitoring

AI algorithms can analyze network traffic and system logs in real-time, allowing them to quickly identify and respond to potential threats. This is particularly useful in large or complex networks, where it may be difficult for human analysts to keep track of all the activity. AI can also flag potential threats that might otherwise go unnoticed by human analysts, such as low-level attacks that are designed to evade detection [25].

6.4.2. Anomaly detection

AI can be trained to recognize normal patterns of network activity, and to flag any deviations from these patterns that might indicate the presence of a cyber threat. For example, AI can detect unusual login activity, identify attempts to exploit known vulnerabilities and alert security teams to potential threats that might otherwise go unnoticed. By detecting potential threats at an early stage, AI can help to minimize the damage caused by a cyber-attack [26].

6.4.3. Automated response

Automated response in cyber security refers to the use of AI-powered tools and algorithms to automatically perform certain actions in response to detected threats or security incidents. These automated actions help to prevent the spread of cyber-attacks and mitigate their impact. Let's explore an example to better understand how automated response works. Imagine a large organization with a sophisticated AI-powered intrusion detection system in place. This system continuously monitors the network for any suspicious activities or potential cyber threats. One day, the intrusion detection system identifies a series of network packets exhibiting patterns indicative of a DDoS (Distributed Denial of Service) attack. Upon detecting this potential threat, the AI-powered security tool automatically springs into action. It analyzes the incoming network traffic, identifies the malicious packets, and determines the best course of action to mitigate the attack. In this case, the AI system decides to block the IP addresses associated with the attacking packets. Using its

automated response capabilities, the AI tool sends instructions to the organization's network infrastructure, specifically the firewalls or routers. These instructions result in the immediate blocking of the identified IP addresses, effectively stopping the malicious traffic from reaching the organization's network resources. Simultaneously, the AI system also initiates actions to isolate any infected systems within the organization's network. It identifies the compromised devices, such as computers or servers that may be participating in the DDoS attack, and quarantines them from the rest of the network. By isolating the infected systems, the AI tool prevents the attack from spreading further and causing additional damage to other network components [27].

In this scenario, the automated response capabilities provided by AI-powered security tools play a vital role in containing and mitigating the DDoS attack. By automatically blocking suspicious traffic and isolating infected systems, the AI system helps prevent the attack from disrupting the organization's network services and causing significant downtime. Furthermore, by automating these routine response tasks, the AI system reduces the workload on human analysts. Instead of spending time manually identifying and blocking malicious traffic, analysts can focus on more complex and strategic security tasks, such as investigating the root cause of the attack, identifying potential vulnerabilities, or fine-tuning the AI system's response algorithms.

Overall, the example highlights how automated response, facilitated by AI, can enhance an organization's ability to respond quickly and effectively to cyber threats. By leveraging AI's speed and precision, organizations can reduce response times, minimize the impact of attacks, and improve the efficiency of their security operations [28].

6.4.4. Predictive analysis

AI can also be used for predictive analysis, which involves using historical data to identify potential future threats. By analyzing patterns and trends in network activity over time, AI algorithms can identify potential vulnerabilities and anticipate potential threats before they occur. This can help organizations to proactively mitigate these threats before they can cause any damage.

However, it's important to remember that AI is not a panacea for all cyber security challenges, and it should be used in conjunction with other tools and techniques. For example, AI algorithms may not be able to detect advanced persistent threats (APTs) or zero-day vulnerabilities, which require human expertise and intuition to identify. Additionally, AI algorithms may be susceptible to false positives or false negatives, which can lead to unnecessary alerts or missed threats [29].

7. Incident Response

Although they use different process methodologies, incident response and computer forensics have similar goals. While both situations' primary goals are to investigate computer

security incidents and contain their effects, incident response is more focused on bringing things back to normal while computer forensics is more focused on producing evidence that can be used in court.

An organization's response to improper or undesirable behavior using a computer or network component is known as an incident response. A methodical and well-planned approach should be employed to react rather than being caught off guard and launching a disorderly and potentially disastrous response. As a result, events are typically handled by a team known as the Computer Security Incident Response Team, or CSIRT, which is made up of individuals who possess the various certifications required for the response procedure [30].

7.*1. Real time analysis of security events*

The gathering, storing, and analyzing of all data relating to the incident that has occurred or is still occurring is one of the key activities in dealing with cyber security incidents [31].

Detecting security threats in real time is the responsibility of the security operations centre (SOC), a centralised organisation. It is an essential part of a CSIRT (Corporate Security Incident Response Team). A key piece of technology used in SOCs, SIEM systems collect security events from various sources within enterprise networks, normalise the events to a standard format, store the normalised events for forensic analysis, and correlate the events to detect malicious activities in real time. The authors of this essay emphasise the critical role SIEM systems play for SOCs, address current operational barriers to properly employing SIEM systems, and identify upcoming technical problems that SIEM systems will need to overcome to remain relevant [32].

7.2. *Automated Incident Triage*

Recent years have seen a dramatic rise in the number of computer security incidents across all industries. Even small businesses suffer significant financial and reputational losses as a result of these accidents. Naturally, there has been a rise in demand for incident management relating to computers. Today, incident handling is still a challenging job that is primarily carried out by human expert teams. It is exceedingly expensive to retain such a team on call around-the-clock, especially in large organizations with extensive networks. Consequently, it is highly desirable to have automated incident handling. It was extremely difficult to automate this process due to its complexity and reliance on humans [33].

Data triage is used by Security Operation Centers to separate the real "signals" from a lot of noisy alerts and "connect the dots" to answer some higher-level questions about the activities of the attack. This work intends to naturally produce information emergency robots straightforwardly from network safety investigators' activity follows. Data triage automatons that are currently in use, such as SIEMs and Security Information and Event Management systems (SIEMs), require expert analysts to dedicate time and effort to the creation of event correlation rules [34].

7.3. *Role of AI in Incident Response*

Artificial intelligence (AI) has a significant role to play in incident response, particularly in the early detection and rapid response to security incidents. AI-powered systems can monitor and analyze vast amounts of data and quickly identify anomalous behaviors or patterns that may indicate a potential security breach.

Here are some ways in which AI can help with incident response:

7.3.1. Early detection

Early detection is a crucial aspect of cyber security as it allows organizations to identify potential threats and take proactive measures to mitigate them. Artificial Intelligence (AI)-powered systems play a significant role in enhancing early detection capabilities by monitoring network traffic, endpoints, and critical infrastructure for any signs of unusual activity or behavior. AI-powered systems leverage advanced algorithms and machine learning techniques to analyze vast amounts of data in real-time. By establishing a baseline of normal network behavior, these systems can identify anomalies that may indicate the presence of a threat. These anomalies could be deviations from typical patterns, such as unexpected network traffic spikes, unauthorized access attempts, or unusual data transfers. One of the significant advantages of AI-powered systems is their ability to detect threats that may go unnoticed by human analysts. While human analysts play a critical role in cybersecurity, they are limited by their capacity to process large volumes of data and to recognize subtle patterns or anomalies. AI systems, on the other hand, can analyze massive amounts of data quickly and efficiently, allowing them to identify potential threats in near real-time. To achieve early detection, AI systems employ various techniques. One common approach is anomaly detection, where AI algorithms learn from historical data to establish normal patterns of network behavior. They then continuously monitor incoming data and compare it to the established baseline. Any deviation from the norm triggers an alert, indicating a potential security threat. Another technique used by AI-powered systems is behavioral analysis. These systems monitor and analyze the behavior of endpoints, such as individual devices or users, to identify any abnormal activities. By learning from historical data and establishing typical user behaviors, AI algorithms can identify behavior that deviates from the norm, which may suggest malicious intent or compromised endpoints [35].

7.3.2. Rapid response

AI systems play a crucial role in alerting security teams to potential security incidents, enabling them to respond promptly and mitigate the impact of the incident. Through continuous monitoring and analysis of network traffic, endpoints, and critical infrastructure, AI-powered systems can quickly identify anomalies and suspicious activities that may indicate a security breach or cyber attack. When an AI system detects unusual activity or behavior, it generates an alert that is immediately relayed to the security team. These alerts serve as early warnings, providing crucial

information about potential threats before they can cause significant harm. By leveraging advanced algorithms and machine learning techniques, AI systems can differentiate between normal and abnormal patterns, helping to identify potential security incidents in real-time. The quick alerting capability of AI systems is beneficial for several reasons. First, it allows security teams to respond swiftly, minimizing the time window for attackers to exploit vulnerabilities or escalate their activities. By receiving alerts in near real-time, security professionals can take immediate action to investigate and contain the incident, preventing further compromise of systems and data. Second, early detection and rapid response help mitigate the impact of security incidents. By identifying threats at an early stage, organizations can limit the potential damage caused by unauthorized access, data breaches, or malicious activities. Security teams can implement appropriate countermeasures, such as isolating affected systems, blocking malicious traffic, or initiating incident response protocols to contain and mitigate the incident swiftly [36].

7.3.3. Automated investigation

AI can help automate the process of investigating security incidents. This can help reduce the time and resources required to identify and remediate security issues.

7.3.4. Threat intelligence

AI can analyze vast amounts of threat intelligence data and provide insights into emerging threats and vulnerabilities. This can help security teams stay ahead of the curve and proactively address potential security risks.

7.3.5. Behavioral analysis

AI can analyze user behavior and identify anomalous patterns that may indicate insider threats or other malicious activity [37].

8. Forensics Analysis

The development of digital technology over the past ten years has had a significant impact on our day-to-day lives and business practices. As a result, the digital forensics field will face numerous challenges as this evolution continues [38].

The goal of forensic analysis is to uncover and interpret evidence that can help investigators understand what happened, identify potential suspects or perpetrators, and provide evidence for use in court. Forensic analysts may work for law enforcement agencies, government agencies, or private companies, and their work may be used in criminal investigations, civil lawsuits, and other legal proceedings. Therefore, Digital forensics is a complex and evolving field. To conduct effective forensic analysis in cyber security, analysts must have a deep understanding of computer systems, network protocols, and cyber threats. They must also be familiar with the legal and regulatory requirements for handling digital evidence, as well as the ethical considerations involved in handling sensitive data [39].

9. How AI Can Assist in Forensics Analysis

Compared to other application domains, digital forensics appears to have used automation and AI less frequently[40]. Artificial intelligence (AI) has the potential to significantly aid forensic analysis in a number of ways. Here are a few instances:

9.1. Data Analysis

AI can analyze vast amounts of data collected during forensic investigations, including network traffic logs, system logs, and other digital evidence. With machine learning algorithms, AI can identify patterns and anomalies in the data, which may be indicative of a cyber attack or other malicious activity [37].

9.2. Image and Audio Analysis

When it comes to image analysis, AI algorithms can be trained to identify and classify objects, faces, and other visual elements within images. By utilizing deep learning models and neural networks, AI can accurately detect and recognize specific objects or individuals. This capability proves invaluable in forensic investigations where identifying suspects or potential evidence is crucial. AI systems can rapidly process large volumes of images and flag relevant information, significantly reducing the time and effort required for manual examination. Furthermore, AI can assist in facial recognition, comparing faces captured in images or video footage against databases of known individuals. This technology can help identify persons of interest or locate missing individuals by matching faces from surveillance footage, social media images, or other sources. AI-powered facial recognition systems have been instrumental in solving numerous criminal cases by linking suspects to evidence or establishing the presence of certain individuals at crime scenes. In the context of video analysis, AI algorithms can analyze video content to extract meaningful information. This includes tracking the movement of objects or individuals, detecting specific activities or behaviors, and identifying important events within the footage. AI can also perform forensic video enhancement, enhancing the quality of low-resolution or poorly captured videos to improve visibility and aid in identifying key details. These capabilities enable investigators to reconstruct events, identify patterns, and gather evidence from video recordings more efficiently [41].

9.3. Predictive Analytic

Predictive analytic is a type of data analysis that uses machine learning algorithms to analyze historical data and identify patterns and trends that can be used to predict future events. In the context of cyber security, predictive analytic can be used to identify potential security threats or vulnerabilities by analyzing historical data from previous incidents. Predictive analytic models driven by AI can examine a large amount of data from a variety of sources, including system logs, network traffic logs, and other digital evidence. The models can spot trends and oddities in the data that might point to a security risk, such a cyberattack attempt or a system weakness that could be used by hackers. By using these predictive models, security teams can be alerted to potential security breaches in real-time, allowing them to take proactive steps to prevent or

mitigate the damage caused by a cyber attack. For example, if a predictive model identifies a potential threat in real-time, security teams can investigate the issue and take steps to prevent the attack before it causes any damage. The use of predictive analytics in cyber security can help organizations to stay ahead of potential security threats and to anticipate new attack methods, allowing them to implement proactive security measures to prevent cyber attacks. Additionally, predictive analytic can be used to identify vulnerabilities in systems and applications, enabling organizations to take corrective action to secure their infrastructure and reduce the risk of a successful attack [42].

9.4. Natural Language Processing (NLP)

AI-powered NLP algorithms can analyze text data, such as emails, chat logs, and social media posts, to identify keywords or phrases that may be related to an incident. This can help investigators identify potential suspects or gain insights into the motives behind an attack [43].

9.5. Malware Analysis

AI can help in analyzing malware by detecting and classifying malicious code. It can also identify patterns in the behavior of malware to help investigators identify its origin and the extent of the damage caused. The makers of the Magnet Axiom forensic examination tool, Magnet Forensics, included machine learning in their Magnet [44].

10. Identifying The Source And Cause Of A Security Incident

Forensic analysis plays a critical role in determining the origin and cause of a security incident. It involves a systematic examination of digital evidence to understand what happened, how it occurred, who was responsible, and the extent of the damage [45]. Below are steps involved in conducting forensic analysis to identify the source and cause of a security incident:

1. ***Secure the Affected System:*** The initial step is to isolate and secure the affected system to prevent further harm or data loss. This may entail disconnecting the system from the network or taking it offline.
2. ***Document the Incident:*** Promptly document the incident by taking comprehensive notes, photographs, or videos of the affected system. Capture relevant information like error messages, timestamps, or any unusual behavior observed.
3. ***Preserve Evidence:*** To maintain the integrity of the evidence, create a forensic copy of the affected system's storage media. This involves making a bit-by-bit replica of the entire storage device or disk partition. The copy will be used for analysis while leaving the original evidence untouched.
4. ***Conduct Initial Analysis:*** Analyze system logs, network traffic logs, firewall logs, intrusion detection system (IDS) logs, and other relevant data sources to gather initial information about the incident. Look for signs of unauthorized access, unusual activities, or anomalies.
5. ***Recover Deleted or Hidden Data:***

Employ forensic tools and techniques to recover deleted or concealed data that may provide valuable insights into the incident. This may involve examining temporary files, registry entries, or system artifacts that can shed light on the source and cause.

6. ***Perform Malware Analysis:*** If malware is suspected, conduct a detailed analysis of suspicious files or software. Use specialized tools to analyze the malware's behavior, identify its characteristics, and determine its origin.
7. ***Network Traffic Analysis:*** Scrutinize network traffic logs, packet captures, or firewall logs to identify any suspicious or unauthorized network activity. Look for indicators of unauthorized access, data exfiltration, or communication with known malicious entities.
8. ***Timeline Reconstruction:*** Create a timeline of events based on the gathered evidence. This timeline should outline the sequence of actions leading up to and following the incident. It can help identify the initial compromise and the attacker's activities throughout the attack.
9. ***User and System Analysis:*** Analyze user accounts, system configurations, and access controls to identify potential vulnerabilities or weaknesses that may have been exploited during the incident. Look for signs of unauthorized access or privilege escalation.
10. ***Collaboration and Expert Consultation:*** In complex cases, collaborate with other experts such as network administrators, incident response teams, or law enforcement agencies. Their expertise and resources can assist in the investigation and analysis process.
11. ***Report Findings:*** Prepare a detailed report summarizing the forensic analysis findings. Include a description of the incident, the methods used for analysis, the identified source and cause of the incident, and recommendations for preventing future incidents.

It's important to note that forensic analysis is a specialized field, and it is advisable to involve experienced professionals or a dedicated incident response team to ensure a comprehensive and accurate investigation.

12. Data Carving

Data carving is a fundamental technique employed in the field of digital forensics to retrieve fragmented or deleted files from storage media. It involves the identification and reconstruction of files based on their distinct signatures or patterns, circumventing the structure of the file system. Data carving proves particularly valuable when conventional file recovery methods are ineffective or when dealing with intentionally erased or damaged files [46].

The process of data carving entails scouring the raw binary data of a storage device in search of specific file headers, footers, or other data patterns. These patterns serve as indicators suggesting the presence of a particular file

type, such as documents, images, videos, or archives. By recognizing these signatures, data carving tools can extract and reconstruct files from the scattered or unallocated space on the storage medium [47].

Data carving algorithms typically function by scrutinizing the binary data and identifying distinct patterns or structures that signify the beginning and end of a file. Once a potential file is detected, the carving tool proceeds to extract the file by copying the corresponding data blocks into a separate file, ultimately generating a reconstructed version of the original file. One of the primary challenges encountered in data carving involves handling fragmented files. Due to factors like partial overwriting or deletion, files on a storage device are often stored in non-contiguous clusters or sectors. Data carving algorithms must possess the ability to identify and assemble these dispersed fragments in order to accurately reconstruct the complete file [48].
Another obstacle involves the potential occurrence of false positives or false negatives during the data carving process. False positives arise when the carving tool incorrectly identifies non-file data as a file, which can lead to the recovery of irrelevant or corrupted data. Conversely, false negatives occur when a carving tool fails to identify and recover a valid file.To enhance the accuracy and efficiency of data carving, a range of techniques and heuristics have been developed. These include advanced signature matching algorithms, file format-specific carving, entropy analysis, and error correction mechanisms [49].
Data carving plays a critical role in digital forensics, enabling investigators to retrieve valuable evidence from storage media, even in cases where the file system has been compromised or intentionally tampered with. It is an indispensable tool in investigations related to cyber crime, data breaches, intellectual property theft, and other digital offenses [50].

12. CONCLUSION

The role of artificial intelligence (AI) in cyber security and incident response is constantly evolving and holds great potential for future developments. Looking ahead, the future of cyber security will likely be shaped by emerging technologies such as quantum computing, 5G networks, and the increasing integration of AI and automation. These advancements bring new opportunities but also introduce novel security risks and challenges that will require proactive measures and innovative solutions.

13. REFERENCES

[1]. Kemmerer, R. A. (2003). Cyber security. 25th International Conference on Software Engineering, 2003.

[2]. C.Felix . Freiling Laboratory for Dependable Distributed Systems University of Mannheim, Bastian Schwittay Symantec (Deutschland) GmbH,

[3]. LJUBOMIR LAZIĆ Belgrade Metropolitan University, Faculty of Information Technologies, BENEFIT FROM AI IN CYBERSECURITY the 11th International Conference on Business Information Security, 18th October

2019, Belgrade, Serbia

[4]. R.Trifonov, R.Yoshinov, S.Manolov, G.Tsoche, & G.Pavlova. Artificial Intelligence methods are suitable for Incident Handling Automation. MATEC Web of Conferences, 292, 01044.

[5]. Vasileios Anastopoulos, PhD Davide Giovannelli, LL. M./05/2022/Automated/Autonomous Incident Response[Online]. Available: https://www.bath.ac.uk/publications/library-guides-to-citing-referencing/attachments/ieee-style-guide.pdf

[6]. B. Seumo, "Cyber Security Administration Introduction," in Conf. Introduction to Cyber Security Administration by Dr. Blondel Seumo, Dubai, United Arab Emirates, 2023, pp.2.

[7]. D. R. McKinnel, T. Dargahi, A. Dehghantanha, K. -K. R. Choo, "A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment," C&EE, vol.75, pp. 175-188, 2019.

[8]. J. Agarwal, M. Liu, D. Blockley, "Vulnerability, Uncertainty, and Risk Analysis, Modeling and Management," in Conf. Proceedings of First International Conference on Vulnerability and Risk Analysis and Management, Hyattsville, Maryland, 2011, pp. 230-237.

[9]. S. Kommrusch, "Artificial Intelligence Techniques for Security Vulnerability Prevention," Fort Collins, USA, 2018.

[10]. S. A. Jawaid, "Artificial Intelligence with respect to Cyber Security," Vienna, USA, 2023.

[11]. Q. Zhu, L. Liang, "Research on Security Vulnerabilities Based on Artificial Intelligence," in ICIC, 2019, pp. 377-387.

[12]. D. Baca, B. Carlsson, K. Petersen, L. Lundberg, "Improving software security with static automated code analysis in an industry setting," Softw. Pract. Exper., 2012.

[13]. N. Alqudah, Q. Yaseen, "Machine Learning for Traffic Analysis: A Review," in Conf. International Workshop on Data-Driven Security (DDS 2020), Warsaw, Poland, 2020, pp. 911-916.

[14]. N. Schagen, K. Koning, H. Bos, C. Giuffrida, "Towards Automated Vulnerability Scanning of Network Servers," Portugal, 2018

[15]. Y. S. Park, C. S. Choi, C. Jang, D. G. Shin, G. C. Cho and H. S. Kim, "Development of Incident Response Tool for Cyber Security Training Based on Virtualization and Cloud," 2019 International Workshop on Big Data and Information Security (IWBIS), Bali, Indonesia, 2019, pp. 115-118, doi: 10.1109/IWBIS.2019.8935723.

[16]. L. A. H. Ahmed and Y. A. M. Hamad, "Machine Learning Techniques for Network-based Intrusion Detection System: A Survey Paper," IEEE Xplore, Mar. 01, 2021. https://ieeexplore.ieee.org/document/9428827 (accessed Oct. 28, 2022)

[17]. D.-S. Kim and Jong Chun Park, "Network-Based Intrusion Detection

with Support Vector Machines," pp. 747–756, Feb. 2003, doi: https://-doi.org/10.1007/978-3-540-45235-5_73 .

[18]. P. Ioulianou, V. Vassilakis, I. Moscholios, and M. Logothetis, "This is a repository copy of A Signature-based Intrusion Detection System for the Internet of Things. A Signature-based Intrusion Detection System for the Internet of Things," 2018. Available: https://eprints.whiterose.ac.uk/133312/1/ictf_2018_IoT.pdf

[19]. P. M and S. Bose, "Design of Intrusion Detection and Prevention System (IDPS) using DGSOTFC in collaborative protection networks," IEEE Xplore, Dec. 01, 2013. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6921946 (accessed Dec. 14, 2021).

[20]. A. N. Jaber, M. F. Zolkipli, H. A. Shakir, and M. R. Jassim, "Host Based Intrusion Detection and Prevention Model Against DDoS Attack in Cloud Computing," Advances on P2P, Parallel, Grid, Cloud and Internet Computing, pp. 241–252, Nov. 2017, doi: https://-doi.org/10.1007/978-3-319-69835-9_23 .

[21]. "(PDF) Host-based Intrusion Detection and Prevention System (HIDPS)," ResearchGate. https://www.researchgate.net/publication/271070098_Host based_Intrusion_Detection_and_Prevention_System_HIDPS

[22]. A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, Jul. 2019, doi: https://-doi.org/10.1186/s42400-019-0038-7.

[23]. K. Scarfone and P. Mell, "Special Publication 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS) Recommendations of the National Institute of Standards and Technology," 2007. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

[24]. A. Sharifi, F. F. Zad, F. Farokhmanesh, A. Noorollahi, and J. Sharif, "An Overview of Intrusion Detection and Prevention Systems (IDPS) and Security Issues," IOSR Journal of Computer Engineering, vol. 16, no. 1, pp. 47–52, 2014, doi: https://-doi.org/10.9790/0661-16114752.

[25]. Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," IEEE Access, vol. 10, pp. 93104–93139, 2022, doi: https://-doi.org/10.1109/access.2022.3204051.

[26]. "Artificial Intelligence in CyberSecurity," IEEE Access, Mar. 11, 2019. https://ieeeaccess.ieee.org/closed-special-sections/artificial-intelligence-in-cybersecurity/

[27]. M. Khanbhai, P. Anyadi, J. Symons, K. Flott, A. Darzi, and E. Mayer, "Applying natural language processing and machine learning techniques to patient experience feedback: a systematic review," BMJ Health & Care Informatics, vol. 28, no. 1, p. e100262, Mar. 2021, doi: https://doi.org/10.1136/bmjh-

ci-2020-100262.

[28]. V. Mathane and P. V. Lakshmi, "Predictive Analysis of Ransomware Attacks using Context-aware AI in IoT Systems," International Journal of Advanced Computer Science and Applications, vol. 12, no. 4, 2021, doi: https://doi.org/10.14569/ijacsa.2021.0120432

[29]. [1] F. C. Freiling and Bastian Schwittay, "A Common Process Model for Incident Response and Computer Forensics.," ResearchGate, 2007. https://www.researchgate.net/publication/221002732_A_Common_-Process_Model_for_Incident_Response_and_Computer_Forensics

[30]. [2] M. Evans et al., "Real-Time Information Security Incident Management: A Case Study Using the IS-CHEC Technique," IEEE Access, 2019. https://www.semanticscholar.org/paper/Real-Time-Information-Security-Incident-Management%3A-Evans-He/49dbe6d1ddc0862726351c939ebedf5811e15bf5 (accessed May 02, 2023).

[31]. [3] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The Operational Role of Security Information and Event Management Systems," IEEE Security & Privacy, vol. 12, no. 5, pp. 35–41, Sep. 2014, doi: https://doi.org/10.1109/msp.2014.103.

[32]. [4] S. H. Hashemi, M. Babaeizadeh, M. Nowruzi, H. H. Jazi, M. Shahmoradi, and E. B. Beigi Samani, "A comprehensive semi-automated incident handling workflow," IEEE Xplore, Nov. 01, 2012. https://ieeexplore.ieee.org/document/6483144 (accessed May 02, 2023).

[33]. [5] C. Zhong, J. Yen, P. Liu, and R. F. Erbacher, "Automate Cybersecurity Data Triage by Leveraging Human Analysts' Cognitive Process," IEEE Xplore, Apr. 01, 2016. https://ieeexplore.ieee.org/document/7502316 (accessed May 02, 2023).

[34]. [6] Z. Chen, Y. Kang, P. Zhao, B. Qiao, and Q. Lin, "Towards intelligent incident management: why we need it and how we make it," Semantic Scholar, 2020, doi: https://-doi.org/10.1145/3368089.3417055.

[35]. [7] B. Ai, B. Li, S. Gao, J. Xu, and H. Shang, "An Intelligent Decision Algorithm for the Generation of Maritime Search and Rescue Emergency Response Plans," IEEE Access, vol. 7, pp. 155835–155850, 2019, doi: https://-doi.org/10.1109/ACCESS.2019.2949366.

[36]. [8] J. Williams, "A SANS Survey Written by Alissa Torres," 2014. Available: https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/Articles/Ch3_IR_SANSSurvey.pdf

[37]. N. M. Karie and H. S. Venter, "Taxonomy of Challenges for Digital Forensics," Journal of Forensic Sciences, vol. 60, no. 4, pp. 885–893, Jul. 2015, doi: https://-doi.org/10.1111/1556-4029.12809.

[38]. M. Pollitt, "A History of Digital Forensics," Advances in Digital Forensics VI, vol. 337, pp. 3–15, 2010, doi: https://-doi.org/10.1007/978-3-642-15506-2_1.

[39]. A. Jarrett and K. R. Choo, "The impact

of automation and artificial intelligence on digital forensics," WIREs Forensic Science, Apr. 2021, doi: https://-doi.org/10.1002/wfs2.1418.

[40]. S. Ikram and H. Malik, "Digital audio forensics using background noise," IEEE Xplore, Jul. 01, 2010. https://ieeexplore.ieee.org/abstract/document/5582981 (accessed Mar. 27, 2022).

[41]. V. R. Kebande et al., "Towards an Integrated Digital Forensic Investigation Framework for an IoT-Based Ecosystem," IEEE Xplore, Aug. 01, 2018. https://ieeexplore.ieee.org/abstract/document/8465532/

[42]. D. O. Ukwen and M. Karabatak, "Review of NLP-based Systems in Digital Forensics and Cybersecurity," 2021 9th International Symposium on Digital Forensics and Security (ISDFS), Jun. 2021, doi: https://-doi.org/10.1109/isdfs52919.2021.9486354.

[43]. S. W. Hall, A. Sakzad, and K. R. Choo, "Explainable artificial intelligence for digital forensics," WIREs Forensic Science, Jun. 2021, doi: https://-doi.org/10.1002/wfs2.1434.

[44]. N. H. Ab Rahman and K.-K. R. Choo, "A survey of information security incident handling in the cloud," Computers & Security, vol. 49, pp. 45–69, Mar. 2015, doi: https://-doi.org/10.1016/j.cose.2014.11.006.

[45]. B. B. Meshram and D. N. Patil, "Digital Forensic Analysis of Hard Disk for Evidence Collection," International Journal of Cyber-Security and Digital Forensics (IJCSDF), vol. 7, no. 2, pp. 100–110, 2018, Accessed: May 24, 2023. [Online]. Available: http://sdiwc.net/digital-library/digital-forensic-analysis-of-hard-disk-for-evidence-collection

[46]. D. Povar and V. K. Bhadran, "Forensic Data Carving," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 137–148, 2011, doi: https://-doi.org/10.1007/978-3-642-19513-6_12.

[47]. A. Pal and N. Memon, "The evolution of file carving," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 59–71, Mar. 2009, doi: https://-doi.org/10.1109/msp.2008.931081.

[48]. M. Meyers and M. Rogers, "Computer Forensics: The Need for Standardization and Certification," International Journal of Digital Evidence Fall, vol. 3, no. 2, 2004, Available: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf

[49]. G. Cantrell, "Teaching Data Carving Using The Real World Problem of Text Message Extraction From Unstructured Mobile Device Data Dumps," The Journal of Digital Forensics, Security and Law, 2019, doi: https://-doi.org/10.15394/jdfsl.2019.1603.

[50]. K. Zhang and A. B. Aslan, "AI technologies for education: Recent research & future directions," Computers and Education: Artificial Intelligence, vol. 2, p. 100025, 2021, doi: https://-doi.org/10.1016/j.caeai.2021.100025.