International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

AI for Continuous Security in DevOps (DevSecOps): Integrating Machine Learning into CI/CD Pipelines

Nagateja Alugunuri

Submitted: 01/11/2024 **Revised:** 05/12/2024 **Accepted:** 16/12/2024

Abstract: The paper determines the impact that Artificial Intelligence (AI) has on security practises in DevSecOps environments when integrated into the Continuous Integration Continuous Delivery (CI/CD) pipelines. The research explores how AI-powered instruments combined with machine learning algorithms can foster security testing and improve vulnerability detection and automatic remediation, deliver threat intelligence and maintain DevSecOps speed performance. The research shows that AI helps improve security vulnerability detection and resolution because it enables faster identification and accuracy so that unknowns can be solved immediately. There are still challenges in developing AI models and system integration complexities that an organisation has no control over. Human security tests of AI systems are necessary to help the regular development of improvements in AI models. Organisations must create AI investment plans by finding sensible artificial intelligence tools and establishing open and ethical regulations. Research reveals that AI holds important value for DevSecOps security development, though complete assessment of both procedural aspects and artificial intelligence algorithms remains necessary during installation. Future research must tackle current limitations before researchers can create next-generation artificial intelligence models to combat rising cybersecurity threats.

Keywords: *Artificial Intelligence, DevSecOps, instruments, remediation.*

Chapter 1: Introduction

1.1 Background of DevOps and DevSecOps

DevOps is a development method that involves the development personnel and IT operations teams in a way that results in better outcomes [1]. Automating development and operations facilitates speed for the delivery of better quality results and, thus, better efficiency in the software lifecycle [2]. Continuous integration (CI), continuous delivery (CD) and continual testing are DevOps principles that allow organisations to rapidly (but) reliably deploy software updates. Security gets relegated to afterthought if it is not built into initial work, the main focus being relentless speed and continuous development that must be what happens [3]. DevSecOps is a solution based on extending DevOps principles that integrates security functions at each stage in the development process. Security practises are programmed to function inside CI/CD pipelines, allowing developers to handle vulnerabilities continuously instead of waiting until after deployment [4]. DevSecOps seeks to accomplish an "early security shift" since security functions best when implemented during development before its final stages [5]. The move towards early security identification is necessary because security breaches are increasingly hard to manage and expensive to solve during development when detection and mitigation happen late. Secure measures must transform because DevOps speed up software deployment cycles that constantly stream new code and deployments through production environments. DevSecOps fortifies early security detection capabilities when testing is built into each phase of the CI/CD pipeline, which leads to savings in the cost of avoided production environment vulnerabilities [6].

1.2 Relevance of AI in DevSecOps

Security enhancement in DevOps can greatly benefit from the emerging role of artificial intelligence (AI) and machine learning (ML) technologies [7]. Artificial intelligence takes just a little time to examine large amounts of data quickly and precisely to gain patterns beyond human ability to analyse speed. By utilising AI and ML technology, AI and ML technology are used to

Principal DevOps Engineer, Raleigh, NC, USA

nagateja4224@gmail.com

continuously automate key security features like vulnerability scanning and penetration tests with code review stream protection in CI/CD pipelines [8]. The security tools it provides to teams are made possible by AI's ability to conduct continuous real-time threat detection and security testing without human intervention as applications become more complex and massive.

There is also a use beyond the typical automation tasks of AI in DevSecOps. AI security platforms scan the code for vulnerability, track activities for suspicious activities, and later, find vulnerable points in upcoming software versions [9]. Machine learning algorithms can utilise the ability to learn from past data to improve their identification ability and, therefore, can quickly and accurately detect current security risks as they occur [10]. Artificial Intelligence improves threat intelligence by consuming external threat information from the feeds, internal logs and the Dark Web, supporting security teams in taking preventative action instead of waiting for the threat to occur.

1.3 Research Problem and Objectives

Organisations that try to maintain security without negatively affecting the tempo of development find that DevOps security integration is still an exploit [11]. Security protocols that worked traditionally are struggling to react to the speed of DevOps speed, which leaves security holes allowing production platforms to be breached. Although the CI/CD pipeline runs against DevOps benefits, it slows down with manual security checks and vulnerability scans as a process. Artificial intelligence enhances security operations via automated security testing to detect vulnerabilities in advance and achieve accelerated threat response time over manual methods [12]. Integration of AI alongside DevSecOps tools and the need for the latter to have large datasets for AI model training are the issues with the implementation of AI. Assessment of AI's potential as a solution to DevSecOps security problems is made in this investigation to validate whether or not AI can be used to enhance the practice of security [13]. Therefore, this research studies how AI technology performs security-related automated functions such as vulnerability detection, penetration testing, and real-time CI/CD process remediation. This research will explain how fast AI-based tools can find vulnerabilities and how AI aids both in speeding up software application security and the operational speed in DevOps.

1.4 Aim and Research Objectives

1.4.1 Aim

The research aims to study how AI and machine learning technologies can be used in DevSecOps and how they can be utilised within the CI/CD ecosystem for continuous security testing, automatic vulnerability identification, and system remediation.

1.4.2 Research Objectives

- To assess the current state of DevSecOps practises in keeping CI/CD pipelines secured.
- To study the possibility of automating and optimising security testing in DevSecOps environments with the help of AI and ML technologies.
- To analyse the role of AI in detecting and remediating vulnerabilities in real-time during the CI/CD cycle.
- To evaluate the impact of AI on improving security efficiency and speed without compromising on quality.
- To identify potential limitations of AI in DevSecOps and propose recommendations for overcoming these challenges.

1.5 Structure of the Paper

This paper is structured as follows:

- **Chapter 1: Introduction** – The chapter explains the research paper's main subject, discusses DevOps concepts alongside DevSecOps features, and demonstrates how AI helps enhance framework security. Additionally, the paper introduces its research question and organisational structure along with its main points.
- **Chapter 2: Literature Review** – This chapter provides a detailed review of the existing literature on DevOps, DevSecOps, AI, and machine learning applications in cybersecurity. It examines AI-led security instrumentation tools and shows the rewards of applying AI to DevSecOps and the obstacles to its implementation.
- **Chapter 3: Methodology** – This chapter reveals the research methodology, which relies on secondary data collection to evaluate the effect of AI on DevSecOps practises. The chapter outlines

the approach for analysing data to fulfil the research objectives.

- **Chapter 4: Results and Findings** – The secondary research findings will be presented, along with a synthesis of the best AI-driven security practices for DevSecOps and their effects on CI/CD pipeline security.

- **Chapter 5: Conclusion and Recommendations** – The conclusion chapter presents an overview of the research outcomes with specific implementation advice about incorporating AI solutions in DevSecOps systems. Future research initiatives for AI-driven security development will be proposed together with relevant investigation domains.

Chapter 2: Literature Review

2.1 DevOps and Security in CI/CD Pipelines

DevOps connects development and IT operations teams through automation to boost software delivery performance and cooperation [14]. Its core principles are continuous integration (CI), continuous delivery (CD), and continuous testing. These principles facilitate developers' conducting automated code testing and deployment at regular intervals, which accelerates reliable software delivery [15]. A fundamental requirement within DevOps exists in the CI/CD pipeline, which programmed applications for integration, testing, and deployment [16]. The pipeline enables developers to send continuous updates essential for contemporary software production. DevOps has achieved impressive speeds during software delivery through its efficiency, but security often becomes a trailing issue compared to the parallel development pace. Standard security practises typically handle security checks during the development's late stages, but this approach fails in DevOps's rapid operation environment. Security vulnerabilities develop due to delayed testing, allowing them to persist until system deployment without fixations, and thus exposing the production environment to breaches [17]. DevSecOps is the solution enabling security practices to run throughout every stage of the CI/CD pipeline [18]. DevSecOps enables developers to work security into each developmental phase so security issues can get resolved before they reach late development stages [19]. Implementing DevSecOps faces the difficulty of integrating quick software delivery with complete security measures. The traditional manual resource-intensive security tools of the past do not fit with DevOps speed requirements, thus creating workflow delays in the CI/CD process. Security tools that operate automatically enable testing at development's beginning stages, thus keeping security intact and development speed [20].

2.2 AI and Machine Learning in Cybersecurity

The field of cybersecurity highly depends on Artificial Intelligence (AI) and Machine Learning (ML) technologies as their importance increases daily [21]. Computers use AI techniques to execute tasks which human intelligence would have handled before through processes like pattern detection and decision-making. ML acts as an AI subset, which allows systems to automatically learn from data to enhance themselves without written code [22]. AI and ML are highly beneficial for cybersecurity work because they execute regular operations automatically, detect data patterns, and foresee dangers with enhanced effectiveness beyond standard approaches. AI and ML have been adopted by DevSecOps systems to conduct ongoing security testing, identify flaws, and collect threat data [23]. These modern technologies surpass traditional methods by detecting security dangers in advance through their ability to study big volumes of suspicious data patterns. AI algorithms process system logs alongside network traffic data and application code to detect organisational weaknesses and identify abnormal system operations through this method which speeds up security incident management [24]. AI utilises learned historical data to modify security measures by adjusting its predictive models to prevent future security breaches.

The history of AI development for cybersecurity has progressed toward becoming more complex and automated. AI was used to automate virus scanning and anomaly detection but was the main function during its initial deployment in the field. Current advances in machine learning technology have allowed AI systems to detect real-time vulnerabilities while preventing potential threats and executing intelligent remediation tasks [25]. AI-driven cybersecurity solutions now offer the automatic performance of new attack vector identification and vulnerability patching with the additional capability to forecast locations of expected cyber threats, thus becoming vital

components for modern DevSecOps security solutions.

2.3 AI for Continuous Security Testing

Security tests should operate unsustainably within DevOps environments to verify software integrity and protect against security threats. Code changes in CI/CD pipelines require modern security testing beyond traditional methods since they depend on periodic assessments and manual processes. AI-driven security testing tools allow organisations to check code and applications while operating in real-time so security threats receive immediate detection and resolution [26]. Tools such as SonarQube with AI plugins, Checkmarx, and GitHub Advanced Security integrate with CI/CD platforms to perform real-time static and dynamic analysis. These tools provide dashboards that highlight issues as developers commit code, enabling shift-left testing. The main value of AI for continuous security testing consists of its automated task execution capability, which identifies vulnerabilities throughout all stages of the CI/CD pipeline. Figure 1 demonstrates a typical CI/CD ecosystem integrated with popular DevSecOps tools like Jenkins, GitLab, and GitHub, where AI-driven static and dynamic security testing can be seamlessly embedded.

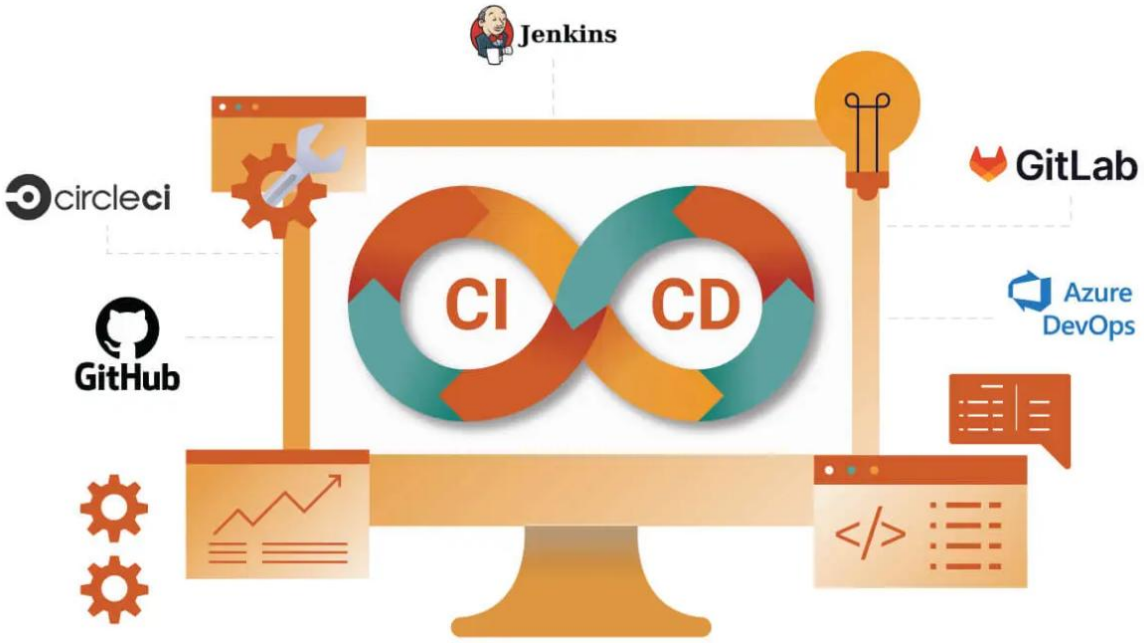

Figure 1 Example of a CI/CD pipeline integrating multiple DevOps platforms used for AI-enhanced security testing.

Machine learning tools incorporate programmes that simultaneously detect security vulnerabilities in code, including SQL injection and system configuration compliance against security standards [27]. Developments in automated software admit threats faster with minimum human involvement, which helps teams handle additional tasks while keeping security under constant monitoring. Security testing benefits from AI capabilities because these systems can apply security customisation and approaches to support different project requirements. The testing process operates through machine learning algorithms which leverage previous data to create custom adjustments according to the one-of-a-kind characteristics of current development applications [28]. The custom design of AI tools makes them perform better in identifying application weaknesses, which results in enhanced precision and speed of security evaluation.

2.4 Vulnerability Detection and AI Integration

The critical security process of vulnerability detection becomes more efficient through AI as it establishes a prominent role in automating this process. The current vulnerability detection tools use predefined signatures to identify known threats [29]. Some capabilities of this methodology decrease because it falls short of detecting zero-day vulnerabilities and advanced attacks, which

researchers have not yet confirmed. Artificial intelligence detects unknown security vulnerabilities by following machine learning approaches to find patterns in collected data showing potential risks. AI-driven security software technologies recognise security threats in large data collections from code to network data to system logs better and faster than traditional approaches [30]. Machine learning models show particular value in this case since they use historical datasets to adjust their responses to new attack methods and mutate system weaknesses. Tools like Snyk, Tenable.io, and Aqua Trivy use AI/ML to identify known and unknown vulnerabilities in dependencies, container images, and Infrastructure as Code (IaC). These tools connect with platforms such as Jenkins, GitLab, and CircleCI to automate detection as part of the pipeline flow. The system's security posture improves through continuously accurate and efficient model performance over time. Organisations achieve vulnerability detection speed and prevention of significant damage by integrating AI into their processes [31]. Security teams can direct their vulnerability response effort using AI to determine the most significant hazards for fast remediation.

2.5 AI for Automated Remediation and Threat Intelligence

After vulnerabilities become detectable, organisations should act swiftly to correct them to safeguard against exploitation. Security threat remediation automation by AI reduces repair time and human intervention required to fix vulnerabilities [32]. Remediation processes traditionally demand hand-based human interaction, but these procedures introduce human operators who can make mistakes and prolong the remediation process. AI-powered remediation tools like Tenable Nessus, Deepfactor, and Microsoft Defender for DevOps can auto-apply fixes or raise automated tickets in tools like Jira. These solutions integrate with code repositories and build pipelines to reduce manual patch management. Real-time automatic fix implementations through AI-driven remediation tools include vulnerability patching and system configuration updating. AI serves dual functions in threat intelligence operations since it requires this technology for data collection and threat analysis processes. Organisations obtain potential threat understanding through threat intelligence that collects data from external threat feeds, internal logs, and network traffic sources [33]. By receiving and analysing data collections, AI systems generate analytical information about upcoming risks, enabling protective security responses before reactive measures become necessary. Through AI automation of remediation functions and better threat intelligence acquisition, organisations can constantly navigate ahead of attackers while improving their security system [34]. Real-time threat monitoring functions of AI allow vulnerabilities to receive immediate attention that avoids exploitation.

2.6 Recent Developments in AI-Driven DevSecOps

Artificial intelligence security solutions that have appeared in recent times significantly enhance DevSecOps operations through penetration testing, security scanning, and threat intelligence collection functions [35]. AI tools, through penetration testing, execute fake cyberattacks against software applications, thus finding weaknesses that attackers could exploit beforehand. The technology operates autonomously to identify security system vulnerabilities and generate recommended solutions that simplify the testing process for security. Continuous security monitoring tools that check for application vulnerabilities have emerged from AI technology while operating without impacting the CI/CD pipeline [36]. The tools automatically check the development code when written to find security flaws that engineers need to repair during the early development stages. AI security scanners help teams because these tools decide which vulnerabilities require immediate attention by determining their severity levels. The sophistication of artificial intelligence threat intelligence tools continues to increase because they deliver live threat detections to security teams [37]. AI utilises diverse source data to reveal upcoming security attack vectors and forecast potential vulnerability creation areas, allowing organisations better protection against future threats.

Chapter 3: Methodology

3.1 Research Design

The investigation applied secondary research techniques to determine the implementation of Artificial Intelligence (AI) for DevSecOps operations within CI/CD pipelines. Secondary

research methodology utilised existing literature, case studies, and published materials to help researchers enhance knowledge already developed around the field [38]. Using secondary data allowed for a comprehensive review of AI adoption in DevSecOps through secondary research before any primary data collection operations started. The secondary data collection method gave substantial benefits by offering valuable information from established sources for analytical purposes [39].

The research used specific selection standards to assess the appropriate literature and case studies according to their relevance, credibility, and timeliness of the content. The research drew information from peer-reviewed academic journals, and both research papers were presented at reputable conferences and industry reports prepared by recognised organisations and relevant online resources. The research employed these sources because they conform to the most current and reliable information standards. The selected literature sources provided research on both positive and negative aspects of integrating AI into DevSecOps practises [40]. The analysed studies presented real situations of AI implementation in DevSecOps practices and theoretical structures, which helped understand AI's effects on continuous security evaluations, automated vulnerability recognition, and remedial actions.

3.2 Data Collection and Sources

The main data source for this research originated from secondary documents that included academic journals, research papers, and industry reports. Academic journals that went through the peer review process established the foundation of this research by delivering evidence-based findings regarding AI implementation in DevSecOps. Research papers from recognised conferences provided the framework for recent field developments and engineering applications regarding AI in CI/CD pipeline integration [41]. Information from white papers and industry reports of major cybersecurity companies IBM, Cisco and McAfee added valuable content to this research. These sources delivered functional knowledge about actual implementations of AI-enabled tools that occurred within DevSecOps environments. A review of online resources, including technical documentation and AI and cybersecurity expert articles, delivered additional information about industry usage of AI-based solutions [42]. Such sources provided theoretical elements and practical tools that delivered an all-encompassing view of the subject matter.

3.3 Data Analysis Approach

An analysis of the gathered responses employed thematic methods to search for typical integrations between AI technology and DevSecOps implementations. This analytical approach succeeded in evaluating AI effects specifically within the different aspects of DevSecOps, including security testing, vulnerability detection, and threat remediation. Security testing improvements in CI/CD pipelines through AI techniques were arranged into categories as one of the research considerations. What difficulties did organisations face when deploying AI tools during DevSecOps operations? The analysis of each segment finalised conclusions utilising the evidence from corresponding literature [43].

A second analysis method included a comparison of the effectiveness of the AI tool in different DevSecOps environments. A comparison between real-world AI implementations from case studies and industry reports generated detailed information about their deployments. The research focuses on successful practices and organisation-level obstacles for AI pipeline integration within DevSecOps environments. Analysing this collected information allowed the study to comprehensively view AI's effects on DevSecOps practises with its security benefit potential for CI/CD pipelines [44].

3.4 Limitations of the Study

The study obtained valuable knowledge from secondary research, although a dependency on existing literature created natural boundaries. The study was substantially limited because the reviewed sources might display biased information. Researchers used studies that presented incomplete information due to their specific goals and organisational targets. AI-focused industry reports generally published findings about AI tools with positive descriptions yet avoided disclosing operational hurdles. Academic papers about theoretical aspects failed to address implementation-related challenges [45]. The danger of using obsolete information presented itself as another research constraint. AI technology had quick advancements, which caused some studies to lose relevance regarding modern developments and trends in security practices that use AI. The

available information may have described an unsatisfactory state of AI implementation within DevSecOps. The research used recent literature from the past five years to maintain relevance [44]. Secondary research provided quick results, although it failed to fully represent the practical issues organisations faced when adopting AI for their DevSecOps pipelines. The method-based research limitations did not prevent researchers from generating a fundamental framework for understanding AI integration with DevSecOps. The study examined numerous reliable sources to create a complete understanding of how AI brings alterations to security practices throughout CI/CD pipelines along with DevSecOps environments.

Chapter 4: Results and Findings

4.1 Overview of AI Integration in DevSecOps

DevSecOps environments now use Artificial Intelligence (AI) integration as the backbone of a transformative development that yields multiple essential benefits while encountering specific obstacles. Adopting AI-powered instruments and machine learning (ML) algorithms has shaped multiple DevSecOps functions through continuous security testing operations, vulnerability identification, automated trouble rectification methods and threat analytics [46]. Testing has demonstrated that AI technology enables improved security practices in CI/CD pipelines while supporting software delivery speed and efficiency.

Integrating AI within DevSecOps operations brought about fundamental upgrades to development security testing practices. Through its advanced tools, artificial intelligence allows seamless execution of vulnerability detection and penetration testing along with real-time security surveillance capabilities. Organisations shifting towards advanced development practises with agile and automated methods require continuous automated security testing, which AI delivers by delivering rapid, precise security evaluations [47]. Implementing automation techniques in security assessment procedures enables organisations to decrease response times and eliminate human mistakes in detecting vulnerabilities that affect CI/CD pipeline security in agile development settings [48].

However, AI implementation in DevSecOps brings multiple obstacles to its adoption. Integrating AI into current DevSecOps pipelines requires organisations to invest considerable time and resources. AI model training presents organisational challenges because organisations struggle to educate their models and ensure they follow current security protocols and adjust for shifting threats. AI models require ongoing updates and consistent training with fresh security data to monitor evolving threats and defence strategies. However, too much customisation stands in the way of AI tool integration when organisations add them to existing security frameworks [49]. Organisations should thoroughly investigate the trade-offs between AI advantages and implementation difficulties when adopting this technology. The researched findings demonstrate AI capability for boosting security operations and automation in DevSecOps frameworks.

4.2 AI for Continuous Security Testing in CI/CD Pipelines

DevSecOps benefits significantly from continuous security testing, demonstrating the highest impact of Artificial Intelligence (AI) [18]. The conventional security testing methods through static and dynamic analysis are time-intensive and inadequate for early vulnerability identification during development stages. The security assessment process through these methods occurs only during specific development phases, making monitoring code security constantly challenging throughout the development cycle. AI solves security testing challenges by enabling automatic continuous pipeline testing throughout the CI/CD process. AI-based code scanning technology performs checks during every development phase to discover security issues immediately and support efficient problem resolution [48]. One example is GitHub Copilot Security which provides inline vulnerability warnings. OWASP ZAP's automation framework allows DAST integration with Jenkins pipelines. Also, Fortify provides AI-assisted prioritisation of scan results based on severity and exploitability.

Research data showed that AI security testing tools outperformed traditional systems in vulnerability identification effectiveness. Machine learning models applied pattern analysis on code to find security vulnerabilities in software code [31]. Over time, these tools have gained better capabilities to identify fresh vulnerabilities and unknown threats by studying old vulnerability reports [49]. Security checks within CI/CD pipelines enable organisations

to identify vulnerabilities, thus lowering the chances of production interruptions, which require costly remediation after new software reaches deployment. Security testing powered by artificial intelligence provides many benefits to organisations, but several constraints remain to consider. Even though AI detection tools analysed numerous vulnerabilities, they still sometimes made errors. The detection process still produced incorrect positive and negative results, so human monitoring was necessary under specific conditions. AI models did not possess enough capability to recognise zero-day vulnerabilities unless scientists trained and refined the systems to identify them [29]. Organisations needed to maintain ongoing upgrades for their AI-based security testing tools to remain competent against developing threats [50]. DevSecOps security testing benefits from AI technology, but humans must continue managerial roles, and their tools need regular maintenance updates. Implementing security metrics within CI/CD pipelines provides organisations with noticeable advancements in both productivity and speed regarding security vulnerability detections and remediation processes.

4.3 AI-Driven Vulnerability Detection

Based on this research, AI systems play a fundamental part in vulnerability discovery operations of CI/CD pipelines. Signature-based tools are the conventional approach for vulnerability detection, yet they only recognise known vulnerabilities. AI provides advanced vulnerability detection capabilities via updated methods for identifying new and previously undocumented security threats. The detection of new vulnerabilities becomes critical for DevSecOps because code development remains constant, and threats might appear at any time during this period [51]. Research demonstrated that AI-based security tools detected security vulnerabilities at a higher speed than conventional testing systems. Examples include WhiteSource Bolt, which flags known vulnerabilities in dependencies using natural language processing (NLP) techniques, and Clair, an open-source project for static analysis of container images. The machine learning algorithms analysed big code bases in concert with security logs using pattern recognition to discover potential vulnerabilities in the data. The combination of AI technology showed outstanding effectiveness in detecting hard-to-spot areas of weak code, like logical problems and unsafe programming practices that manual testing often misses [52]. Figure 2 shows how AI-enhanced bug triaging techniques help automate the detection, categorisation, and assignment of vulnerabilities to developers, thereby improving efficiency in DevSecOps environments.

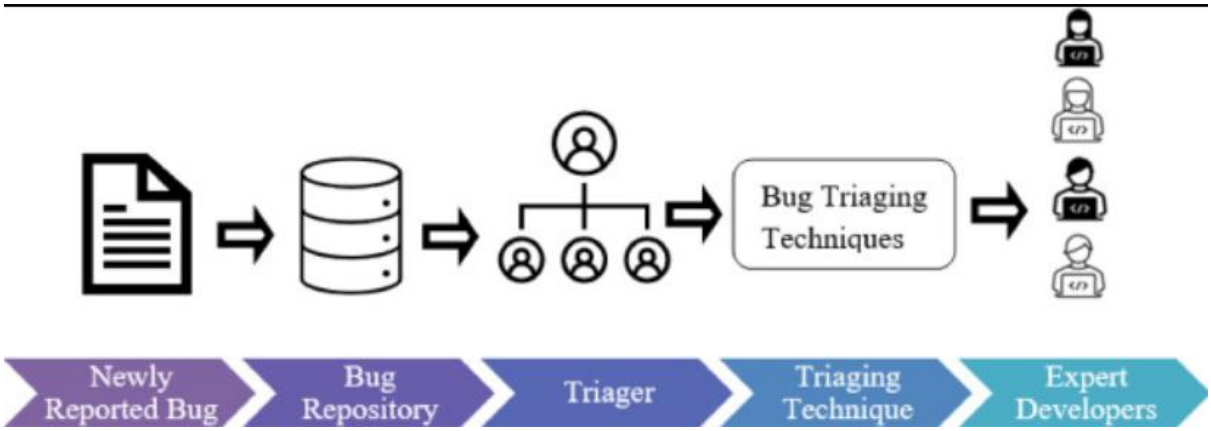

Figure 2 AI-supported bug triaging pipeline that automates detection and assignment in security operations.

According to Pahune and Akhtar [53], AI-driven vulnerability detection tools still face multiple associated difficulties. These tools achieved their results based directly on the quality level of the data that trained their models. Some implementations of vulnerability detection failed due to the use of underprepared or biased training data. Several organisations found implementing

AI-driven detection technology throughout their existing DevSecOps methodology challenging because these tools needed substantial customisation and optimisation to work properly within their specified environments [53].

4.4 Automated Remediation with AI in DevSecOps

AI's potential to automate the remediation of security vulnerabilities was one of the most significant findings of this study. The traditional security team in DevSecOps suffered from excessive vulnerability load because they had to fix each issue manually. The advantage of AI-driven remediation tools enabled automated system security through vulnerability patching while establishing secure system configurations and deploying security policies independent of human operators [54]. The implemented automation decreased the vulnerability detection to remediation period, thus improving the organisational security posture. According to the results, organisations implementing AI-driven remediation tools substantially enhanced their security operations. AI tools automatically implemented patches instantaneously after detection, thus blocking attacks before any damage could happen [55]. The AI-driven vulnerability remediation process involves a continuous loop of identifying, prioritising, fixing, and monitoring vulnerabilities across CI/CD pipelines. Figure 3 illustrates this cyclical process. For instance, GitGuardian not only detects leaked secrets but also initiates automated revocation processes. Automox and Chef Automate use AI to suggest and implement security patches without developer input. AI systems predict upcoming security vulnerabilities by analysing past events, enabling organisations to take preventive security actions before failure points emerge.

Figure 3 AI-driven vulnerability remediation cycle – Find, Prioritise, Fix, and Monitor.

According to the research findings, several issues emerged from using automated remediation systems. Automation's speed and efficiency enhancements in remediation tactics introduced a parallel issue because organisations became dependent on AI tools that occasionally produced improper or inadequate patch solutions. Organisations have pointed out the insufficient visibility within AI-driven remediation procedures as a critical issue because it complicates monitoring AI tool activities and maintaining compliance with security standards [56].

4.5 AI and Threat Intelligence

A major aspect of this research analysed AI's role in enhancing threat intelligence operations within DevSecOps frameworks. Organisations use threat intelligence to analyse information collected from different sources to instantly detect and respond to security threats. The analysis of major data sets, including internal records, external threat feeds, and network traffic, has experienced dramatic improvement through AI automation [57]. AI threat intelligence systems analyse data patterns to recognise developing threats from which security breaches normally form. Platforms like IBM QRadar, Splunk, and Recorded Future use AI to

correlate logs, identify anomaly patterns, and predict potential exploit paths based on historical incidents. The research data showed that AI threat intelligence tools provided quicker detections of developing threats than conventional security systems. Research shows that machine learning models use historical data and trends to discover new attack entry points while making threat forecasts [58]. These tools could collect data from multiple source platforms, which generated an extensive threat overview for security teams. Organisations achieved better threat response and defence capabilities by implementing AI systems in their threat intelligence operations.

The implementation of AI systems for threat intelligence operations, however, has evolved, as presented by the research. From the combinations of quality and diverse training data, these AI-driven threat intelligence tools reached their highest level of effectiveness. When the data used was not enough, it would generate both threats undetected and false prediction results [59]. Imposing AI-related tools became hard for organisations due to the need for complete customisation and expertise in (AI) tools [60].

4.6 Summary of Key Findings

Integration of AI in DevSecOps environments yields many positive changes in security testing procedures, vulnerability detection, remediation, and threat data gathering. These tools help organisations detect and fix security vulnerabilities through AI-driven tools that are precise and fast to advance DevSecOps' operational speed. Automated security testing allows organisations to benefit substantially by using AI to deliver better vulnerability detection and more efficient, proactive threat intelligence. There are multiple obstacles organisations face when adopting AI. The continuation of model training is a key challenge, along with the fact that the integration of AI tools into a DevSecOps workflow comes at an additional cost. In addition, the danger of using the AI model is questionable. While it is and can be faced with many obstacles, the indispensability of AI as an element that makes security methods inside DevSecOps better can be established. Research findings prove that AI has very good capabilities in advancing security practises with support for the DevSecOps environment. The successful implementation would be with a comprehensive approach, with care to study selection, with data quality enhancement and procedure optimisation. However, the resolution of the observed study difficulties must be worked on in future investigations, which involve AI model development for adaptable performance in the evolving cybersecurity environment.

Chapter 5: Conclusion and Recommendations

5.1 Conclusion

The research studied the effects of AI-based technology applications in DevSecOps as being brought into play in affecting continuous security test continuity vulnerability recognition, automated fix on conditions, and threat knowledge. Both security vulnerability detection speed and accuracy of AI-driven tools are exceptionally good, enabling organisations to handle threats from an early development phase without impacting the operational speed of DevSecOps. AI has steadily improved the efficiency of security systems by performing live vulnerability discovery so that organisations can remain proactive towards their CI/CD infrastructure’s robust security. The adoption of AI introduces numerous challenges to DevSecOps operation, due to which the organisations cannot go on with the model training periodically and face difficulties while integrating AI tools as it is into the existing processes. As organisations struggle with AI tool dependency vulnerability and the limit of identifying blind complex or completely new security threats, implementing the same must be managed wisely. AI favours DevSecOps practice through risk mitigation during fast software delivery and ongoing development operations. Artificial intelligence has major transformative potential in DevSecOps process security procedures. AI technological development continues to grow in DevSecOps security solutions to be able to tackle more complex threats. It will be easier to integrate AI development with DevSecOps practises to speed up the development cycles with higher security and efficiency.

5.2 Recommendations for Practice

For organisations to gain the maximum advantage of Devsecops applications, they must integrate the methodology. Based on these practical recommendations, it is possible to manage the AI implementation in DevSecOps in the same way as DevSecOps processes.

1. **Prioritise AI Tool Selection**: AI security tools must be evaluated in a processive way to ensure that an organisation will always meet its particular infrastructure and needs. To address new security threats, organisations need to pick security tools that are connected easily to their DevSecOps pipelines that automatically update with system updates. Machine learning capabilities in security solutions must be bought, so security organisations have to continuously buy in order to keep up with the changing threats.

2. **Invest in Continuous Model Training**: The best AI security tool requires continuous model training operations to be developed by organisations. AI models need to deal with a constant flow of new information in terms of the number of entities, occurrences of vulnerabilities, relations between vulnerabilities, and characteristics of vulnerabilities. In order to continuously detect new security risks, the AI models have to be updated with the most recent information about the entities and vulnerabilities. The system must operate within a constant feedback loop to continuously learn from real attacks, thereby increasing its ability to detect them over time.

3. **Ensure Human Oversight and Collaboration**: To secure with AI technology, one has to recognise that computer systems cannot stop all security threats. Security staff must have human oversight to examine AI-based scan outcomes, clear incorrect security alerts, and then make judgments in terms of risk in the context of understanding particular threats from experience. AI tools will be enabled to learn more capable progressively, while security experts working with AI tools can deploy the best security practices.

4. **Focus on Integration**: Preparing AI is an exercise that requires a lot of work, from the details to the coordination of the whole organisation team. Security teams must work closely with a lot of the departments dealing with IT operations development and security for the success of the adoption of AI-based security solutions into operational routines. A structured integration plan allows security testing problems to be resolved and an organised security assessment process to be developed. Tool orchestration platforms like Torus, Terraform with Sentinel policies, and AWS CodePipeline support the coordinated integration of AI tools across security, development, and operations teams.

5. **Address Ethical and Transparency Concerns**: As AI tools become more autonomous, organisations must ensure they are undertaking the ethical nature and transparency of systems. If the organisation relies on artificial intelligence in security operations, these should be backed with specific policies for watching and auditing AI system decisions. When the process by which they decide is open, and people can see it, AI security systems are safe to use.

5.3 Suggestions for Future Research

Based on the conclusions of this study, additional work in AI and DevSecOps should continue to grow in numerous directions. Based on the future investigation recommendations these core aspects have been identified that require further investigation.

1. **Emerging AI Technologies and Their Impact**: The continuous technological progress of deep learning and reinforcement learning gives rise to these growing AI strategies, which is why these applications have started to exploit them in the cybersecurity area. On the other hand, analysis is needed to develop security improvement strategies for new AI techniques based on anomaly identification and future threat prediction methods in frameworks of DevSecOps.

2. **AI in Threat Intelligence Gathering**: Although artificial intelligence is currently actively developing threat intelligence, it has yet to reach a high level. There is a need for research to analyse how well AI can carry out the collection of threat intelligence data from different information sources, including social media and dark web surveillance, as well as internal monitoring logs. The systems for future threat prediction can be developed using AI-based methods to forecast future threats on the basis of historical data.

3. **Human-AI Collaboration in DevSecOps**: AI is a strong and ideal cybersecurity tool which depends on human operators for proper execution. For instance, to figure out how AI can strengthen security professional functions instead of eliminating them, one needs to study optimal ideas of AI-human interaction. Optimal human supervisory methods form the research to strike the required balance between automated processes and

human involvement, and this research must establish it.

4. **AI in Security Automation beyond Vulnerability Detection**: The research investigated how AI can be utilised in the realm of security testing and how it is able to discover vulnerabilities and recover from them. Security automation through artificial intelligence is a useful tool both in the testing and remediating activities, but there is also great potential for accelerators in the areas of incident response and post-incident assessment. Potential implementations of artificial intelligence in security operations should be analysed by future studies in light of improving relevant performance-related metrics.

5. **Overcoming Barriers to AI Adoption in DevSecOps**: DevSecOps organisation's resistance to AI deployment is due to the barriers to implementation, such as resource demands, expense, and system complexity. The research should study the obstacles to organisations accepting AI implementations and whether systems that could make this process easier could be created. DevSecOps projects that have successfully implemented AI should be studied by researchers, and organisations, where the implementation of DevSecOps projects went wrong, should be used to obtain experiences.

Thus, AI is a digital service that is a significant advancement and upgrading trend in the domain of CI/CD infrastructure, and better security practices. Perpetual research development will need to improve AI models to be successfully integrated with security workflows to keep this approach effective in combating creeping cybersecurity threats. Through the development of AI, DevSecOps operations will become stronger and will be able to bring more secure, efficient, and agile development cycles.

References

[1] Yarlagadda, R.T., 2019. How DevOps enhances the software dévelopment quality. International Journal of Creative Research Thoughts (IJCRT), ISSN, pp.2320-2882.

[2] Manchana, R., 2021. The DevOps Automation Imperative: Enhancing Software Lifecycle Efficiency and Collaboration. European Journal of Advances in Engineering and Technology, 8(7), pp.100-112.

[3] Ugwueze, V.U. and Chukwunweike, J.N., 2024. Continuous integration and deployment strategies for streamlined DevOps in software engineering and application delivery. Int J Comput Appl Technol Res, 14(1), pp.1-24.

[4] Owoade, S.J., Uzoka, A., Akerele, J.I. and Ojukwu, P.U., 2024. Cloud-based compliance and data security solutions in financial applications using CI/CD pipelines. *World Journal of Engineering and Technology Research*, *8*(2), pp.152-169.

[5] Butter, K., 2024. Shifting Security Left: A Qualitative Study (Doctoral dissertation, Capella University).

[6] D'Onofrio, D.S., Fusco, M.L. and Zhong, H., 2023. *CI/CD Pipeline and DevSecOps Integration for Security and Load Testing* (No. SAND-2023-08255). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

[7] Tatineni, S., 2024. *Integrating Artificial Intelligence with DevOps: Advanced Techniques, Predictive Analytics, and Automation for Real-Time Optimization and Security in Modern Software Development*. Libertatem Media Private Limited.

[8] Kokku, R., Revolutionizing DevOps Security: AI and ML-Enabled Automated Testing Approaches.

[9] Kyler, T., 2024. AI-Driven DevSecOps: Integrating Security into Continuous Integration and Deployment Pipelines.

[10] Bahaa, A., Abdelaziz, A., Sayed, A., Elfangary, L. and Fahmy, H., 2021. Monitoring real time security attacks for IoT systems using DevSecOps: a systematic literature review. *Information*, *12*(4), p.154.

[11] El Aouni, F., Moumane, K., Idri, A., Najib, M. and Jan, S.U., 2024. A systematic literature review on Agile, Cloud, and DevOps integration: Challenges, benefits. *Information and Software Technology*, p.107569.

[12] Vadde, B.C. and Munagandla, V.B., 2023. Security-First DevOps: Integrating AI for

Real-Time Threat Detection in CI/CD Pipelines. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(03), pp.423-433.

[13] Fu, M., Pasuksmit, J. and Tantithamthavorn, C., 2024. Ai for devsecops: A landscape and future opportunities. *ACM Transactions on Software Engineering and Methodology*.

[14] Moeez, M., Mahmood, R., Asif, H., Iqbal, M.W., Hamid, K., Ali, U. and Khan, N., 2024. Comprehensive Analysis of DevOps: Integration, Automation, Collaboration, and Continuous Delivery. *Bulletin of Business and Economics (BBE)*, *13*(1).

[15] Banala, S., 2024. DevOps Essentials: Key Practices for Continuous Integration and Continuous Delivery. *International Numeric Journal of Machine Learning and Robots*, *8*(8), pp.1-14.

[16] MUSTYALA, A., 2022. CI/CD Pipelines in Kubernetes: Accelerating Software Development and Deployment. *EPH-International Journal of Science And Engineering*, *8*(3), pp.1-11.

[17] Dapshima, B.A. and Ahmad, S.K., 2024. Evaluation and Assessment of Software Security Risks and Vulnerabilities Within the Realm of Secure DevOps. *no. July*.

[18] Thota, R.C., 2024. Cloud-Native DevSecOps: Integrating Security Automation into CI/CD Pipelines. *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH AND CREATIVE TECHNOLOGY*, *10*(6), pp.1-19.

[19] Rajapakse, R.N., Zahedi, M., Babar, M.A. and Shen, H., 2022. Challenges and solutions when adopting DevSecOps: A systematic review. *Information and software technology*, *141*, p.106700.

[20] Rangnau, T., Buijtenen, R.V., Fransen, F. and Turkmen, F., 2020, October. Continuous security testing: A case study on integrating dynamic security testing tools in ci/cd pipelines. In *2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC)* (pp. 145-154). IEEE.

[21] Geluvaraj, B., Satwik, P.M. and Ashok Kumar, T.A., 2019. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International Conference on Computer Networks and Communication Technologies: ICCNCT 2018* (pp. 739-747). Springer Singapore.

[22] Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I. and Beloev, I., 2024. A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. *IEEe Access*, *12*, pp.12229-12256.

[23] Yulianto, S. and Ngo, G.N.C., 2024, September. Enhancing DevSecOps Pipelines with AI-Driven Threat Detection and Response. In *2024 International Conference on ICT for Smart Society (ICISS)* (pp. 1-8). IEEE.

[24] Hassan, S.K. and Ibrahim, A., 2023. The role of artificial intelligence in cyber security and incident response. *International Journal for Electronic Crime Investigation*, *7*(2).

[25] Saad, W. and Aslam, M., 2023. The Role of Artificial Intelligence in Remediation and Risk Mitigation for Cybersecurity.

[26] Myllynen, T., Kamau, E., Mustapha, S.D., Babatunde, G.O. and Collins, A., 2024. Review of advances in AI-powered monitoring and diagnostics for CI/CD pipelines. *International Journal of Multidisciplinary Research and Growth Evaluation*, *5*(1), pp.1119-1130.

[27] Nandi, S., 2024. EVALUATING THE EFFECTIVENESS OF SECURITY TESTING TOOLS IN AUTOMATED TESTING.

[28] Sarker, I.H., 2021. Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), p.160.

[29] Khan, S. and Parkinson, S., 2018. Review into state of the art of vulnerability assessment using artificial intelligence. *Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach*, pp.3-32.

[30] Prince, N.U., Faheem, M.A., Khan, O.U., Hossain, K., Alkhayyat, A., Hamdache, A. and Elmouki, I., 2024. AI-powered data-driven cybersecurity techniques: Boosting threat identification and reaction. *Nanotechnology Perceptions*, *20*, pp.332-353.

[31] Pala, S.K., Study to Develop AI Models for Early Detection of Network Vulnerabilities. *International Journal of Enhanced Research in Science, Technology & Engineering ISSN*, pp.2319-7463.

[32] Komaragiri, V.B. and Edward, A., 2022. AI-Driven Vulnerability Management and Automated Threat Mitigation. *International Journal of Scientific Research and Management (IJSRM)*, *10*(10), pp.981-998.

[33] Manda, J.K., 2024. AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations. *Available at SSRN 5003638*.

[34] Jimmy, F., 2021. Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*, pp.564-74.

[35] Allam, A.R., 2023. Enhancing Cybersecurity in Distributed Systems: DevOps Approaches for Proactive Threat Detection. *Silicon Valley Tech Review*, *2*(1), pp.54-66.

[36] Tyagi, A., 2021. Intelligent DevOps: Harnessing Artificial Intelligence to Revolutionize CI/CD Pipelines and Optimize Software Delivery Lifecycles. *Journal of Emerging Technologies and Innovative Research*, *8*, pp.367-385.

[37] Lawal, K., 2025. Real-Time Threat Intelligence: AI-Driven Automation and Response.

[38] Cui, J., 2024. The Enhancement of Software Delivery Performance through Enterprise DevSecOps and Generative Artificial Intelligence in Chinese Technology Firms. *arXiv preprint arXiv:2411.02255*.

[39] Ayidiya, M., 2023. *AI Usage in Development, Security, and Operations* (Doctoral dissertation, Walden University).

[40] Camacho, N.G., 2024. Unlocking the potential of AI/ML in DevSecOps: effective strategies and optimal practices. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), pp.106-115.

[41] Cheenepalli, J., Hastings, J.D., Ahmed, K.M. and Fenner, C., 2025. Advancing DevSecOps in SMEs: Challenges and Best Practices for Secure CI/CD Pipelines. *arXiv preprint arXiv:2503.22612*.

[42] Chittala, S., 2024. Securing DevOps Pipelines: Automating Security in DevSecOps Frameworks. *JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE)*, *12*(5), pp.31-44.

[43] Zhao, X., Clear, T. and Lal, R., 2024. Identifying the primary dimensions of DevSecOps: A multi-vocal literature review. *Journal of Systems and Software*, p.112063.

[44] Heijstek, A., 2023. *Bridging theory and practice: insights into practical implementations of security practices in secure devops and ci/cd environments* (Doctoral dissertation, Ph. D. thesis, Universiteit van Amsterdam).

[45] Akbar, M.A., Smolander, K., Mahmood, S. and Alsanad, A., 2022. Toward successful DevSecOps in software development organizations: A decision-making framework. *Information and Software Technology*, *147*, p.106894.

[46] Dasanayake, S.D.L.V., Senanayake, J. and Wijayanayake, W.M.J.I., 2025. Devsecops for Continuous Security in Trading Software Application Development: a Systematic Literature Review. *Journal of desk research review and analysis*, *2*(2).

[47] Nutalapati, V., 2023. Automated Security Testing for Mobile Apps: Tools, Techniques, and Best Practices. *International Research Journal of Engineering & Applied Sciences (IRJEAS)*, *11*(1), pp.26-31.

[48] Neupane, K., Continuous Automation with DevOps practices for Threat Detection.

[49] Sapkota, D., 2023. *A Framework of DevSecOps for Software Development Teams* (Doctoral dissertation, University of Turku).

[50] Antiya, D., 2024. *DevOps for Compliance: Building Automated Compliance Pipelines for Cloud Security*. Xoffencer international book publication house.

[51] Pandya, K., 2024. *Automated Software Compliance Using Smart Contracts and Large Language Models in Continuous Integration and Continuous Deployment With DevSecOps* (Master's thesis, Arizona State University).

[52] SEKER, S.E., 2024. Experiences and Challenges in AI-Driven Modular Software Development Using Large Language Models for Code Generation.

[53] Pahune, S. and Akhtar, Z., 2025. Transitioning from MLOps to LLMOps: Navigating the Unique Challenges of Large Language Models. *Information*, *16*(2), p.87.

[54] Bishop, S., 2024. AI for Continuous Compliance and Policy Enforcement in DevOps Security Frameworks.

[55] Waizel, G., 2024, July. Bridging the AI divide: The evolving arms race between AI-driven cyber attacks and AI-powered cybersecurity defenses. In *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings* (Vol. 1, pp. 141-156).

[56] Pasam, P.R.A.S.A.N.N.A., Kothapalli, K.R.V., Mohammed, R.A.H.I.M.O.D.D.I.N. and Ying, D.E.N.G., 2023. Integrating Data Remediation Strategies in Robotic Data Processing. *American Digits: Journal of Computing and Digital Technologies*, *1*(1), pp.90-104.

[57] Jawed, M., 2019. *Continuous security in DevOps environment: Integrating automated security checks at each stage of continuous deployment pipeline* (Doctoral dissertation, Wien).

[58] Salman, A.M., Al-Nuaimi, B.T., Subhi, A.A., Alkattan, H. and Alfilh, R.H., 2025. Enhancing cybersecurity with machine learning: A hybrid approach for anomaly detection and threat prediction. *Mesopotamian Journal of CyberSecurity*, *5*(1), pp.202-215.

[59] Ofili, B.T., Obasuyi, O.T. and Osaruwenese, E., 2024. Threat intelligence and predictive analytics in USA cloud security: mitigating AI-driven cyber threats. *Int J Eng Technol Res Manag*, *8*(11), p.631.

[60] Chung, J., 2024. *DevSecOps Metrics, Benefits, and Improvements* (Doctoral dissertation, National University).