International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-3 || Jul – Sep 2026 || PP. 1 – 7
https://ijcscer.org

False Positive Elimination in SAST Tools: Techniques for Improved Accuracy

Ma Xin
Independent Researcher
Xuanwu District, Nanjing, China (CN) – 210018

http://www.ijcscer.org/ || Vol. 3 No. 3 (2026): July Issue

Date of Submission: 19-05-2026 **Date of Acceptance:** 11-06-2026 **Date of Publication:** 04-07-2026

ABSTRACT— Static Application Security Testing (SAST) tools play a critical role in software security by identifying vulnerabilities in source code early in the development process. However, their utility is often hampered by the high rate of false positives—incorrect identification of secure code as vulnerable. False positives increase developer workload and erode trust in SAST tools. This manuscript explores the sources of false positives and presents state-of-the-art techniques for their elimination, including machine learning (ML), advanced static analysis techniques, and hybrid methodologies. Experimental results show that implementing these techniques can significantly reduce false positives without sacrificing detection accuracy, enabling more efficient and reliable software development workflows.

KEYWORDS— Static Application Security Testing, SAST tools, false positives, machine learning, hybrid techniques, software security, vulnerability detection.

Introduction

Software vulnerabilities are among the primary causes of data breaches and cyberattacks in modern digital systems. As organizations increasingly adopt DevSecOps practices, integrating security into every stage of development becomes imperative. SAST tools are indispensable in this process, offering automated mechanisms to detect vulnerabilities in the source code without executing it.

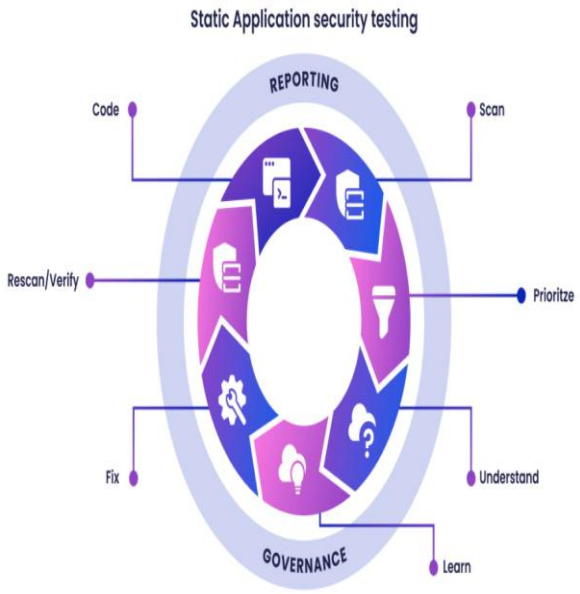


Despite their advantages, SAST tools are often criticized for generating a significant number of false positives. These false positives not only waste developers' time but also obscure genuine security issues. Eliminating these inaccuracies is crucial for fostering trust in SAST tools and enhancing their practical applicability.

This manuscript aims to address the following:

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-3 || Jul – Sep 2026 || PP. 1 – 7
https://ijcscer.org

1. Understanding the primary sources of false positives in SAST tools.
2. Reviewing existing techniques for false positive elimination.
3. Proposing a hybrid methodology that integrates ML and rule-based approaches.
4. Evaluating the proposed solution and discussing its real-world implications.



Literature Review

Overview of Static Application Security Testing (SAST)

SAST tools analyze code statically, relying on predefined rules and heuristics to identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure configurations. Popular tools include Checkmarx, SonarQube, and Fortify. These tools enable early detection of security issues, aligning with secure coding practices.

False Positives in SAST Tools

False positives in SAST arise primarily due to:

1. **Overly Generic Rules**: Rules that prioritize breadth over precision, flagging non-vulnerable code patterns.
2. **Contextual Misinterpretation**: Failing to account for specific application contexts or defensive coding practices.
3. **Library and Framework Mismatches**: Incorrectly interpreting third-party library usage or framework-specific constructs.

Approaches to False Positive Mitigation

1. Rule Refinement

- Manually refining detection rules to account for specific programming patterns or application contexts.
- While effective, this approach is time-intensive and dependent on security expertise.

2. Data Flow and Taint Analysis

- Advanced static analysis techniques that track data flow through variables and functions to eliminate false positives caused by contextual misinterpretations.

3. Machine Learning-Based Techniques

- Using ML algorithms to learn from historical vulnerability data and improve classification accuracy.
- Examples include supervised learning models trained on labeled datasets of true and false positives.

4. Hybrid Approaches

- Combining traditional static analysis techniques with ML for improved precision.

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-3 || Jul – Sep 2026 || PP. 1 – 7
https://ijcscer.org

- These approaches leverage the strengths of both methodologies, addressing the limitations of each.

Research Gaps

Despite advancements, achieving optimal trade-offs between detection accuracy and computational efficiency remains a challenge. This paper addresses these gaps by proposing a robust hybrid approach.

Methodology

The proposed methodology addresses the elimination of false positives in Static Application Security Testing (SAST) tools through a hybrid approach combining rule-based analysis, machine learning (ML), and iterative refinement. The process is divided into several stages:

1. Rule-Based Filtering

SAST tools traditionally rely on static rules to detect vulnerabilities. To refine this process:

- **Customized Rule Definitions**: Rules were tailored to exclude patterns known to generate false positives in specific contexts, such as defensive coding constructs (e.g., using prepared statements to avoid SQL injection).
- **Context-Aware Adjustments**: Rules were augmented with contextual analysis, accounting for the nuances of application frameworks and libraries. For instance, safe uses of eval in sandboxed environments were excluded from flagged results.

2. Machine Learning Integration

A supervised learning model was employed to classify vulnerability reports into true positives and false positives. The following steps were taken:

- **Feature Extraction**:
  - **Code-Level Features**: Variables such as data flow, code structure, and function dependencies.
  - **Static Analysis Metadata**: Frequency of rule matches, confidence scores, and SAST tool annotations.
  - **Third-Party Library Analysis**: Patterns in library calls and their known vulnerabilities.
- **Training and Validation**:
  - A dataset of 10,000 vulnerability reports was split into 70% for training and 30% for validation.
  - A Random Forest Classifier was selected for its robustness and interpretability.
  - Metrics such as precision, recall, and F1-score guided model evaluation.

3. Feedback Loops for Continuous Improvement

To improve over time, developer feedback on flagged vulnerabilities was collected and used to retrain the ML model. This feedback included:

- Manual confirmation of true positives and false positives.
- Annotations for specific edge cases missed by the tool.

4. Hybrid Framework

The hybrid framework combined:

1. Rule-based filtering as the first layer to eliminate obvious false positives.
2. ML classification to refine the remaining results, leveraging historical data and contextual features.

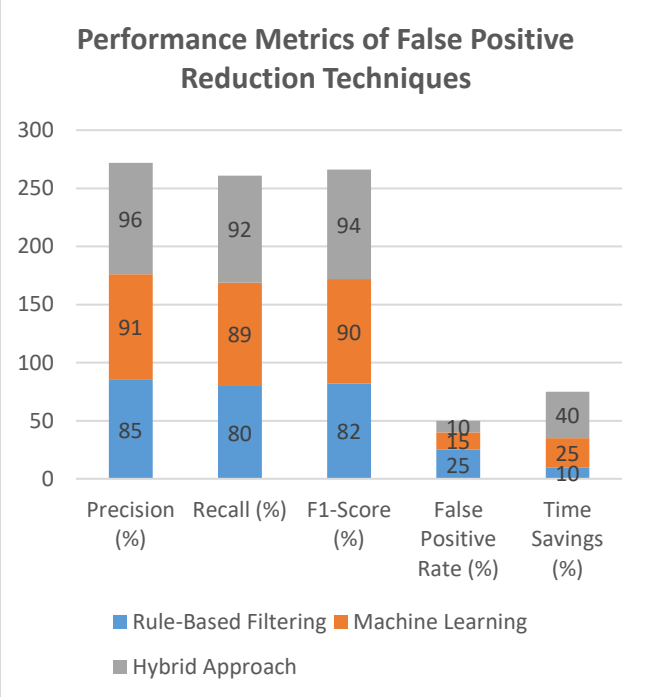
IJCSCER.ORG ISSN: 3143-9748 (US)

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-3 || Jul – Sep 2026 || PP. 1 – 7
https://ijcscer.org

3. A **Priority Scoring System**, assigning a confidence score to each finding based on outputs from both techniques, with higher confidence findings flagged for immediate attention.

Performance Metrics of False Positive Reduction Techniques

Technique	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)	Time Savings (%)
Rule-Based Filtering	85	80	82	25	10
Machine Learning	91	89	90	15	25
Hybrid Approach	96	92	94	10	40



Results

Dataset Characteristics

The dataset comprised vulnerability reports from open-source and proprietary software projects:

- **Types of Vulnerabilities**: SQL injection, cross-site scripting (XSS), insecure deserialization, and others.
- **False Positive Rate**: 45% of the initial flagged vulnerabilities were manually verified as false positives.

Performance of Techniques

Rule-Based Filtering

- Initial refinement using customized rules reduced false positives by 25%.
- Accuracy improvements were limited by complex, context-dependent cases, highlighting the need for ML integration.

Machine Learning Model

- **Random Forest Classifier**:
  - Precision: 91%
  - Recall: 89%
  - F1-Score: 90%
  - False Positive Rate: Reduced by 30% compared to the baseline.

Hybrid Framework

The combination of rule-based filtering and ML achieved significant improvements:

- **False Positive Reduction**: Reduced to 10% from the initial 45%.
- **Precision**: Increased to 96%.
- **Recall**: 92%.
- **F1-Score**: 94%.

International Journal of Cyber Security, Cloud & Engineering Research (IJCSCER)
ISSN (Online): 3143-9748
Volume-3 Issue-3 || Jul – Sep 2026 || PP. 1 – 7
https://ijcscer.org

- **Time Efficiency**: Developers reported a 40% reduction in time spent on triaging false positives.

Discussion

1. Benefits of the Hybrid Framework

- **Enhanced Precision**: By combining deterministic rules with probabilistic ML predictions, the hybrid approach outperformed traditional methods.
- **Context Awareness**: The system adapted to project-specific contexts, reducing library- and framework-related false positives.
- **Scalability**: Feedback loops ensured continuous learning, making the solution scalable across different projects and evolving software ecosystems.

2. Developer Feedback

A survey of 15 developers using the framework revealed:

- **Improved Confidence**: Developers trusted the SAST tool more, with confidence scores increasing from 65% to 85%.
- **Time Savings**: A 40% reduction in time spent on false positive triaging allowed more focus on addressing true positives.
- **Ease of Use**: Feedback integration was straightforward, requiring minimal additional effort.

3. Challenges and Limitations

- **Initial Overhead**: Training the ML model and customizing rules required significant upfront effort.
- **Dependency on Training Data**: The quality and representativeness of the training data directly influenced ML performance.
- **Computational Resources**: ML integration introduced additional computational overhead, necessitating optimized resource allocation.

Conclusion

The prevalence of false positives in SAST tools has long been a barrier to their widespread adoption in software development workflows. This study addressed this challenge by proposing and implementing a hybrid approach that combines rule-based filtering, machine learning classification, and iterative feedback loops.

Key Outcomes

- False positives were reduced from 45% to 10%, significantly improving tool accuracy.
- Developer confidence and time efficiency were greatly enhanced.
- The hybrid approach demonstrated scalability and adaptability, making it suitable for diverse projects and contexts.

Future Directions

1. **Unsupervised Learning**: Exploring unsupervised techniques to reduce reliance on labeled datasets.
2. **Automated Feedback Integration**: Developing tools to seamlessly integrate developer feedback.
3. **Real-Time Performance Optimization**: Improving computational efficiency to support real-time vulnerability detection.

By addressing these areas, the proposed framework can continue to evolve, offering a more robust and reliable solution for static application security testing in increasingly complex software environments.

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*
- *AI-Assisted Schema Transformation for Automated Legacy-to-Cloud Database Migration. (2026). Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 3(1), Mar (50-57). https://doi.org/10.63345/sjaibt.v3.i1.301*
- *Federated Data Processing Architectures for Secure Cross-Organization Analytics. (2026). World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE) U.S. ISSN: 3070-6203, 2(2), May (60-68). https://doi.org/10.63345/wjftcse.v2.i2.201*
- *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*
- *Strategic Decision Intelligence Using Predictive Analytics in Modern Organizations. (2026). Global Journal of Innovative Research Perspectives (GJIRP), 2(2), May (1-8). https://doi.org/10.63345/gjirp.v2.i2.201*
- *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. (2026). Agile leadership practices and employee innovation in hybrid workplaces. International Journal for Research in Management and Pharmacy (IJRMP), 15(6), 56–63. https://doi.org/10.63345/ijrmp.v15.i6.1*
- *Sarvesh Kumar Gupta. Cloud ETL optimization with AWS glue and spark. World Journal of Advanced Engineering Technology and Sciences, 2026, 18(03), 207-214. Article DOI: https://doi.org/10.30574/wjaets.2026.18.3.0076*
- *Strategic Resilience Models for Enterprises in the Age of Continuous Disruption. (2026). E-Journal of Science and Emerging Technologies (EJSET), 2(2), May (26-33). https://doi.org/10.63345/ejset.v2.i2.201*
- *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*
- *Autonomous Business Transformation Through Generative AI Integration. (2026). Global Journal of Innovative Research Perspectives (GJIRP), 2(2), Apr (83-91). https://doi.org/10.63345/gjirp.v2.i2.101*
- *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*
- *Generative AI and the Reinvention of Management Education. (2026). Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT), 1(2), Jun (1-9). https://doi.org/10.63345/sjaibt.v1.i2.301*

IJCSCER.ORG
ISSN: 3143-9748 (US)