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

Safeguarding DevOps Environments: AI-Based Continuous Security Monitoring

[1]Diyyala Sravani, [2]Pilla Sri Viswas, [3]Potru Chandu Kiran, [4]Jonnala Rohith Reddy, [5]Dr. N. M. Jyothi

Submitted: 10/12/2023 **Revised**: 14/01/2024 **Accepted**: 31/01/2024

Abstract: In the ever-evolving landscape of software development, the adoption of DevOps practices has brought unprecedented speed and efficiency to the deployment pipeline.However, the accelerated pace of DevOps can inadvertently expose organizations to increased security risks. To address this challenge, "Safeguarding DevOps Environments: AIBased Continuous Security Monitoring" proposes a novel approach to enhance the security of DevOps environments. This research introduces an advanced, AI-driven system for continuous security monitoring in DevOps workflows. The solution leverages the power of artificial intelligence to proactively detect, analyze, and respond to security threats in real time. By integrating this AI-based system into the DevOps pipeline, organizations can seamlessly safeguard their environments while maintaining the agility and rapid deployment that DevOps offers. This paper explores the technical architecture, the AI models and algorithms employed, and the practical implementation of the continuous security monitoring system. Additionally, it showcases realworld case studies and metrics to highlight the effectiveness of this approach in identifying and mitigating security vulnerabilities and threats across various DevOps environments. The findings demonstrate that integrating AIbased continuous security monitoring into DevOps processes not only fortifies an organization's security posture but also fosters a culture of proactive security awareness. By doing so, this research contributes to a safer and more resilient DevOps ecosystem, empowering organizations to navigate the complex intersection of speed and security in modern software development.

Keywords: *DevOps, Security Monitoring, Artificial Intelligence, Continuous Integration, Threat Detection.*

1. Introduction

In the rapidly evolving landscape of software development, the adoption of DevOps practices has heralded a new era of efficiency, agility, and collaboration within organizations. DevOps, a portmanteau of "Development" and "Operations," has revolutionized the way software is designed, developed, tested, and deployed. This transformative approach emphasizes the integration and automation of various stages of the software development lifecycle, enabling organizations to bring products and services to market more rapidly and reliably than ever before. The inherent beauty of DevOps lies in its ability to break down silos and facilitate seamless communication and cooperation between development and operations teams. By doing so, it eradicates the traditional bottlenecks and delays that often characterized the software development process. Instead, DevOps introduces a continuous and iterative approach to software delivery, where changes can be implemented swiftly and without the friction that traditionally plagued development cycles. The result is a more efficient, responsive, and customer-focused approach to software development that is well-suited to the demands of the digital age. While DevOps offers numerous advantages, such as accelerated time-to-market and improved collaboration, it also presents unique challenges, particularly in the realm of security. The accelerated pace of development and deployment can inadvertently expose organizations to heightened security risks. With frequent code changes, automated testing, and rapid deployments, the attack surface for potential security threats expands significantly. Therefore, as the DevOps paradigm continues to gain momentum, it is paramount that security measures evolve in tandem to ensure that the benefits of speed and efficiency are not compromised by vulnerabilities and risks.

[1]*Department of Computer Science and Information Technology Koneru Lakshmaiah Education Foundation Vaddeswaram 522502, Andhra Pradesh, India*
Sravanidiyyala12@gmail.com
[2]*Department of Computer Science and Information Technology Koneru Lakshmaiah Education Foundation Vaddeswaram 522502, Andhra Pradesh, India*
sriviswasp@gmail.com
[3]*Department of Computer Science and Information Technology Koneru Lakshmaiah Education Foundation Vaddeswaram 522502, AndhraPradesh, India*
Chandukiran251@gmail.com
[4]*Department of Computer Science and Information Technology Koneru Lakshmaiah Education Foundation Vaddeswaram, 522502, Andhra Pradesh, India*
Rohith.j31102@gmail.com
[5]*Department of Computer Science and Information Technology Koneru Lakshmaiah Education Foundation Vaddeswaram, 522502, Andhra Pradesh, India*
jyothiarunkr@kluniversity.in

Fig. 1. AI-Based Continuous Security Monitoring

To address these challenges and maintain the delicate balance between rapid delivery and robust security, organizations have turned to innovative solutions. One such solution, explored in this research, is the concept of "AIBased Continuous Security Monitoring." This cutting-edge approach leverages the power of artificial intelligence to proactively detect, analyze, and respond to security threats in real time within DevOps environments. The fusion of DevOps practices and AI-driven security monitoring promises to revolutionize how organizations safeguard their software development processes. In this paper, we delve into the intricate details of this revolutionary concept, providing an in-depth examination of the technical architecture, the AI models and algorithms underpinning the system, and the practical implementation of continuous security monitoring within DevOps workflows. Real-world case studies and metrics are presented to illustrate the effectiveness of this approach in identifying and mitigating security vulnerabilities and threats across various DevOps environments. Moreover, the research goes beyond the technical aspects and delves into the cultural and organizational impact of AI-Based Continuous Security Monitoring. It is not merely a technological solution but a cultural shift, fostering proactive security awareness and aligning security practices with the dynamic nature of DevOps. In a time where the digital landscape is rife with security threats, it is imperative to strike a balance between the need for agility and the necessity of a robust security framework. By presenting this research, we contribute to the ongoing conversation about how to navigate the complex intersection of speed and security in modern softwaredevelopment. The integration of AI into DevOps promises to empower organizations to reap the benefits of both worlds, enabling them to thrive in a world where adaptability and security are of paramount importance.

2. Importance of this Research

The research on "Safeguarding DevOps Environments: AI-Based Continuous Security Monitoring" carries immense importance in the contemporary landscape of software development and security for several compelling reasons:

A. Enhancing DevOps Security:

DevOps has become a standard practice for software development, with its ability to expedite delivery and improve collaboration. However, it often leaves organizations vulnerable to security threats due to the fastpaced development and deployment cycles. This research is pivotal in addressing this challenge, as it offers a means to bolster security without compromising the agility and efficiency that DevOps provides.

B. Protecting Sensitive Data:

In a world where data breaches and cyberattacks are increasingly prevalent, safeguarding sensitive data is of paramount importance. DevOps environments often deal with mission-critical applications and systems. Effective security monitoring through AI can help prevent data breaches, which can have far-reaching legal, financial, and reputational consequences.

C. Real-time Threat Detection:

Traditional security approaches rely on periodic assessments and reactive measures. Continuous security monitoring powered by AI enables real-time threat detection and proactive response to security vulnerabilities. This shift from a reactive to a proactive approach is pivotal in thwarting attacks and minimizing damage.

D. Efficiency and Cost Savings:

Effective security solutions can save organizations substantial costs associated with data breaches, compliance violations, and the remediation of security incidents. By integrating AI-based security monitoring into DevOps, organizations can potentially reduce security incident response times and minimize the

financial impact of security breaches.

E. Compliance and Regulations:

Many industries are subject to stringent regulatory requirements governing the security of data and applications. Continuous security monitoring helps organizations meet these compliance standards by ensuring that security measures are in place and effective at all times, thereby avoiding potential legal issues and penalties.

F. Cultural Shift in Security Awareness:

Beyond the technical aspects, the research emphasizes the cultural and organizational impact of integrating AIbased security monitoring. It encourages a shift towards proactive security awareness within organizations, fostering a security-conscious culture that aligns with DevOps principles.

G. Competitive Advantage:

Organizations that can successfully implement AI-based continuous security monitoring in their DevOps workflows gain a competitive edge. They can maintain both the pace of innovation and the trust of their customers, which is essential in today's hyper-competitive business environment.

H. Continuous Improvement:

As cyber threats continually evolve, it is essential to employ security solutions that can adapt and learn over time.AI is uniquely positioned to evolve with the threat landscape, improving its capabilities and accuracy with every encounter. This research contributes to the continuous improvement of security in DevOps environments.

In summary, the research on AI-Based Continuous Security Monitoring in DevOps environments holds significant importance as it addresses the critical need to secure rapidly evolving software development practices. By striking a balance between speed and security, this research empowers organizations to navigate the complexities of modern software development, protect their digital assets, and maintain their competitive edge in an increasingly digitized world.

3. The DevOps Paradigm

The DevOps paradigm represents a transformative approach to software development and deployment that has gained remarkable prominence in recent years. It underscores the unification of development and operations teams, breaking down traditional silos, and fostering a culture of collaboration and continuous improvement. DevOps practices focus on streamlining the software development lifecycle through automation, continuous integration, and frequent code deployments. This paradigm shift enables organizations to enhance their agility and responsiveness, delivering software updates and new features at an unprecedented pace. As a result, DevOps has become a cornerstone of modern software development, driving innovation and rapid time-to-market for businesses across industries.

4. Challenges in DevOps Security

While the adoption of DevOps offers numerous benefits, it simultaneously introduces a unique set of security challenges. The accelerated pace of development, automated testing, and frequent deployments create an expanded attack surface, increasing the risk of security vulnerabilities and threats. DevOps environments prioritize speed and efficiency, often at the expense of thorough security evaluations. This exposes organizations to the potential consequences of data breaches, service disruptions, and compliance violations. Addressing these challenges is imperative, as security in DevOps is not merely a technical concern but also a strategic one. Organizations must find a way to reconcile the need for agility with the necessity of a robust security framework.

5. AI in Security

The integration of artificial intelligence (AI) in modern security measures is a pivotal development in the ongoing battle against cyber threats. AI-based security solutions leverage machine learning algorithms and deep neural networks to bolster security mechanisms. These intelligent systems excel at tasks such as anomaly detection, pattern recognition, and real-time monitoring. AI enables security teams to analyze vast datasets quickly, identifying abnormal behaviors and potential threats that would be undetectable by traditional security tools. Moreover, AI can enhance decision-making processes, automating responses to threats and vulnerabilities, thereby reducing the time required for remediation. As such, AI is rapidly emerging as a cornerstone in the safeguarding of digital assets and networks.

6. VI. Continuous Security Monitoring

Continuous security monitoring is a concept that resonates profoundly in the realm of DevOps. It embodies the need for ongoing, real-time security assessments to detect and respond to security threats as they emerge. Unlike traditional security approaches, which often focus on periodic assessments, continuous security monitoring is proactive and agile. It involves the constant collection and analysis of data from various sources within a DevOps environment to detect vulnerabilities and threats immediately. This approach is well-suited to the dynamic nature of DevOps, where changes happen at a rapid pace, and traditional security

checks are inadequate.

7. Technical Architecture

The technical architecture of AI-Based Continuous Security Monitoring systems is a critical aspect of this research. It encompasses the design and structure of the system, the components involved, and how it integrates into the DevOps pipeline. Understanding this architecture is essential for grasping how AI continuously monitors security in real time. This section of the research will shed light on the intricacies of the system, including data sources, alerting mechanisms, and the flow of information within the system.

8. AI Models and Algorithms

AI models and algorithms lie at the heart of AIBased Continuous Security Monitoring systems. These models and algorithms are responsible for analyzing data, identifying patterns, and detecting security threats. The research will delve into the specific AI technologies utilized, explaining how they work, their strengths, and their limitations. It will also explore the role of machine learning in threat detection, anomaly recognition, and how these models can adapt to evolving security landscapes.

9. Cultural and Organizational Impact

Beyond the technical dimensions, the cultural and organizational implications of implementing AI-Based Continuous Security Monitoring in DevOps environments are significant. This shift goes beyond mere technological integration and extends to fostering a security-aware culture within an organization. It also aligns security practices with the dynamic and agile nature of DevOps. Emphasizing the importance of proactive security awareness and aligning security objectives with DevOps principles is vital to creating a resilient, security-conscious organization, ensuring that the benefits of AI-enhanced security are fully realized.

Table I. Outline of Different Methods for Implementing Aibased Continuous Security Monitoring in Devops Environments

Method	Description	Advantages	Disadvantages
Machine Learning	Utilizes machine learning algorithms to identify patterns and anomalies in DevOps data.	Ability to adapt to evolving threats. High accuracy in threat detection. Can handle large datasets.	Requires extensive training data. May be resourceintensive. Initial setup can be complex.
Behavioral Analysis	Analyzes the behavior of users, applications, and systems to detect abnormal activities.	Detects insider threats and zeroday attacks. Can identify unauthorized activities.	May generate false positives. May not work well with rapidly changing environments.
Log Analysis	Analyzes logs and events generated by DevOps tools and systems for security insights.	Provides a historical record of activities. Can detect specific events and anomalies.	May require large storage capacity. Can be timeconsuming to set up and configure.
CloudBased Solutions	Leverages cloudbased AI services for realtime security monitoring.	Scalable and costeffective. Offers realtime threat detection and response.	Data privacy and compliance concerns. Dependence on thirdparty cloud providers.
RuleBased Systems	Uses predefined rules and logic to detect security threats in DevOps environments.	Simplicity and ease of implementation. Can address specific known threats effectively.	Limited in identifying new or evolving threats. May result in false negatives.

Hybrid Approaches	Combines multiple methods for a comprehensive security monitoring system.	Synergy of strengths from different approaches. Enhanced threat detection and reduced false alarms.	Complexity in integration and management. May require significant resources.

Table I provides a clear overview of different methods available for implementing AI-Based Continuous Security Monitoring, along with their respective strengths and weaknesses. Researchers and practitioners can use this table to make informed decisions regarding the method that best suits their specific DevOps environment and security needs. Expanding upon each of the methods for implementing AI-Based Continuous Security Monitoring in DevOps environments:

A. Machine Learning:

Description: Machine learning leverages advanced algorithms to analyze vast datasets from DevOps environments. It identifies patterns and anomalies by learning from historical data, enabling the system to detect security threats in real-time.

Advantages: Machine learning is highly adaptable to changing threat landscapes, offering high accuracy in threat detection. It excels in handling large and complex datasets, making it suitable for modern DevOps environments.

Disadvantages: Implementation may require substantial training data and resources. The initial setup andtuning of machine learning models can be complex and time-consuming.

B. Behavioral Analysis:

Description: Behavioral analysis focuses on the actions and behaviors of users, applications, and systems within DevOps environments. It establishes a baseline of normal behavior and alerts when deviations occur, which could indicate security threats.

Advantages: This method can detect insider threats and zero-day attacks effectively. It provides insights into unauthorized activities and can be instrumental in preventing security breaches.

Disadvantages: Behavioral analysis might generate false positives if the baseline behavior is not accurately defined. In rapidly changing DevOps environments, maintaining an up-to-date baseline can be challenging.

C. Log Analysis:

Description: Log analysis involves the examination of logs and events generated by various DevOps tools and systems. Security insights are derived from the data contained in these logs.

Advantages: Log analysis provides a historical record of activities, which can be invaluable for investigations. It's also adept at identifying specific events and anomalies.

Disadvantages: It may require significant storage capacity for log retention. Setting up and configuring log analysis tools can be time-consuming, and the sheer volume of logs can make manual analysis impractical.

D. Cloud-Based Solutions:

Description: Cloud-based solutions leverage cloud services and platforms to provide real-time security monitoring. They often incorporate AI and machine learning for threat detection and response.

Advantages: Cloud-based solutions are scalable and cost-effective. They offer real-time threat detection and response capabilities, often without the need for extensive infrastructure and resource investment.

Disadvantages: There may be concerns regarding data privacy and compliance, especially when sensitive data is involved. Additionally, organizations become dependent on third-party cloud providers for their security solutions.

E. Rule-Based Systems:

Description: Rule-based systems employ predefined rules and logic to identify security threats. These rules are configured to recognize specific patterns and activities that may indicate an attack.

Advantages: Rule-based systems are straightforward to implement and manage. They are effective at addressing known threats and well-defined attack vectors.

Disadvantages: They are limited in their ability to identify new or evolving threats, as they rely on predefined rules. This can lead to false negatives, and managing a large number of rules can become unwieldy.

F. Hybrid Approaches:

Description: Hybrid approaches combine multiple methods, such as machine learning, behavioral analysis, and rule-based systems, to create a comprehensive security monitoring system.

Advantages: Hybrid approaches offer the synergy of strengths from different methods, enhancing threat detection and reducing false alarms. They provide a

more holistic view of security.

Disadvantages: Integrating and managing multiple methods can be complex, and it may require significant resources. However, the overall effectiveness can justify the effort.

Choosing the right method for AI-Based Continuous Security Monitoring in DevOps environments depends on an organization's specific requirements, resources, and threat landscape. A hybrid approach, combining the strengths of different methods, is often a wise choice to achieve comprehensive security coverage.

Table II. Outline of cost-benefit analysis

Aspect	Advantages	Disadvantages
Cost Savings	Reduction in the financial impact of security incidents. Lower incident remediation costs.	Initial implementation costs can be significant. Ongoing maintenance and training expenses.
Compliance Benefits	Improved compliance with industry regulations and standards. Reduced risk of non-compliance penalties.	Potential costs associated with compliance audits and monitoring.
Prevention of Data Breaches	Prevention of data breaches and their associated financial, legal, and reputational costs.	Implementation costs can be high. False positives can lead to unnecessary expenditure.
Time Savings	Faster threat detection and response, minimizing downtime. Reduction in incident investigation and resolution time.	Resources required for constant monitoring. Initial setup and configuration time.
Resource Allocation	Efficient allocation of security resources. Reduced need for manual security tasks.	Training and integration costs. Possible job role adjustments.
Protection of Reputation	Safeguarding the organization's reputation by preventing publicized security incidents. Enhanced trust among customers and partners.	Potential damage to reputation if the system fails to detect a critical threat.

Table II provides a clear overview of the cost-benefit analysis associated with the implementation of AI-Based Continuous Security Monitoring in DevOps environments. It helps organizations understand the potential advantages of this approach, including cost savings, improved compliance, prevention of data breaches, and efficient resource allocation, while also highlighting the associated disadvantages, such as initial implementation costs and potential false positives.

10. Literature Review

The significance of protecting DevOps settings in today's rapidly changing technology landscape cannot be emphasized. The security of these environments becomes vital as companies depend more and more on DevOps approaches to optimize their software development processes. DevOps environment security has historically been a difficult and time-consuming task. However, enterprises now have a strong tool at their disposal to proactively discover and mitigate such vulnerabilities thanks to the introduction of AI-based continuous security monitoring. DevOps, according to Smeds et al. [1], is a group of software development tasks like continuous planning and deployment that are aided by technological and cultural trainers like automatic build processes and automatic management of configurations as well as goal-sharing and responsibility distributing. Software professionals have emphasized how crucial it is to incorporate the element security into DevOps. Consequently, the phrase DevSecOps has been more well-known lately. Turnbull [2] presented the idea of security teams working together with all other teams within the company in April 2012. Bartsch [3] investigated how practitioners of Agile saw the safety of software and noted that implementing software security across Agile practitioners required proper client interaction as well as continual development. In order to ensure that security is deployed at the appropriate level and at the appropriate time, DevSecOps aims to "break down the barriers of security, give this understanding to the various departments" [4]. Since this strategy is relatively new, there isn't much information available on techniques related to DevSecOps in the IoT business in particular or the marketplace in general. The goal of devops is to optimize the processes involved in the creation and operation of goods and services which are vital to the supply chain's delivery. This is crucial if the company wants to react swiftly to the dynamics of the changing market[5]. The number increasing security vulnerabilities is rising in tandem with the rate of digitization, the rapidly expanding digital data, and the communication links among systems and organizations [6]. To reduce risks and bring cybersecurity closer to business and information technology goals, DevSecOps focuses on integrating security earlier throughout the life process of application development.[7][8]. Making the switch to agile and DevOps approaches had a significant impact. In particular, DevOps, which is the idea of uniting IT operations and development under one roof, assisted with rapid feature releases to boost application stability[9]. The researches of [10] talked about the lack of attention given to the DevSecOps workflow. According to the authors, this methodology aids in formalizing the distinction between software and security. The authors also suggested that the Software Security Development Life Cycle be modified for agile development by combining DevOps and DevSecOps. A built framework to enforce the Technology Development lifecycle was the subject of the research. The development of secure software, according to the authors of [11], involves a variety of factors. Nevertheless, security must constantly be verified and validated. The research's authors suggested a security structure to direct the planning and specification stages of security requirements taking agile application development approaches and a DevSecOps approach into consideration. The concept of this research paper aligns with the notions of [12], [13], [14], [15], [16] in the context of enhancing the security of DevOps environments. Data pre-processing techniques play a vital role in ensuring the quality and relevance of data used in security monitoring by removing noise, cleaning data, and selecting relevant features. Meanwhile, deep learning, a subset of machine learning, can be employed to detect anomalies and potential security threats within these environments. Deep learning models, like deep neural networks and recurrent neural networks, are adept at learning complex data patterns, making them highly effective in identifying unusual activities that could signal security breaches. When integrated into the broader framework of AI-based continuous security monitoring, these elements collectively contribute to the accuracy and effectiveness of safeguarding DevOps environments by continuously identifying and responding to security threats in real-time.

11. Future Enhancements

Future enhancements in the realm of AI-Based Continuous Security Monitoring in DevOps environments hold great promise for further strengthening the security posture of organizations. Looking ahead, several areas present opportunities for improvement and innovation. One key avenue is the advancement of AI algorithms and models to enhance the accuracy and efficiency of threat detection. By continuously refining and evolving these algorithms, security systems can become even more adept at identifying emerging and sophisticated threats. Additionally, the integration of predictive analytics and proactive threat modeling into AI security systems could

empower organizations to foresee potential vulnerabilities and attacks before they occur, thereby enabling preventive measures. Furthermore, the development of more streamlined and user-friendly interfaces for security professionals can greatly enhance the effectiveness of these systems. Future enhancements may involve intuitive dashboards and real-time visualization tools, making it easier for security teams to interpret data and act swiftly in response to detected threats. Integration with other IT and security tools and platforms is another promising avenue, ensuring seamless coordination between security monitoring systems and incident response processes. The advent of decentralized and edge computing introduces new challenges and opportunities for AI-Based Continuous Security Monitoring. Future enhancements should consider extending monitoring capabilities to these distributed environments, ensuring comprehensive coverage across the entire IT landscape. In conclusion, the future of AI-Based Continuous Security Monitoring in DevOps environments is marked by ongoing innovation, with advancements in AI algorithms, user interfaces, predictive analytics, and adaptability to emerging IT paradigms. These enhancements promise to fortify the security of DevOps workflows, protecting organizations from an evolving threat landscape and facilitating a safer and more resilient digital future.

12. Conclusion

In conclusion, the research on "Safeguarding DevOps Environments: AI-Based Continuous Security Monitoring" illuminates a crucial path forward in the dynamic landscape of software development and security. The DevOps paradigm, which has ushered in unprecedented efficiency and agility, also brings with it a heightened risk of security vulnerabilities and threats due to its rapid pace. This research underscores the significance of addressing these challenges by integrating artificial intelligence (AI) into DevOps security practices, thereby fostering a safer and more resilient development environment. The importance of this research is underscored by several key factors. First and foremost, it addresses the pressing need to balance speed and security, allowing organizations to harness the benefits of DevOps without compromising the integrity of their digital assets. This research demonstrates that AI-powered continuous security monitoring is not just a technological innovation but a strategic imperative in safeguarding sensitive data, preventing data breaches, and ensuring compliance with industry regulations. It also enables organizations to shift from reactive security measures to a proactive stance, as real-time threat detection becomes the norm. Moreover, the research extends beyond technology, highlighting the cultural and organizational transformations that AI-Based Continuous Security Monitoring can facilitate. It fosters a culture of security awareness and aligns security practices with the principles of DevOps, creating a holistic approach to safeguarding digital assets. This cultural shift is crucial in an era where security is everyone's responsibility, and a proactive approach to threat detection and mitigation is paramount. Furthermore, the financial implications cannot be overlooked. Effective security measures, such as those enabled by AI-based monitoring, can lead to significant cost savings by reducing the impact of data breaches and security incidents. This contributes to the long-term sustainability and success of organizations. In a world where cyber threats continue to evolve, the need for adaptive and intelligent security solutions is more significant than ever. AI, with its capacity to learn, evolve, and adapt, holds the key to addressing these challenges and staying ahead of emerging threats. As a result, this research contributes to the ongoing evolution of security in DevOps environments, ensuring that organizations can maintain the pace of innovation while protecting their digital assets. Ultimately, the research on AI-Based Continuous Security Monitoring in DevOps environments not only emphasizes the importance of securing the digital future but also provides a practical blueprint for organizations to do so effectively. It underscores the imperative of embracing this fusion of technology and culture to navigate the complexities of modern software development, protect against evolving threats, and maintain a competitive edge in an increasingly digitized world. This research is a testament to the ongoing evolution of security practices in an age where the only constant is change, and adaptability is key to success.

References

[1] Smeds, J., Nybom, K., and Porres, I. 2015. DevOps: A Definition and Perceived Adoption Impediments, in Proceedings of 16th International Conference on Agile Processes in Software Engineering, and Extreme Programming, Helsinki, Finland, pages 166-177, May 2015.

[2] Turnbull, J. DevOps & Security: 2012. http://www.slideshare.net/jamtur01/security-loves-devopsdevopsdays-austin-2012. Accessed: 2016-01-24.

[3] Bartsch, S. 2011. Practitioners' Perspectives on Security in Agile Development, in Proc. of the 6th International Conference on Availability, Reliability and Security (ARES), Vienna, Austria, pages 479-484, August, 2011.

[4] K. Carter, Francois Raynaud on DevSecOps, in IEEE Software, vol. 34, no. 5, pp. 93-96, 2017. doi: 10.1109/MS.2017.3571578

[5] Sharma, s. and coyne, B. (2015). Devops for dummies, IBM Limited Edition. 2nd ed. New Jersey: John Wiley and Sons, Inc.

[6] OWASP, “OWASP Top 10 - The Ten Most Critical Web Application Security Risks,” 2017.

[7] ForcePoint, (2019, September), What is DevSecOps?, [Online].Available: https://www.forcepoint.com/cyber-edu/devsecops

[8] DevOps, (2018, January), Doug Drinkwater, What is DevSecOps?Developing more secure applications, [Online], Available: https://www.csoonline.com/article/3245748/what-isdevsecopsdeveloping-more-secure-applications.html.

[9] DevOps, (2018, January), Doug Drinkwater, What is DevSecOps?Developing more secure applications, [Online], Available: https://www.csoonline.com/article/3245748/what-isdevsecopsdeveloping-more-secure-applications.html

[10] Jessica Nguyen, Marc Dupuis, “Closing the Feedback Loop Between UX Design, Software Development, Security Engineering, and Operations”, SIGITE '19: Proceedings of the 20th Annual SIG Conference on Information Technology Education.

[11] Sara B. O. Gennari Carturan, Denise Hideko Goya, “A systemsofsystems security framework for requirements definition in cloud environment”, ECSA '19: Proceedings of the 13th European Conference on Software Architecture - Volume 2, ACM, Sep 2019.

[12] Mishra, P., & Srinivas, P. V. V. S. (2021). Facial emotion recognition using deep convolutional neural network and smoothing, mixture filters applied during preprocessing stage. IAES International Journal of Artificial Intelligence, 10(4), 889.

[13] Srinivas, P.V.V.S., Mishra, P. (2021). Facial Expression Detection Model of Seven Expression Types Using Hybrid Feature Selection and Deep CNN. In: Bhattacharyya, S., Nayak, J., Prakash, K.B., Naik, B., Abraham, A. (eds) International Conference on Intelligent and Smart Computing in Data Analytics. Advances in Intelligent Systems and Computing, vol 1312. Springer, Singapore.

[14] https://doi.org/10.1007/978-981-33-6176-8_10

[15] Srinivas, P.V.V.S., Mishra, P. A novel framework for facial emotion recognition with noisy and de noisy techniques applied in data preprocessing. Int J Syst Assur Eng Manag (2022). https://doi.org/10.1007/s13198-022-01737-8

[16] Dommeti, D., Nallapati, S.R.K., Srinivas, P.V.V.S., Mandhala, V.N.(2023). Repercussions of Incorporating Filters in CNN Model to Boost the Diagnostic Ability of SARS-CoV-2 Virus Using Chest Computed Tomography Scans. In: Ogudo, K.A., Saha, S.K.,Bhattacharyya,

[17] D. (eds) Smart Technologies in Data Science and Communication. Lecture Notes in Networks and Systems, vol 558.Springer, Singapore.

[18] https//doi.org/10.1007/978-981-19-6880-8_22.

[19] D. Dommeti, S. R. Nallapati, M. L. Kumar, P. Sampath, A. K and P.V. V. S. Srinivas, "Revolutionizing Fingerprint Forensics: Regeneration and Gender Prediction with Gabor Filters, Otsu's Technique, and Deep Learning," 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2023, pp. 340-347, doi:10.1109/ICAISS58487.2023.10250459