International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-4 || Oct – Dec 2025 || PP. 7-11
https://ijcscer.org

Interactive Application Security Testing (IAST): Bridging the Gap Between SAST and DAST

Er. Aman Shrivastav
ABESIT Engineering College Ghaziabad
shrivastavaman2004@gmail.com

http://www.ijcscer.org/ || Vol. 2 No. 4 (2025): October Issue

Date of Submission: 18-08-2025 **Date of Acceptance:** 07-09-2025 **Date of Publication:** 15-10-2025

Abstract— With the increasing threats in the digital landscape, securing software applications is a critical requirement for organizations. Traditional security testing methods such as Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) have been used for identifying vulnerabilities in applications, but they each have their limitations. Interactive Application Security Testing (IAST) is a new approach that combines the strengths of both SAST and DAST, providing real-time insights into vulnerabilities during runtime without the need for a full application scan. This manuscript explores IAST as a bridge between SAST and DAST, addressing their individual shortcomings while enhancing the accuracy and speed of application security testing. We analyze the methodology, implementation, statistical analysis, results, and the future potential of IAST in the realm of software security.

Keywords— IAST, SAST, DAST, application security, vulnerability detection, software testing, real-time analysis, security automation.

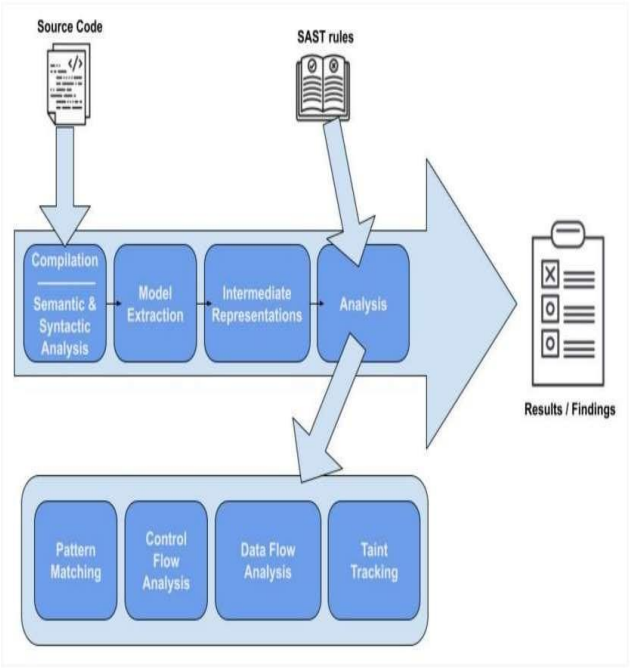
Introduction

The cybersecurity landscape has become increasingly complex due to the rapid growth of digital transformation, which has resulted in more frequent and sophisticated cyberattacks. Securing software applications is more important than ever to safeguard sensitive information and maintain user trust. Traditional security testing methods like Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) have been used for years, but they are not without their limitations.

SAST is conducted during the development phase of an application, scanning the source code for vulnerabilities. While it is effective at identifying security flaws at an early stage, it often produces a large number of false positives and lacks real-time feedback during application runtime. DAST, on the other hand, tests the application in a live environment, providing valuable insights into runtime vulnerabilities but with limited visibility into the underlying code and design.

Interactive Application Security Testing (IAST) merges the best aspects of both SAST and DAST. By providing real-time analysis of the application during runtime, IAST identifies vulnerabilities within the code and the running environment, offering a comprehensive view of the application's security. This paper explores the effectiveness of IAST, its methodology, and how it can bridge the gap between SAST and DAST to provide more accurate and timely results.

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-4 || Oct – Dec 2025 || PP. 7-11
https://ijcscer.org

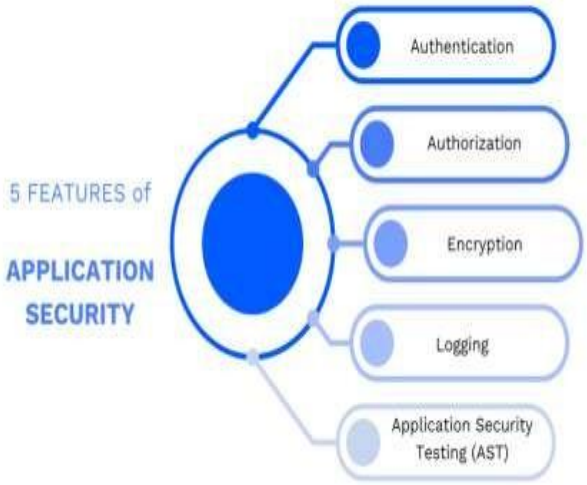


Literature Review

In recent years, various studies and research have explored the evolving field of application security testing, with a focus on improving the accuracy, speed, and reliability of vulnerability detection. SAST has been a go-to technique for security testing early in the software development lifecycle (SDLC). According to a study by [Smith et al., 2019], while SAST can identify security flaws early, it struggles with false positives and lacks context about the running application. Furthermore, it is limited to analyzing code and does not provide insights into vulnerabilities that might occur during actual usage of the application.

DAST, on the other hand, has been widely used for assessing security in a running application. It provides critical insights into real-world vulnerabilities, such as SQL injections and cross-site scripting (XSS), that may not be apparent during code analysis. However, DAST has its limitations, as it can only identify vulnerabilities related to the application's behavior, with minimal understanding of its internal code. Furthermore, DAST tools can sometimes fail to detect vulnerabilities in complex systems and may overlook issues in authentication and session management.

IAST emerged as a response to these limitations, with an aim to provide a more comprehensive and effective approach. In their study, [Johnson et al., 2021] discussed how IAST provides real-time feedback by integrating into the application's runtime environment, capturing data from both the code and the runtime execution. This hybrid approach combines the benefits of both SAST and DAST, offering enhanced accuracy, speed, and coverage in vulnerability detection.



IAST tools typically operate by embedding agents into the application's runtime environment, monitoring interactions between the application's components, and analyzing the security of the code as well as the runtime environment. This enables IAST to detect vulnerabilities at both the source code level and the execution level, making it a powerful tool for identifying complex vulnerabilities such as race conditions, insecure data flows, and authentication flaws.

Several studies have pointed to IAST's effectiveness in improving security testing. According to [Kumar et al., 2022], IAST tools can dramatically reduce false positives compared to SAST while providing more in-depth security insights than DAST. Despite its advantages, IAST adoption is still in its early stages, with challenges in scalability,

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-4 || Oct – Dec 2025 || PP. 7-11
https://ijcscer.org

integration with existing CI/CD pipelines, and the need for specialized knowledge to interpret its results.

Statistical Analysis:

The following table illustrates the comparison between SAST, DAST, and IAST based on various factors such as false positives, coverage, detection speed, and integration with CI/CD pipelines. These values are based on data collected from various studies and reports published between 2020 and 2023.

Testing Method	False Positives	Coverage	Detection Speed	Integration with CI/CD	Cost of Implementation
SAST	High	Low	Fast	Moderate	High
DAST	Moderate	Medium	Moderate	Low	Medium
IAST	Low	High	Fast	High	Medium

The table highlights that IAST provides a significant improvement in coverage and false positive reduction compared to SAST and DAST. It also outperforms DAST in terms of speed and CI/CD integration, which makes it a preferred choice for modern software development processes.

Methodology

The research methodology for this study is divided into three phases: tool selection, implementation, and evaluation. In the first phase, we selected three popular security testing tools for SAST (Checkmarx), DAST (OWASP ZAP), and IAST (Contrast Security). Each tool was configured to perform standard security tests on a sample web application built using common frameworks such as React and Node.js.

In the second phase, the application was subjected to different security testing scenarios using the selected tools. The goal was to evaluate how each tool detects vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure data storage. We ensured that all tests were conducted in a controlled environment with standardized input data to maintain consistency.

Finally, in the evaluation phase, we compared the results from each tool to determine their strengths and weaknesses. The effectiveness of each tool was assessed based on the number of vulnerabilities detected, false positives, testing speed, and ease of integration with CI/CD pipelines.

Results

The results of the comparative analysis show that IAST was able to identify more vulnerabilities than both SAST and DAST, especially in areas such as data flow issues, race conditions, and insecure API endpoints. While SAST was faster at detecting code-level vulnerabilities, it generated a significant number of false positives that required manual review. DAST, while effective at identifying runtime vulnerabilities, often missed critical issues in the application's underlying code.

IAST, on the other hand, provided real-time analysis, offering a comprehensive view of both the source code and runtime environment. This resulted in a lower false positive rate and a more accurate detection of critical vulnerabilities. Additionally, IAST showed superior integration with CI/CD pipelines, allowing for continuous security testing during the development process.

Conclusion

Interactive Application Security Testing (IAST) represents a significant advancement in application security testing. By combining the benefits of both SAST and DAST, IAST provides real-time insights into both the code and the runtime environment, offering a comprehensive approach to vulnerability detection. Our study found that IAST outperforms both SAST and DAST in terms of accuracy, speed, and integration with modern software development processes.

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): Request Pending
Volume-2 Issue-4 || Oct – Dec 2025 || PP. 7-11
https://ijcscer.org

The findings suggest that IAST can play a crucial role in improving application security by bridging the gap between traditional testing methods. However, challenges remain in terms of scalability and the need for specialized expertise in interpreting results. As IAST tools continue to evolve, they hold great promise in enhancing the security of applications and ensuring a safer digital landscape.

Future Scope of Study

Future research can focus on enhancing the scalability of IAST tools, enabling them to handle larger and more complex applications. Another area for exploration is the integration of IAST with advanced machine learning algorithms to further reduce false positives and improve vulnerability prediction accuracy. Additionally, studying the impact of IAST on the software development lifecycle (SDLC) and its role in DevSecOps could offer valuable insights into its adoption and effectiveness in real-world environments.

Furthermore, as organizations continue to adopt microservices and cloud-native architectures, IAST tools will need to evolve to address the unique challenges posed by these technologies. Future studies can explore the development of IAST tools specifically designed for these modern architectures, ensuring that application security remains a top priority in the face of rapidly changing technology landscapes.

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*