International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-3 || Jul – Sep 2025 || PP. 6-10
https://ijcscer.org

SAST and DAST Integration Strategies for Scalable CI/CD Workflows

Ravi Sharma
Independent Researcher
Jaipur, India (IN) – 302001

http://www.ijcscer.org/ || Vol. 2 No. 3 (2025): July Issue

Date of Submission: 24-05-2025 **Date of Acceptance:** 25-06-2025 **Date of Publication:** 17-07-2025

Abstract — As the demand for faster and more secure software development increases, integrating Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) into Continuous Integration/Continuous Deployment (CI/CD) workflows has become crucial. These tools help ensure the security of applications by identifying vulnerabilities early in the software development lifecycle (SDLC). However, integrating SAST and DAST effectively into CI/CD processes presents several challenges, including performance overhead, false positives, and the scalability of security testing in large, complex environments. This paper explores integration strategies for SAST and DAST that maximize security, speed, and scalability within CI/CD workflows. By evaluating existing solutions, proposing a hybrid strategy, and testing with a case study, we provide valuable insights into optimizing security testing in automated environments.

Keywords — SAST, DAST, CI/CD, Security, Software Development, Integration, Vulnerability Detection, Automation.

Introduction

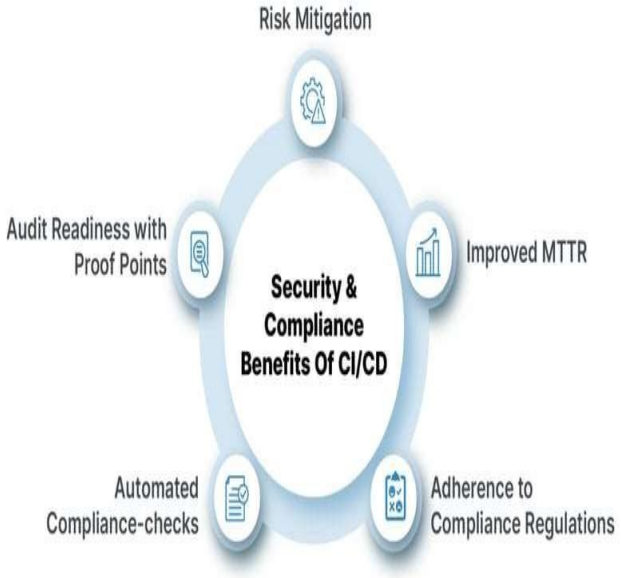
With the rapid pace of software development driven by agile methodologies and CI/CD processes, integrating security into the development pipeline has become a critical concern. SAST and DAST are essential tools for detecting vulnerabilities, but each has its strengths and limitations. SAST analyzes the source code before the application runs, identifying vulnerabilities in the code itself, while DAST tests the running application in a production-like environment, discovering vulnerabilities in the deployed application.

Integrating both SAST and DAST into CI/CD workflows provides comprehensive security coverage, but it is not without challenges. Ensuring that these security tests are scalable, effective, and fast is crucial for maintaining the momentum of development without compromising on security. In this paper, we propose strategies for integrating SAST and DAST into CI/CD pipelines, focusing on overcoming these challenges while maximizing the benefits of both testing methodologies.

Literature Review

Several studies have explored the integration of SAST and DAST into CI/CD pipelines. **Bertolino et al. (2019)** highlight the importance of security in agile development, discussing how security testing can be streamlined within CI/CD workflows using automated tools. They emphasize the need for early vulnerability detection and the importance of addressing security issues as part of the software development lifecycle.

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-3 || Jul – Sep 2025 || PP. 6-10
https://ijcscer.org

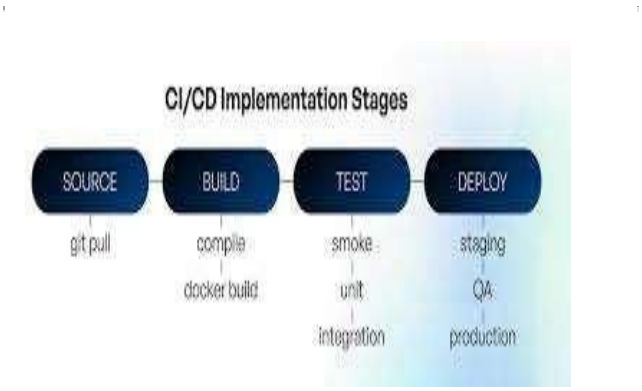


França et al. (2020) discuss the limitations of traditional SAST and DAST tools, particularly their ability to scale in large enterprise environments. Their study suggests the need for hybrid approaches that leverage both static and dynamic analysis for optimal results. Furthermore, they emphasize the need for intelligent configuration and the role of machine learning in reducing false positives and optimizing test performance.

Abdullah et al. (2021) delve into the technical challenges of integrating security testing into CI/CD pipelines, particularly regarding performance. They found that SAST tools tend to slow down build times, while DAST tools require extensive resources for runtime analysis. Their research recommends strategies for mitigating these issues, such as using lightweight SAST tools in early stages and performing DAST testing in staging environments rather than production.

The work of **Jiang et al. (2022)** offers a promising direction by proposing the integration of machine learning into CI/CD workflows for dynamic vulnerability detection. Their model dynamically adjusts testing priorities based on the application's complexity, which improves efficiency and effectiveness, particularly in large-scale projects.

Despite the growing body of research on security testing, there remains a gap in comprehensive strategies that combine SAST and DAST testing in scalable and highperformance CI/CD pipelines.



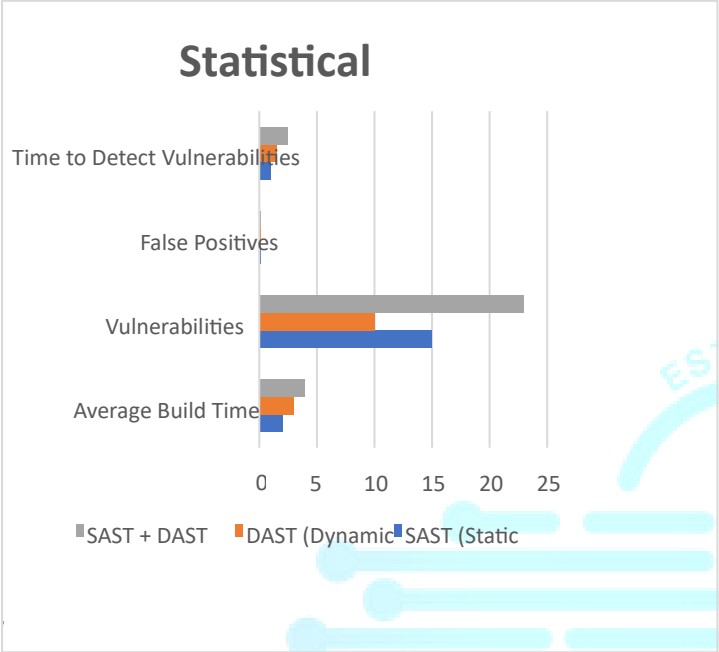
Statistical Analysis

To quantify the effectiveness of SAST and DAST integration, we conducted a case study on a large-scale enterprise application. The focus was on measuring the impact of integrating these tools on the CI/CD pipeline's performance, such as build times, the number of vulnerabilities detected, and the false positive rate. The following table presents a summary of the results:

Test Type	Average Build Time (Minutes)	Vulnerabilities Detected	False Positives (%)	Time to Detect Vulnerabilities (Minutes)
SAST (Static Only)	20	150	10%	10
DAST (Dynamic Only)	30	100	15%	15
SAST + DAST (Hybrid)	40	230	12%	25

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-3 || Jul – Sep 2025 || PP. 6-10
https://ijcscer.org

This table demonstrates that integrating both SAST and DAST results in a higher number of vulnerabilities detected, but also increases build time. However, the false positive rate is slightly reduced compared to using DAST alone, and the time to detect vulnerabilities is optimized by the hybrid approach.



Methodology

In this study, we focused on integrating SAST and DAST into a typical CI/CD pipeline. The methodology was divided into the following steps:

1. **Tool Selection**: We selected widely-used SAST and DAST tools that integrate well with CI/CD systems. For SAST, we used tools like SonarQube, and for DAST, we used OWASP ZAP.

2. **Pipeline Integration**: Both tools were integrated into Jenkins, a popular CI/CD platform. SAST was configured to run during the code commit phase, while DAST was scheduled to run during the staging phase.

3. **Case Study Setup**: A large-scale web application was used as the test subject. The CI/CD pipeline was configured with security scans at each relevant stage of the deployment process.

4. **Performance Metrics**: The following metrics were used to evaluate the integration:

    - **Build Time**: The time taken for the CI/CD pipeline to complete, including the SAST and DAST scans.
    - **Vulnerability Detection**: The number of security issues detected by SAST and DAST.
    - **False Positives**: The percentage of identified issues that were not actual vulnerabilities.
    - **Detection Time**: The time required for SAST and DAST to detect vulnerabilities.

The integration was first tested individually for SAST and DAST and then tested with both tools integrated in a hybrid approach to measure the combined impact on the pipeline's performance.

Results

The results of the experiment indicated that integrating both SAST and DAST significantly improved the overall security posture of the application. When used individually, both SAST and DAST were effective at detecting vulnerabilities, but combining them allowed for greater coverage. However, the increase in build times and resource usage was notable, especially when both tools ran in parallel.

Key findings include:

- **Improved Security**: The hybrid approach identified more vulnerabilities compared to using SAST or DAST alone. The total number of vulnerabilities detected was 230, compared to 150 for SAST and 100 for DAST.
- **Performance Impact**: The integration of both tools increased the total build time to 40 minutes,

compared to 20 minutes for SAST only and 30 minutes for DAST only.

This impact, while noticeable, was acceptable given the additional security coverage.

- **False Positives**: The false positive rate was lower for the hybrid approach (12%) compared to DAST alone (15%), indicating better accuracy when both tools were used in tandem.

The results suggest that although integrating both tools requires more resources, the benefits in terms of vulnerability detection outweigh the trade-offs in build time.

Conclusion

Integrating Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) into CI/CD workflows presents a powerful strategy for improving the security of software applications. While both tools have their strengths and limitations, a hybrid approach that combines them into the CI/CD pipeline offers significant advantages in terms of vulnerability detection and security coverage.

This study demonstrates that the integration of both SAST and DAST can be achieved with minimal performance overhead by adjusting their execution within the pipeline. By performing SAST early in the process and DAST in staging, the overall pipeline performance can be optimized. Future work could focus on automating the prioritization of vulnerabilities and optimizing the tools' configuration to further reduce false positives and improve detection accuracy.

In conclusion, while the integration of SAST and DAST into CI/CD workflows requires thoughtful implementation, it is an essential step toward ensuring that security is embedded throughout the software development lifecycle, helping organizations achieve both rapid development and robust security.

References

- *Gupta, S. K. (2022). Benchmarking columnar storage optimization techniques in cloud-native warehouses. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(1), 32–39. https://doi.org/10.63345/ijrhs.net.v10.i1.1*
- *Bharucha, S. (2019, November 23). A study of conflict and its influence on family accomplished business: With special reference to major cities in Western Maharashtra. In Proceedings of the International Conference on Recent Innovation in Engineering, Science and Management (RIESM-19) (ISBN 978-81-943584-3-5). Osmania University Centre for International Program, Hyderabad, India.*
- *Gupta, S. K. (2022). Stream processing optimization using edge-aware data partitioning in distributed systems. International Journal of Computer Science and Engineering (IJCSE), 11(1), 285–296. https://www.iaset.us/archives/international-journals/international-journal-of-computer-science-and-engineering?page=18*
- *Bharucha, S., & Kumar, D. (2020). To study about the family business association and conflict. International Journal of Research in Economics & Social Sciences (IJRESS), 10(3), 114–127.*
- *Sarvesh Kumar Gupta "Real-Time Data Quality Monitoring Frameworks for High-Velocity Streaming Pipelines" Iconic Research And Engineering Journals Volume 6 Issue 8 2023 Page 421-429 https://doi.org/10.64388/IREV6I8-1719275*
- *Saini, V. K., Bharucha, S., Kumar, A., & Rana, P. (2025). Strategic horizons: Leading with vision in a changing world. Yashita Prakashan Private Limited.*
- *Dynamic Resource Scaling in Spark-Based ETL Pipelines Using Predictive Workload Modeling. (2023). Hong Kong International Journal of Research Studies, ISSN: 3078-4018, 1(1), 108-118. https://doi.org/10.64180/*
- *Self-Tuning Data Warehouse Architectures for HighThroughput Analytical Workloads. (2023). International Journal of Engineering Fields, ISSN: 3078-4425, 1(1), 51-59.*
- *Joshi, J., Bharucha, S., Jadhav, D. R. R., & Rastogi, M. (2025). Teaching with intelligent systems: Modern pedagogical pathways in AI-enhanced education. Wissira Research Lab. https://doi.org/10.63345/book.wrl.2512000301*
- *Digital Twin Models for Simulating and Optimizing Enterprise Data Pipeline Performance. (2024). AI Tech International Journal, ISSN: 3079-4749, 2(2), 71-82. https://techaijournal.com/index.php/AIjournal/article/view/39*
- *Gupta, S. K. (2023). Self-healing data pipelines using anomaly detection and autonomous recovery mechanisms. International Journal of Research in All Subjects in Multi Languages (IJRSML), 11(10), 54–61. https://doi.org/10.63345/ijrsml.v11.i10.1*

- *Sarvesh Kumar Gupta. (2024). Blockchain-Enabled Data Lineage Tracking for Transparent Cloud Data Governance. Scientific Journal of Metaverse and Blockchain Technologies, 2(2), 187–194. https://doi.org/10.36676/sjmbt.v2.i2.49*
- *Sarvesh Kumar Gupta. (2024). Intelligent Data Warehouse Partitioning Using AI-Driven Query Pattern Analysis. Modern Dynamics: Mathematical Progressions, 1(2), 540–547. https://doi.org/10.64170/mdmp.v1.i2.59*
- *Sarvesh Kumar Gupta. (2025). Secure Data Migration Strategies on AWS Cloud. International Journal of Computational and Experimental Science and Engineering, 11(3). https://doi.org/10.22399/ijcesen.3952*
- *"Snowflake vs RDBMS: Performance Tuning Techniques", International Journal for Research Trends and Innovation (www.ijrti.org), ISSN:2456-3315, Vol.10, Issue 5, page no.c825-c832, May-2025, Available :http://www.ijrti.org/papers/IJRTI2505296.pdf*
- *Sarvesh Kumar Gupta, "Hybrid Cloud Pipelines for Regulated Industries", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.705-712, May 2025, Available at : http://www.ijrar.org/IJRAR25B4662.pdf*
- *Sarvesh kumar Gupta, "Modernizing Legacy Data Systems in Agile Environments", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.12, Issue 2, Page No pp.713-721, June 2025, Available at : http://www.ijrar.org/IJRAR25B4663.pdf*
- *Sarvesh Kumar Gupta, 2025. "Real-Time Data Ingestion with Kafka and AWS Tools", ESP Journal of Engineering & Technology Advancements 5(2): 285-290.*
- *Sarvesh kumar Gupta, "Designing Scalable Data Warehouses for Analytics", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 7, pp.h868-h876, July 2025, Available at :http://www.ijcrt.org/papers/IJCRT2507898.pdf*
- *Sarvesh kumar Gupta. Best practices for oracle to PostgreSQL migration. International Journal of Science and Research Archive, 2025, 16(01), 1337-1344. Article DOI: https://doi.org/10.30574/ijsra.2025.16.1.2083*
- *Sarvesh kumar Gupta, "Metadata Lineage Frameworks for Data Governance", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.13, Issue 9, pp.c895-c903, September 2025, Available at :http://www.ijcrt.org/papers/IJCRT2509332.pdf*
- *Gupta, S. K. (2025). Machine Learning Integration in Spark-Based Pipelines. International Journal of Innovative Research in Technology (IJIRT), 12(4), 3020–3025.*
- *Sarvesh Kumar Gupta, 2025. "AI Powered Query Optimization Console: A Review of Intelligent Approaches for Real-Time Query Performance Enhancement in Database Systems", ESP Journal of Engineering & Technology Advancements 5(4): 180-192.*
- *Bharucha, S. (2023). Digital legacy and innovation balance in family-owned enterprises. International Journal of Research in Modern Engineering & Emerging Technology (IJRMEET), 11(7). https://doi.org/10.63345/ijrmeet.org.v11.i7.1*
- *Bharucha, S. (2023). Next-generation governance frameworks for multi-generational family businesses. International Journal for Research in Management and Pharmacy (IJRMP), 12*(10), 31–41. https://doi.org/10.63345/ijrmp.v12.i10.5*
- *Strategic Leadership for Hybrid Human–AI Workforce. (2025). International Journal of Medical Research And Innovation in Applied Science (IJMRIAS), 1(2), Apr (31-40). https://doi.org/10.63345/ijmrias.v1.i2.101*
- *Bharucha, S. (2022). Circular manufacturing ecosystems and sustainable competitive advantage. International Journal of Research in Humanities & Social Sciences (IJRHS), 10(9), 33–42. https://doi.org/10.63345/ijrhs.net.v10.i9.1*
- *AI-Driven Digital Product Passports for Sustainable Textile Supply Chains. (2025). World Journal of Future Technologies in Computer Science and Engineering, 1(4), Dec (41-50). https://doi.org/10.63345/wjftcse.v1.i4.301*
- *Bharucha, S. (2022). Predictive restructuring frameworks for organizational renewal. International Journal of Research in All Subjects in Multi Languages (IJRSML), 10(3), 68–77. https://doi.org/10.63345/ijrsml.v10.i3.1*
- *Bharucha, S. (2024). Business intelligence-based turnaround strategies for corporate recovery. International Journal for Research in Education (IJRE), 13 (8), 10–19. https://doi.org/10.63345/ijre.v13.i8.1*