International Journal of Open Publication and Exploration (IJOPE), ISSN: 3006-2853
Volume 9, Issue 1, January-June, 2021, Available online at: https://ijope.com

DevSecOps in Regulated Industries: Bridging Security and Speed in CI/CD Pipelines

Satish Reddy Goli

Independent Researcher, DevOps Engineer

ABSTRACT

The study is focused on how DevSecOps can be effectively applied in CI/CD pipelines in regulated sectors to achieve a balance between security, speed, and compliance. The literature identifies the challenges of automation, compliance alignment, security metrics, and DevSecOps integration in regulated environments. It employs an explanatory study design and qualitative and quantitative secondary data to reveal vulnerabilities and integration challenges. The results indicate that there is an increasing requirement in the automated security testing, standardised CI/CD definitions, and cross-functional collaboration. DevSecOps becomes one of the possible solutions to integrate security into rapid development to maintain compliance and software quality. The study provides actionable recommendations towards safe and effective digitalisation within regulated industries.

Keywords: DevSecOps, CI/CD Pipelines, Security Automation, Regulatory Compliance, Dynamic Testing, Digital Transformation

INTRODUCTION

A. Background of the Study

The regulated sectors have traditionally been more concerned with security and regulation needs than speed. However, DevOps practices have brought about continuous integration and continuous delivery (CI/CD) to achieve quicker development [1]. This transition increases agility and efficiency also there emerged some new risks of ensuring security and compliance. DevSecOps is proposed as the solution to this problem as security practices being a part of the CI/CD pipeline.

This strategy can help the regulated industries strike the right balance between innovation and the high compliance requirements.

B. Overview

The study investigates how DevSecOps can help to improve the security of software development in regulated sectors and ensure the speed of development with CI/CD pipelines. Healthcare, finance, and government industries are going through digital transformation. They require innovation in terms of maintain appropriate balance of compliance and data security [2]. It identifies some ways that DevSecOps practices such as automated security testing, continuous monitoring, and policy-as-code can be integrated seamlessly into the development lifecycle. The study offers an overview of operational frameworks and tools which can be applied in integrating security through a combination of secondary data analysis and case studies. It will offer guidance concerning the production of secure, agile, as well as regulation-compliant (development) environments.

C. Problem Statement

The challenges of balancing between quick software release and high security requirements often face regulated businesses. The speed of development has been confronted with the paradigm shift towards CI/CD pipelines. It also posed new risks in addition to compliance issues due to absence of security integrations [3]. This can result in late releases or non-compliance software. The disconnect is presenting a massive dilemma to the organisations because they must be creative and adhere to the rules of the industry. The issue is that there is no single framework that successfully integrates security in the CI/CD without interfering with speed. This paper closes this gap by examining the necessity of secure and effective DevSecOps in regulated environments.

D. Objectives

The objectives are: 1. To discuss the effective implementation of DevSecOps practices in CI/CD pipelines for regulated sectors. 2. To understand the impact of DevSecOps to maintain a balance between speed and security in digital

transformation initiatives. 3. To assess the major challenges that organisations have to deal with as adopting DevSecOps on regulated environments

E. Scope and Significance

The scope of this study is the adoption of DevSecOps in regulated as regulation and data security are necessary to integrate. It mainly focuses on ways to incorporate security into the CI/CD pipelines without affecting the speed of development or need to comply with regulations [4]. It will cover the identification of tools with practices alongside frameworks to support the smooth security automation and continuous compliance. The study will compare and contrast real-life case studies and literature to identify and present practical approaches to implementing DevSecOps. This study is significant because it can help organisations to update their development processes to be modern as ensure security and compliance.

LITERATURE REVIEW

A. DevSecOps Implementation in Regulated CI/CD Pipelines

The necessity to combine security with agility has become urgent due to the demand in faster software delivery in regulated industries. Finance and government are the sectors that must be compliant with stringent regulations also being responsive to quick changes in technology and user demands [5]. Conventional models of security tend to slow development thus there is a trade-off between compliance and speed. DevSecOps represents an appropriate balance as it integrates security right into the Continuous Integration and Continuous Deployment pipelines ***[referred to Figure 1]***.

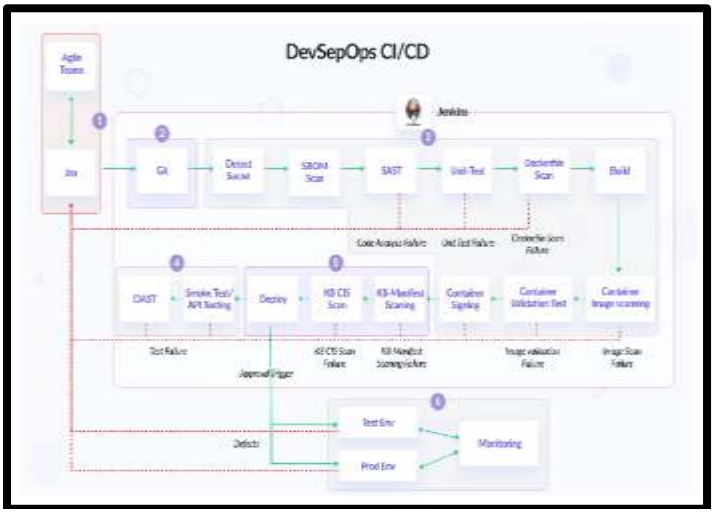

Figure 1: The Architecture of DevSecOps CI/CT Pipeline

This approach makes security not an extra phase but a part of the software development process. Organisations can identify and fix vulnerabilities in the early stages through some significant practices of automated security testing, continuous compliance scans, and infrastructure as code [6]. DevSecOps promotes cross-functional cooperation among development and security teams to balance speed and regulatory compliance. The implementation will be effective as they need to use the appropriate tools with cultural transformation to collective responsibility alongside excellent governance model based on industry regulations.

B. The Impact of DevSecOps in Digital Transformation

The effect of digital transformation on regulated sectors is modifying software development. This necessitates innovation to be provided faster with the same high security and compliance level [7]. While organisations shift towards agile and cloud-native solutions, there is a challenge to balance regulatory integrity without impacting the pace of the development process. DevSecOps refers to the practice of building security into the complete software development cycle [8]. It allows teams to discover and remediate vulnerabilities in the CI/CD pipelines rather than subsequently by incorporating security tools and practices directly within the pipelines. It reduces risk as well as accelerates delivery by preventing last-minute security issues [9]. Continuous monitoring and automatic testing can be employed to confirm compliance with regulatory needs throughout the development lifecycle. DevSecOps about more than a technology as it encourages a cultural change towards a seamless collaboration of developers and operations teams. This model of shared responsibility enhances compliance with innovation. This is key to making digital transformation initiatives agile and secure in highly regulated industries.

C. Key Challenges in DevSecOps Adoption for Regulated Industries

DevSecOps in regulated environments has some specific issues that can make it less effective as not properly considered in implementation process. The strategy offers a secure and fast way to deliver software, organisations across the finance, healthcare, and government industries have to work through the stringent compliance requirements, legacy systems, and organisational silos [10]. A significant difficulty is cultural resistance to change because development, security, and operations teams tend to operate in silos having different priorities and mentalities.

Also, security insertion in CI/CD pipelines requires specific tools and expertise that most organisations do not have. Although security automation and policy-as-code frameworks are powerful, they can be cumbersome to set up, particularly in cases where legacy infrastructure is yet to be retired [11]. Real-time visibility and governance to ensure continuous compliance in fast-changing environments also may not be feasible using current processes. Cost pressures and a lack of executive commitment may cause a slowdown of DevSecOps efforts [12]. That is not all as regulated industries have to contend with audit trials and documentation, which introduce other levels of complexity.

METHODOLOGY

A. Study Design

This study uses an explanatory study design to examine how DevSecOps can be efficiently deployed in regulated environments and consider both speed and compliance. An explanatory design is appropriate due to the possibility to analyse cause-and-effect relations, also how security integration into CI/CD pipelines affects development results. It will apply real-world case studies and secondary data to investigate the underlying causes of successful or failed DevSecOps implementations. The design also supports a more profound comprehension of the tools, framework, and issues of secure software delivery. The study is beneficial in decision-making in compliance-oriented sectors by describing the relationship between regulatory controls and developmental practices during the digital transformation.

B. Data Collection

This study is based on qualitative and quantitative secondary data that allows offering a profound perspective on DevSecOps adoption in regulated sectors. The collection of qualitative data is through industry reports, white papers, and case studies to gain insights into best practices, challenges, and contextual information about security integration in CI/CD pipelines. Evidence-based analysis of DevSecOps effectiveness relies on quantitative data, including statistics generated during market study, compliance audits, and performance measurements. The utilisation of the secondary data is justified because it provides access to a wide scope of verified facts of credible sources, saves time and resources. The collection of data process ensures a well-rounded examination of the security, speed, and compliance in digital development settings.

C. Case Studies Examples

Case Study 1: Vulnerabilities in Continuous Delivery Pipelines

The case study is on security vulnerabilities in industrial Continuous Delivery (CD) pipelines, awareness, detection, and risk mitigation. Secure and reliable infrastructure is becoming more important as organisations continue to accelerate their development pace and time to market by using CI/CD and DevOps [15]. It was conducted as a qualitative survey of agile project teams and two real-world CD pipelines were analysed with the STRIDE threat modeling framework. The results indicated that team members had no specific security training, but they showed the general knowledge of the security principles. The analysis allowed highlighting 22 identified vulnerabilities, which provides evidence of the necessity of more robust security embedding and role-based training in CD processes.

Case Study 2: A Case Study on the Challenges of Integrating Dynamic Security Testing Tools in CI/CD

This case study aims at integrating three automated security testing methods of static, dynamic, and interactive, into a CI/CD pipeline. This study fills the literature gap where most studyers have concentrated on static analysis. Continuous Integration and Continuous Delivery (CI/CD) have accelerated the software development process, but the conventional security processes can no longer keep up.

The case study demonstrates the ability of DevSecOps to incorporate security into the rapid development cycles through automation of the important testing processes. It also addresses implementation difficulties and traps including compatibility between tools, complexity of configuration, and false positives. The insights are intended to help DevOps teams to effectively integrate dynamic security testing. This could improve software quality and compliance with regulations in contemporary pipelines.

D. Metrics of Evaluation

Table 1: Evaluation Metrics

Metric	Description	Purpose
Deployment Frequency	Measures how often new code is released into production.	Evaluates the impact of DevSecOps on development speed.
Time to Remediate Vulnerabilities	Measures the average time taken to fix identified security flaws [7].	Assesses the effectiveness of integrated security practices.
Compliance Audit Success Rate	Percentage of successful regulatory audits or assessments.	Determines the level of adherence to industry-specific compliance standards.
Mean Time to Recovery (MTTR)	Average time taken to recover from system failures or breaches.	Evaluates system resilience and incident response efficiency [9].
Automated Test Coverage	Proportion of code tested through automated security and functional tests [12].	Indicates the extent of automation in detecting vulnerabilities early.
Number of Security Incidents	Count of security breaches or policy violations over a specific period.	Measures the overall improvement in system security with DevSecOps adoption.

(Source: Self-developed)

The table depicts essential metrics utilised to measure DevSecOps efficacy based on development velocity, security embedding, compliance achievement, incident handling, test automation, and overall system robustness ***[referred to Table 1]***.

RESULTS

A. Data Presentation

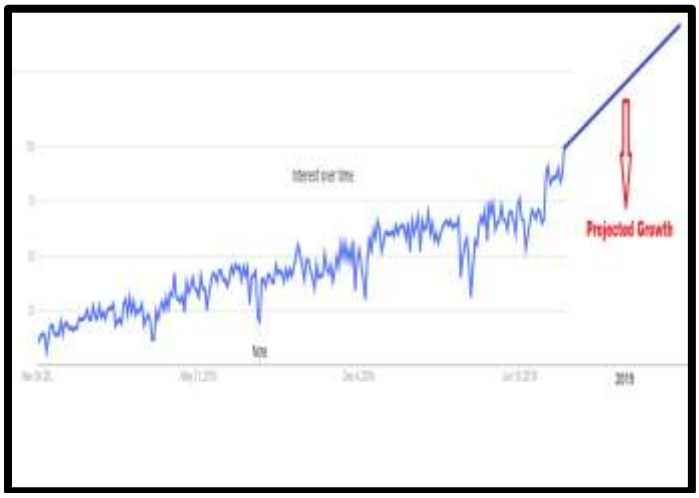

Figure 2: DevOps Adoption in the Market

The graph allows emphasising the consistent upward trend of interest in DevOps between 2014 and 2018 with a significant peak extending into 2019 [17. The DevOps adoption increased by about 8 percentage between 2015 and 2016 as indicates the start of a wider movement toward agile, collaborative development and operations practices. The trend line has been growing steadily since 2016 with a few ups and downs. This estimated increase indicates the growing awareness of the importance of DevOps in deployment cycles also enhancement of the quality of software alongside supporting continuous integration and delivery [17]. The importance of this graph to the context of momentum surrounding DevSecOps that necessity of incorporating security into fast-moving CI/CD pipelines in regulated industries ***[referred to Figure 2]***.

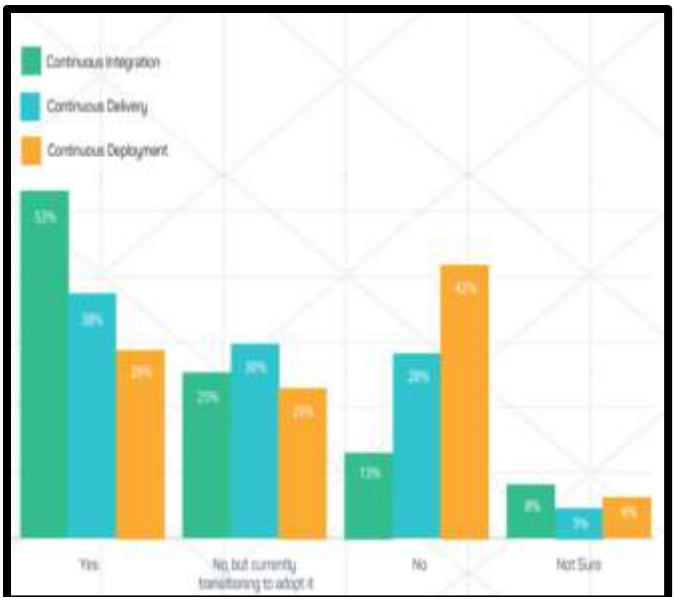

Figure 3: CI/CD Pipeline Adoption in Organisations

The figure shows the rate of adoption of Continuous Integration (CI), Continuous Delivery (CD), and Continuous Deployment in organisations. A survey showed that 53 percent of the respondents used CI, 38 percent practiced CD and only 29 percent had tried Continuous Deployment [18]. Surprisingly, 30% are moving towards CD, and 29% are moving towards Deployment, indicating an increasing amount of interest in CI/CD practices. Nevertheless, a substantial number of 42 percent have not implemented Continuous Deployment with 28 percent not implement CD [18]. This adoption gap is partly because there are no agreed-upon definitions of what each stage of CI/CD entails. This graph is vital to comprehend DevSecOps in regulated sectors, where the security and speed need to address in CI/CD pipelines ***[referred to Figure 3]***.

B. Findings

The results demonstrate the increasing and maintained interest in the DevOps practices, which is a part of the significant trend towards agile and cooperative ways of software development. This trend underscores DevOps is the main driver of efficiency, speed, and quality in deployment [17]. Nevertheless, Continuous Integration is commonly established whereas Continuous Delivery and Deployment are still making slower process. This adoption rate suggests that there remains some uncertainty with regards to implementation standards [18]. These insights highlight the applicability of DevSecOps in regulated industries that need to prioritise compliance, reliability, and fast delivery effectively.

C. Case Study Outcomes

Table 2: Case Studies Key Outcomes

Case Study	*Key Outcomes*
Case Study 1: Vulnerabilities in continuous delivery pipelines	Team members did not have formal security training but possessed general security awareness [15]. Discovered 22 vulnerabilities, emphasising the importance of stronger security integration.
Case Study 2: A Case Study on the Challenges of Integrating Dynamic Security Testing Tools in CI/CD	CI/CD has capability of incorporating static, dynamic and interactive testing. This highlights implementation issues like tool compatibility and false positives [16].

(Source: Self-developed)

The table presents the key outcomes of two case studies which indicate the necessity of more effective security training, effective vulnerability management and the inclusion of dynamic testing tools ***[referred to Table 2]***.

D. Comparative Analysis of Literature Review

Table 3: Comparative Analysis of Literature

Author	Focus	Key Findings	Literature Gap
[5]	DevOps and DevSecOps component analysis	Identified core elements essential to both DevOps and DevSecOps [5].	Lacks practical validation in regulated industries.
[6]	Cybersecurity monitoring in DevSecOps	Promotes self-service monitoring as a critical DevSecOps enabler.	Limited studies on automation in regulated sectors.
[7]	Continuous certification in DevOps	Proposes automated certification to maintain compliance.	Application in CI/CD pipelines not deeply explored [7].
[8]	DevSecOps metrics development	Suggests specific metrics to measure DevSecOps effectiveness [8].	Does not analyze metric application in industry case studies.
[9]	DevOps in oil and gas technology	Demonstrates DevOps pipeline implementation in operational environments.	Security integration not addressed [9].
[10]	Continuous certification (duplicate of [7])	Emphasizes ongoing validation within DevOps cycles.	Overlaps but lacks regulated industry focus.
[11]	Compliance at speed in DevOps	Shows how compliance can align with rapid DevOps cycles [11].	Does not integrate dynamic security testing.
[12]	Cyber defense in cloud and mobile-first environments	Discusses threat evolution and shifting defense strategies.	Not directly applied to CI/CD or DevSecOps scenarios.

(Source: Self-developed)

This table is a summarization of significant studyes regarding DevSecOps and CI/CD, which allows identifying commonalities in findings related to automation, compliance, and metrics but also indicates gaps in the literature in the domain of dynamic testing and regulated industries applications ***[referred to Table 3]***.

DISCUSSION

A. Interpretation of Results

The results indicates that organisations are gradually adopting the DevOps and CI/CD practices to enhance the speed of development and quality of software. However, there are also a visible reluctance to apply Continuous Delivery and Deployment comprehensively. This conservatism has been explained by the issue of security, compliances and lack of unified definition of the CI/CD phases [18].

These results also indicate that teams know security principles but do not always have specialised knowledge to incorporate them efficiently into pipelines. These insights identify the clear opportunity on DevSecOps through automating security checks and establishing cross-functional collaboration. Organisations can ensure secure, compliant, and efficient software delivery in regulated environments.

B. Practical Implications

The potential policy implications of the study point to the lack of security as a stunning issue that regulated industries should address as soon as possible by incorporating security as a natural part of their CI/CD pipelines. Organisations should maintain that security not become a bottleneck of software delivery with increasing pace of digital transformation. DevSecOps provides a viable way by introducing security as a part of all development lifecycle stages so that teams could ensure compliance without sacrificing speed [17].

The results promote the idea of investing in automation security tools, developing and operations teams, and a culture of shared responsibility. These practices are invaluable to any organisation looking to modernise its infrastructure and

simultaneously adhere to rigorous regulatory requirements and produce quality and secure software in an efficient and consistent manner.

C. Challenges and Limitations

The study had a number of difficulties and drawbacks, including a lack of access to more recent, sector-specific statistics on DevSecOps adoption and regulation in the regulated environment. The difference in definitions and use of CI/CD practices across organisations seemed to be a challenge in making standard comparisons [11]. Furthermore, DevOps teams did not have formal security training, which restricted the insights on advanced DevSecOps strategies. Secondary data used in the study might also fail to provide a comprehensive picture of practices or specific barriers may be changing.

D. Recommendations

The main focus of the organisations should be to integrate security as early as possible in the CI/CD pipeline by using automated tools and security testing frameworks. It is necessary to invest in training of DevOps groups to develop security awareness and competence. Governance and clear definitions of CI/CD practices may contribute to standardisation and less confusion about implementation [16]. On top of that, threat modeling and ongoing compliance monitoring should be implemented to prevent threats before they occur.

CONCLUSION AND FUTURE WORK

This study highlights the increased relevance of DevSecOps in the regulated industry where the pace of development, security, and compliance need to be in alignment. Security as CI/CD pipeline provides a revolutionary perspective in management of software delivery in high-speed environments. As organisations slowly migrate to DevOps practices, most of them are still struggling to integrate effective security because of skills shortage, lack of a consistent definition, and old systems. A feasible solution offered by DevSecOps is to automate security testing, foster cooperation, and assure compliance without reducing development speed.

A further direction of work is the creation of domain-specific DevSecOps frameworks to reflect the particular compliance and operational requirements of each industry, including finance, healthcare, and government. Future work can involve empirical study and longitudinal data to quantify the success of the various models of security integration over the years. The potential use of AI and machine learning to automate threat detection in DevSecOps pipeline is also an exciting topic to explore.

REFERENCES

[1]. Herardian, R., 2019. The soft underbelly of cloud security. *IEEE Security & Privacy*, *17*(3), pp.90-93.
[2]. Nguyen, J. and Dupuis, M., 2019, September. Closing the feedback loop between UX design, software development, security engineering, and operations. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education* (pp. 93-98).
[3]. Rice, T., 2019. Secure DevOps before DevSecOps. *Information System Security Association Journal*, *17*(11), pp.16-19.
[4]. Rahul, B.S., Prajwal, K. and Manu, M.N., 2019. Implementation of DevSecOps using open-source tools. *International Journal of Advance Study, Ideas and Innovations in Technology*, *5*(3), p.10501051.
[5]. Hong, J.K., 2019. Component analysis of DevOps and DevSecOps. *Journal of The Korea Convergence Society*, *10*(9), pp.47-53.
[6]. Diaz, J., Pérez, J.E., Lopez-Peña, M.A., Mena, G.A. and Yagüe, A., 2019. Self-service cybersecurity monitoring as enabler for DevSecOps. *Ieee Access*, *7*, pp.100283-100295.
[7]. Anisetti, M., Ardagna, C.A., Gaudenzi, F. and Damiani, E., 2019, November. A continuous certification methodology for devops. In *Proceedings of the 11th International Conference on Management of Digital EcoSystems* (pp. 205-212).
[8]. Prates, L., Faustino, J., Silva, M. and Pereira, R., 2019. Devsecops metrics. In *Information Systems: Study, Development, Applications, Education: 12th SIGSAND/PLAIS EuroSymposium 2019, Gdansk, Poland, September 19, 2019, Proceedings 12* (pp. 77-90). Springer International Publishing.
[9]. Enemosah, A., 2019. Implementing DevOps Pipelines to Accelerate Software Deployment in Oil and Gas Operational Technology Environments. *International Journal of Computer Applications Technology and Study*, *8*(12), pp.501-515.
[10]. Koppanati, P.K., 2019. Building Custom CI/CD Pipelines for Java Applications in GitLab. *Journal of Scientific and Engineering Study*, *6*(6), pp.233-238.

[11]. Abrahams, M.Z. and Langerman, J.J., 2018, September. Compliance at velocity within a devops environment. In *2018 Thirteenth International Conference on Digital Information Management (ICDIM)* (pp. 94-101). IEEE.
[12]. Haani, V. and Ananya, D., 2018. Shifting Paradigms in Cyber Defense: A 2015 Perspective on Emerging Threats in Cloud Computing and Mobile-First Environments. *International Journal of Trend in Scientific Study and Development*, *2*(6), pp.1711-1731.
[13]. Asenahabi, B.M., 2019. Basics of study design: A guide to selecting appropriate study design. *International Journal of Contemporary Applied Studyes*, *6*(5), pp.76-89.
[14]. Martins, F.S., da Cunha, J.A.C. and Serra, F.A.R., 2018. Secondary data in study–uses and opportunities. *PODIUM sport, leisure and tourism review*, *7*(3), pp.I-IV.
[15]. Paule, C., Düllmann, T.F. and Van Hoorn, A., 2019, March. Vulnerabilities in continuous delivery pipelines? a case study. In *2019 IEEE international conference on software architecture companion (ICSA-C)* (pp. 102-108). IEEE.
[16]. Buijtenen, R.V. and Rangnau, T., 2019. Continuous Security Testing: A Case Study on the Challenges of Integrating Dynamic Security Testing Tools in CI/CD. *17th SC@ RUG 2019-2020*, p.45.
[17]. Dzone, 2019. DevOps Trends 2019. Available at: https://dzone.com/articles/devops-trends-2019-what-you-need-to-know. [Accessed on: 2nd September, 2020].
[18]. The New Stack, 2019. Measuring CI/CD Adoption Rates Is a Problem. Available at: https://thenewstack.io/measuring-ci-cd-adoption-rates-is-a-problem/. [Accessed on: 1st September, 2020].
[19]. Yugandhar, M. B. D. (2020). Digital Operations in Fintech: A Study of Process Automation. International Journal of Information and Electronics Engineering, 10(4), 15-24.
[20]. Chintale, P., Korada, L., Ranjan, P., Malviya, R. K., & Perumal, A. P. (2021). The Impact of Covid-19 on Cloud Service Demand and Pricing in the Fintech Industry. Journal of Harbin Engineering University, 42(7).
[21]. Bucha, S. INTEGRATING CLOUD-BASED LOGISTICS SOLUTIONS: A STRATEGIC APPROACH FOR E-COMMERCE EFFICIENCY.
[22]. Venna, S. R. (2019). Overcoming Submission Challenges in Post-Market Surveillance & Lifecycle Management. *Available at SSRN 5270737*.