ISSN No:-2456-2165

Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security

Sakthiswaran Rangaraju[1]
Product Security Leader at Pure Storage

Dr. Stephanie Ness[2]
Diplomatische Akademie

Rajesh Dharmalingam[3]
DevSecOps Architect at Delphix

Abstract:- This research paper explores the integration of artificial intelligence (AI) strategies into the DevSecOps framework to enhance cloud security including using an analytical techniques, leveraging both quantitative and qualitative methodologies to assess the efficacy of AI-solutions in mitigating security risks. This studies contributes to a nuanced knowledge of the symbiotic relationship among AI and DevSecOps, shedding light on how combining artificial intelligence technology can improves security. The paper additionally discusses implications and challenges related to implementing AI in DevSecOps workflows, considering factors including scalability, interpretability, and adaptability.

I. INTRODUCTION

A. DevSecOps and its Importance in Cloud Security

As the cloud computing becomes mainstream, the conventional techniques to software development and IT operations are being redefined. DevSecOps, a methodology that integrates security practices in the DevOps procedure, has received prominence as corporations attempt to make sure the security and reliability are built into their cloud-based systems. DevSecOps represents a cultural shift towards collaboration and shared responsibility amongst development, security, and operations groups, with the intention of integrating security at some stage in the software development lifecycle. By way of embracing DevSecOps, organizations can proactively address security concerns, reduce vulnerabilities, and deliver robust cloud solutions.

Inside the context of cloud security, DevSecOps performs a pivotal function in ensuring that security features are not an afterthought but are seamlessly integrated into the development and deployment pipeline. This approach emphasizes the importance of automating security practices, undertaking everyday security testing, and fostering a security-first mind-set in the course of the organization. Through incorporating security into the DevOps workflow, companies can identify and manage security issues early in the development cycle, thereby reducing the risk of security breaches and ensuring the integrity of cloud-based applications and infrastructure.

The adoption of DevSecOps is driven with the help of secure development pipelines enabling the rapid pace of software program delivery and deployment in cloud environments. As companies' transition toward cloud-native architectures with micro-services and containers, the complexity of managing security across cloud infrastructure will increase. DevSecOps gives a framework for integrating security controls, compliance checks, and chance management into the continuous delivery pipeline, allowing groups to reap a balance between speed and security without compromising on either.

B. Significance of AI in Cloud Security

The significance of Artificial Intelligence (AI) in cloud security is substantial, as it addresses the evolving and complex challenges associated with safeguarding data, applications, and infrastructure in cloud environments. Here are several key aspects highlighting the significance of AI in cloud security:

➢ *Advanced Threat Detection:*

- *Significance:*

AI-powered algorithms excel in analyzing vast datasets in real-time, enhancing the detection of sophisticated and evolving security threats.

- *Impact:*

Organizations can identify and respond to potential security incidents more rapidly, minimizing the impact of cyberattacks.

➢ *Behavioral Analysis and Anomaly Detection:*

- *Significance:*

AI enables behavioral analysis of users and systems, detecting anomalies that may indicate unauthorized access or malicious activities.

- *Impact:*

The ability to identify deviations from normal behavior enhances the precision of threat detection and reduces false positives.

➢ *Automated Vulnerability Management:*

- *Significance:*
  AI automates the identification and remediation of vulnerabilities, reducing the time between discovery and mitigation.

- *Impact:*
  Organizations can maintain a proactive stance against potential threats, addressing vulnerabilities before they can be exploited.

➢ *Dynamic Adaptability to Threats:*

- *Significance:*
  AI systems can adapt and evolve in response to changing cyber threats, providing a dynamic defense mechanism.

- *Impact:*
  This adaptability is crucial in the face of evolving threats, ensuring that security measures stay relevant and effective.

➢ *Efficient Incident Response:*

- *Significance:*
  AI streamlines incident response by automating the identification, isolation, and mitigation of security incidents.

- *Impact:*
  Faster response times reduce the duration of security incidents, minimizing potential damage and data exposure.

➢ *User and Entity Behavior Analytics (UEBA):*

- *Significance:*
  AI-driven UEBA systems analyze patterns of user behavior to detect anomalies and potential insider threats.

- *Impact:*
  Organizations can proactively address insider threats, protecting sensitive data and critical systems.

➢ *Intelligent Automation in Security Operations:*

- *Significance:*
  AI automates routine security tasks, allowing security teams to focus on strategic aspects of cybersecurity.

- *Impact:*
  Increased efficiency in security operations leads to improved resource allocation and a more proactive security posture.

➢ *Scalability and Real-Time Monitoring:*

- *Significance:*
  Cloud environments often scale rapidly, and AI can efficiently handle large datasets and real-time monitoring.

- *Impact:*
  Cloud security solutions leveraging AI can scale with the dynamic nature of cloud infrastructure, providing continuous protection.

➢ *Privacy-Preserving AI Techniques:*

- *Significance:*
  AI advancements include privacy-preserving techniques that allow for secure data analysis without compromising individual privacy.

- *Impact:*
  Organizations can leverage AI for security analytics without violating data privacy regulations or compromising user confidentiality.

➢ *Compliance and Policy Adherence:*

- *Significance:*
  AI can assist in automating compliance checks, ensuring that security controls align with regulatory requirements and organizational policies.

- *Impact:*
  Organizations can maintain adherence to compliance standards, reducing the risk of legal and regulatory consequences.

The importance of AI in cloud security lies in its potential to enhance threat detection, automate security operations, and offer adaptive and scalable protection mechanisms. As the cybersecurity landscape maintains to conform, integrating AI into cloud security practices will become an increasing number of important for businesses in search of to protect their virtual assets and touchy information.

C. Purpose of Research Paper

This paper seeks to gain several significant outcomes that contribute to the expertise and advancement of cloud security practices, specifically inside the context of incorporating AI-driven techniques inside the DevSecOps framework. The research paper pursuits to provide a holistic information of the integration of AI into DevSecOps for sturdy cloud security, presenting realistic insights, solutions, and strategic pointers that contribute to the persistent development of security practices in cloud environments.

II. LITERATURE REVIEW

➢ *Overview of DevSecOps*

DevSecOps, short for Development, Security, and Operations, is an innovative approach to software development that integrates security practices seamlessly into the DevOps lifecycle. It represents a cultural and operational shift, fostering collaboration and communication between development, security, and operations teams throughout the entire software development process. The primary objective is to build a secure and resilient software

infrastructure by integrating security considerations from the initial design phase to production deployment.

➢ *Key Components*

- *Continuous Integration (CI):*

CI involves the automated building, testing, and integration of code changes into a shared repository multiple times a day. Security checks are integrated into the CI process to identify vulnerabilities early in the development lifecycle.

- *Continuous Deployment (CD):*

CD automates the deployment of code changes to production environments after passing through the CI pipeline. Security checks are conducted in the CD pipeline to ensure that only secure and compliant code is deployed.

- *Infrastructure as Code:*

IaC involves managing and provisioning infrastructure using code and automation. Security controls can be embedded into infrastructure code, ensuring that security is an integral part of the infrastructure deployment process.

- *Containerization and Orchestration:*

DevSecOps frequently leverages containerization (e.g., Docker) and orchestration platform (e.g., Kubernetes) for scalable deployment. Security measures are carried out to secure containerized applications and orchestration environments.

DevSecOps represents a holistic and collaborative technique to software development, ensuring that security is a necessary part of the development process. By combining development, security, and operations into a unified and automatic workflow, corporations can construct and set up software program with each speed and security in mind.

➢ *The Role of AI-Driven Strategies in Enhancing DevSecOps*

In the realm of cloud security, the integration of artificial intelligence (AI) brings a brand-new measurement to DevSecOps by way of allowing advanced threat detection, proactive risk management, and adaptive security measures. AI-driven strategies leverage machine gaining knowledge of algorithms, anomaly detection, and predictive analytics to identify patterns, come across anomalies, and automate reaction mechanisms in real time. By means of harnessing the power of AI, companies can increase their DevSecOps practices with intelligent security capabilities which could adapt to evolving threats and ever changing cloud environments.

The synergy among AI and DevSecOps is rooted within the potential of AI-driven systems to research huge quantities of statistical data, identify security risks accurately and provide actionable insights that empower security teams to make knowledgeable decisions. AI-driven strategies can enhance the visibility and situational attention of security operations, enabling proactive threat detection, incident response, and vulnerability management. Furthermore, AI can facilitate the automation of routine security responsibilities, releasing up security resources to focus on strategic security tasks and reaction to complicated security incidents.

AI-driven techniques also play a vital role in enhancing the resilience and scalability of security features in the DevSecOps framework. Through leveraging AI for dynamic access controls, context-based anomaly detection, and dynamic risk modeling, companies can enhance their cloud security posture and mitigate the effect of increasing threats. Moreover, AI-powered security solutions can continuously analyze from security activities and adapt their defenses, thereby evolving along the dynamic nature of cloud-native environments.

III. METHODOLOGY

A. Implementation and Selection of AI-Driven Tools and Technologies in DevSecOps

The successful implementation of AI- driven tools and technologies in DevSecOps requires a systematic method that encompasses the selection, deployment, and operationalization of AI-powered security solution in the DevSecOps pipeline. The first step is to evaluate the specific security requirements and challenges cloud environments, identifying the areas wherein AI-based strategies can provide the maximum value in enhancing security posture and resilience. This evaluation have to bear in mind the forms of threats and vulnerabilities common in cloud-based infrastructures, the existing security controls and procedures, and the desired effects from incorporating AI into DevSecOps.

As soon as the security needs have been identified, groups can examine and pick out AI-based security solutions that align with their DevSecOps targets and technical environment. This entails carrying out thorough opinions of AI providers, assessing the abilities of AI-powered security solutions, and validating the applicability of AI technologies to the specific needs of the companies. Key issues within the choice system consist of the scalability, interoperability, and adaptability of AI solutions, as well as the convenience of integration with existing DevSecOps toolchains and techniques.

After the selection of AI-driven tool, the next section entails the combination of these tools into the DevSecOps workflow, making sure seamless interoperability with existing development, testing, and deployment approaches. This integration may additionally involve customizing AI programs and algorithms to align with the specific security requirements of the business enterprise, integrating AI-powered security controls into the continuous integration and continuous deployment (CI/CD) pipeline, and organizing feedback loops for enhancing the overall performance of AI-driven security measures. Furthermore, companies want to outline performance metrics and key performance indicators (KPIs) for evaluating the effectiveness and impact of AI in improving DevSecOps practices.

B. Data Collection

➢ *Quantitative Survey Questions*

- *Demographic Information*

✓ Organization Size
✓ Small (1-50 employees)
✓ Medium (51-500 employees)
✓ Large (501+ employees)
✓ Industry Sector:
✓ Technology
✓ Finance
✓ Healthcare
✓ Other (please specify)
✓ Cloud Deployment Model
✓ Public
✓ Private
✓ Hybrid
✓ Multi-cloud

- *AI Adoption in DevSecOps*

✓ On a scale from 1 to 5, how would you rate the current level of adoption of AI-driven security measures in your DevSecOps practices?
✓ Have you implemented machine learning models for threat detection in your DevSecOps pipeline? (Yes/No)

- *Perceived Effectiveness*

✓ How effective do you believe AI-driven security measures are in enhancing the overall security of your cloud environments? (Very Ineffective to Very Effective)
✓ Have you observed a reduction in security incidents since the implementation of AI-driven strategies? (Yes/No)

- *Challenges Faced*

✓ What challenges have you encountered in integrating AI into your DevSecOps practices? (Open-ended)
✓ Rate the level of difficulty in addressing these challenges. (Low to High)

- *Continuous Monitoring*

✓ To what extent do you use continuous monitoring tools in your DevSecOps pipeline? (Not at all to extensively)
✓ How has continuous monitoring impacted your ability to detect and respond to security incidents?

➢ *Qualitative Interview Questions*

- *AI Integration Experience*

✓ Can you describe your experience with integrating AI-driven strategies into your DevSecOps practices?
✓ What motivated your organization to adopt AI in the security domain?

- *Implementation Strategies*

✓ What strategies did you employ to successfully implement AI-driven security measures?
✓ Were there any specific considerations or best practices that guided your implementation process?

- *Impact on Security Outcomes*

✓ How has the integration of AI impacted the overall security posture of your cloud environments?
✓ Can you provide specific examples of security incidents that were mitigated or prevented through AI-driven strategies?

- *Challenges and Lessons Learned*

✓ What challenges did you face during the integration, and how were they addressed?
✓ What lessons have you learned from the implementation of AI in DevSecOps?

- *Documentation and Compliance*

✓ How is the integration of AI-driven strategies documented within your organization?
✓ How do you ensure compliance with security policies and regulations when implementing AI in DevSecOps?

- *Continuous Monitoring Insights*

✓ How do you utilize continuous monitoring in your security practices?
✓ Can you share any insights gained from continuous monitoring data that influenced your security decisions?

➢ *AI Integration in DevSecOps*

- *Shift-Left Security*

DevSecOps emphasizes early integration of security practices in the software development lifecycle, shifting security considerations to the left, or earlier stages of the development process. By addressing security concerns early on, organizations can identify and remediate vulnerabilities before they escalate.

- *Collaboration and Communication*

DevSecOps promotes a culture of collaboration between development, security, and operations teams. This involves breaking down traditional silos and fostering continuous communication throughout the development pipeline. Cross-functional teams collaborate to ensure that security is an integral part of every stage of development.

- *Automation*

Automation is a cornerstone of DevSecOps, enabling the integration of security checks and processes into the continuous integration and continuous deployment (CI/CD) pipeline. Automated testing, code analysis, and security scanning tools help identify and remediate vulnerabilities in an efficient and timely manner.

- *Continuous Monitoring*

DevSecOps emphasizes continuous monitoring of applications and infrastructure to detect and respond to security incidents in real-time. Monitoring tools provide visibility into the security posture of the system, allowing for proactive threat detection and response.

- *Compliance as Code*

Integrating compliance requirements into code and automation processes ensures that security controls and policies are consistently applied. Compliance as code helps organizations meet regulatory standards and reduces the risk of security breaches.

C. Case studies of Successful AI-Driven DevSecOps Implementations

Several companies have effectively leveraged AI-driven techniques to enhance their DevSecOps practices and support the security of their cloud-based infrastructures. One amazing instance is a corporation that included AI-powered anomaly detection and behavior analysis into its DevSecOps pipeline to proactively discover and mitigate security threats in actual time. By way of leveraging AI for continuous monitoring of person conduct and application interactions, the company became capable of detect and replying to anomalous activities, unauthorized access attempts, and potential security breaches, thereby bolstering the security posture of its cloud-primarily based banking programs.

Another compelling case observe entails a global e-commerce platform carried out AI-driven risk intelligence and predictive analytics within its DevSecOps framework to address evolving cyber threats and mitigate the risks related to online transactions and customer data security. The company applied AI to analyze large volumes of security logs, identify patterns indicative of potential threats, and automate the correlation of such occasions across its cloud infrastructure. This proactive technique enabled the e-commerce platform to preemptively deal with security vulnerabilities, protect client information and build trust with its consumer base.

Furthermore, a company embraced AI-driven security automation and orchestration as a part of its DevSecOps strategy, allowing the organization to automate incident response, orchestrate security workflows, and optimize the utilization of security assets throughout its cloud-based offerings and structures. By integrating AI into its security operations, the organization bring in efficiencies in managing incidents, reducing response times, and enhancing the agility and responsiveness of its DevSecOps practices. Those case research exemplify the tangible impact of AI-driven strategies in fortifying cloud security within the DevSecOps paradigm.

D. Challenges and Considerations when Integrating AI-Driven Strategies into DevSecOps

At the same time as incorporating AI-driven strategies into DevSecOps gives compelling benefits, it also gives a set of demanding situations and issues that companies must deal with to ensure a successful implementation and operation of AI-powered security solutions. One of the key demanding situations is the complexity of integrating AI technologies with existing DevSecOps workflows and toolchains. Businesses need to cautiously examine the compatibility of AI-driven security solutions with their existing development and deployment methods, as well as the interoperability with other security tools and platforms.

Additionally, the powerful utilization of AI in DevSecOps calls for a complete understanding of the underlying AI algorithms, models, and records sources. Security groups need to own the critical information relating to systems data to efficiently leverage AI-driven security solutions. Moreover, the availability of data model, classified training statistics is crucial for training AI models to appropriately locate security threats and anomalies. Making sure the integrity and relevance of training data is critical for the effectiveness and reliability of AI-powered security measures.

Another key aspect while integrating AI into DevSecOps is the ethical and privacy implications associated with using AI for security functions. Businesses need to set up clear pointers and governance frameworks for the ethical use of AI in security operations, which include the responsible handling of sensitive data, transparency in AI-driven selection-making, and accountability for the outcomes of AI-powered security features. Addressing those ethical issues is important for building trust in AI-driven security solutions and meeting compliance with regulatory requirements.

E. Key Benefits of Incorporating AI in DevSecOps for Cloud Security

The combination of AI-driven strategies into DevSecOps brings forth many advantages which can considerably increase the security posture of cloud. Firstly, AI empowers businesses to proactively address security incidents by leveraging predictive analytics and real-time intelligence. This proactive approach allows security groups to stay ahead of potential threats and preemptively mitigate security risks, thereby enhancing the resiliency of cloud environments.

Secondly, AI-driven techniques can streamline security operations within DevSecOps through automating general requirements, correlating security activities, and prioritizing indicators based on their criticality. This automation not only improves incident response times and determination but also reduces the load on security teams, allowing them to focus on strategic security areas and proactive threat management. Moreover, AI can assist in contextualizing security statistics and providing actionable insights that resource in making knowledgeable decisions concerning security rules and controls.

Another significant benefit of incorporating AI into DevSecOps is the scaling to meet the evolving nature of cloud environments and the increasingly state-of-the-art tactics used by cyber adversaries. AI-powered security solutions can research from historical security incidents,

adapt to new attack vectors, and continuously enhance their detection capabilities. This ability permits companies to stay agile in their security posture and efficaciously counter rising threats within the ever-changing landscape of cloud security.

➢ *Benefits*

- *Faster Time to Market*

DevSecOps streamlines development processes, reducing time-to-market for software applications. Automated security checks ensure that speed and security are not mutually exclusive.

- *Improved Security Posture*

By integrating security into the development lifecycle, organizations can proactively identify and remediate security vulnerabilities, reducing the risk of security breaches.

- *Enhanced Collaboration*

DevSecOps breaks down traditional barriers between teams, fostering collaboration and shared responsibility for security. Cross-functional teams work together to achieve common goals.

- *Efficient Resource Utilization*

Automation and continuous monitoring reduce manual efforts, allowing teams to focus on strategic tasks and innovation. Efficient resource utilization leads to cost savings and improved overall productivity.

➢ *Future Trends*

- *Emerging Technologies and Evolution of AI-Driven Strategies for Cloud Security*

When predicating the future, the evolution of AI-driven strategies for cloud security is poised to witness several transformative developments with the intention to form the landscape of DevSecOps practices. One of the distinguished traits is the convergence of AI, machine learning, and cybersecurity, leading to the emergence of self-sufficient intelligent systems that may adapt, study, and self-heal in response to security threats. These self-sustaining system will leverage AI to autonomously discover, analyze, and reply to security incidents, thereby lowering the reliance on manual intervention and allowing self-defending cloud environments.

Another future development in AI-driven strategies for cloud security is the integration of descriptive AI and obvious decision-making mechanisms inside security operations. As AI-powered security solutions turn out to be more pervasive, the need for transparent and interpretable AI models that may give an explanation for their decision-making approaches and offer intent for security actions will become paramount. This method will drive the adoption of AI technology that prioritize predictability, fairness, and responsible security operations, thereby fostering trust and assurance in AI-driven security features.

Moreover, the convergence of AI and DevSecOps will lead to the emergence of AI-driven DevSecOps platforms and toolchains which might be particularly designed to embed AI abilities into the stop-to-cease security lifecycle of cloud-based applications. Those AI-pushed DevSecOps systems will provide included security testing, vulnerability evaluation, and compliance monitoring powered by means of AI, allowing companies to integrate security into their DevOps practices whilst leveraging the intelligence and automation provided by AI for proactive threat control.

IV. RECOMMENDATIONS

➢ *Best Practices and Tips for Integrating AI into DevSecOps for Robust Cloud Security*

Incorporating AI into DevSecOps for strong cloud security entails a set of state of art security practices and guidelines that companies can leverage to maximize the effectiveness and impact of AI-driven security strategies. First of all, companies ought to prioritize the alignment of AI projects with their DevSecOps goals and security necessities, ensuring that the combination of AI serves particular security use cases and complements present security controls and techniques. This alignment may be carried out through a radical evaluation of the security landscape, identity of AI-driven security opportunities, and the status quo of clear goals for AI integration.

Secondly, corporations have to foster a culture of life of collaboration and information sharing among security, development, and operations teams to ensure the integration of AI into DevSecOps. This collaboration involves purpose driven training on AI principles and methodologies, the status quo of shared security responsibilities, and the creation of multidisciplinary teams which can collectively power the adoption and operationalization of AI-driven security features inside the DevSecOps pipeline. By means of promoting a collaborative attitude, companies can harness the collective knowledge of their groups to accurately leverage AI for cloud security.

Any best practice is to prioritize the security and integrity of AI-model and algorithms by way of enforcing rigorous testing, validation, and governance processes. Companies must set up robust mechanisms for comparing the accuracy, reliability, and resilience of AI-driven security solutions, in addition to measuring the overall performance and effectiveness of AI models in real-life security scenarios. Moreover, companies should spend money on ongoing training and upskilling of security groups to enhance their talent in leveraging AI tools and technologies for DevSecOps practices.

➢ *Training and Resources for AI-Driven DevSecOps Strategies*

To empower security specialists and DevOps practitioners with the understanding and abilities essential to effectively integrate AI-driven strategies into DevSecOps, a big range of training applications and resources are available. These assets encompass training courses, certification programs, online tutorials, and know-how

repositories that cater to diverse elements of AI-driven DevSecOps techniques. Companies and individuals looking for to delve into the realm of AI-driven security in DevSecOps can leverage those sources to gain useful insights and actionable guidance for implementing AI-powered security features within their cloud environments.

One of the key resources for AI-driven DevSecOps training is the availability of specialized publications and certification programs that concentrate on the intersection of AI and machine learning from a DevSecOps context. These guides combined with AI-driven threat detection, anomaly analysis, security automation, and AI governance, provides members with a comprehensive understanding of the way AI may be appropriately included into DevSecOps practices to enhance cloud security. Additionally, self-learning systems and professional organizations provide a wealth of educational materials, webinars, and workshops that delve into the practical implementation and operationalization of AI-driven security strategies in DevSecOps.

Moreover, organizations can advantage from industry-specific sources and expertise sharing projects that provide insights and industry best practices for integrating AI into DevSecOps within the context of cloud security. Enterprise forums, conferences, and community-driven initiative provide opportunities for security experts to interact with peers, enterprise professionals, and thought leaders with emerging ideas, studies, and review from real life use cases of AI-driven DevSecOps implementations. Leveraging these industry sources can enhance the understanding base and knowledge of security teams in harnessing AI for sturdy cloud security in the DevSecOps paradigm.

V. CONCLUSION

- *The Future of AI-Driven DevSecOps for Robust Cloud Security*

In conclusion, the integration of AI-driven techniques into DevSecOps represents a transformative soar towards bolstering the security and resilience of cloud platforms. Through harnessing the power of AI for threat detection, risk management, and security automation, companies can increase their DevSecOps practices to proactively deal with security threats and give a boost to their cloud environments in tackling emerging threats.

REFERENCES

[1]. (2023). Artificial intelligence in cloud computing security. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets33029
[2]. Ahmad, W., Rasool, A., Javed, A., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: a comprehensive survey. Electronics, 11(1), 16. https://doi.org/10.3390/electronics11010016
[3]. Badarch, T. (2022). Exploring artificial intelligence for network security: a case study of malware defence. American Journal of Computer Science and Technology, 5(2), 108. https://doi.org/10.11648/j.ajcst.20220502.22
[4]. Rahaman, M., Tisha, S., Song, E., & Cerny, T. (2023). Access control design practice and solutions in cloud-native architecture: a systematic mapping study. Sensors, 23(7), 3413. https://doi.org/10.3390/s23073413
[5]. Rangaraju, S. (2023). AI Sentry: Reinventing Cybersecurity Through Intelligent Threat Detection. EPH - International Journal of Science And Engineering, 9(3), Article 211. https://doi.org/10.53555/ephijse.v9i3.211
[6]. Rangaraju, S. (2023). Secure by Intelligence: Enhancing Products with AI-Driven Security Measures. EPH - International Journal of Science And Engineering, 9(3), Article 212. https://doi.org/10.53555/ephijse.v9i3.212
[7]. Xu, Z., Liu, W., Huang, J., Yang, C., Lu, J., & Tan, H. (2020). Artificial intelligence for securing iot services in edge computing: a survey. Security and Communication Networks, 2020, 1-13. https://doi.org/10.1155/2020/8872586
[8]. Zhou, X., Mao, R., Zhang, H., Dai, Q., Huang, H., Shen, H., … & Rong, G. (2023). Revisit security in the era of devops: an evidence-based inquiry into devsecops industry. Iet Software, 17(4), 435-454. https://doi.org/10.1049/sfw2.12132
[9]. Ziegler, V., Schneider, P., Viswanathan, H., Montag, M., Kanugovi, S., & Rezaki, A. (2021). Security and trust in the 6g era. Ieee Access, 9, 142314-142327. https://doi.org/10.1109/access.2021.3120143