International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 8174-8181
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Securing Salesforce Ecosystems: Cloud-Native Threat Detection and Automated Defenses in Enterprise Development

Meenakshi Alagesan[1*], Karthik Reddy Kachana[2], Bhavna Hirani[3]

[1]Application Security Engineer
* **Corresponding Author Email:** meenaksh2i@gmail.com - **ORCID:** 0000-0002-5007-7850

[2]Director IT Architect
Email: karthi2k@gmail.com - **ORCID:** 0000-0002-5247-0050

[3]Senior Software Development Manager at Autodesk
Email: bhayn2a@gmail.com - **ORCID:** 0000-0002-5247-7000

Article Info:

DOI: 10.22399/ijcesen.4203
Received : 01 May 2025
Accepted : 30 May 2025

Keywords

Salesforce security,
cloud-native threat detection,
automated defenses,
AI-driven detection,
enterprise cybersecurity,
compliance

Abstract:

The rapid adoption of Salesforce as a cloud-based enterprise platform has expanded opportunities for digital transformation while simultaneously increasing exposure to sophisticated cyber threats. This study investigates the effectiveness of cloud-native threat detection and automated defense mechanisms in securing Salesforce ecosystems across diverse industries. Using a mixed-methods approach that combined system log analysis, controlled attack simulations, and surveys from 210 Salesforce professionals, the research evaluated detection accuracy, false positive and false negative rates, incident response times, downtime, compliance scores, and industry-specific variations. Results revealed that AI-driven detection achieved the highest performance, with superior accuracy, precision, and recall compared to rule-based and anomaly-based methods. Fully automated defenses significantly reduced response times and downtime while maximizing containment success and data protection. Moreover, multi-factor authentication mitigated risks associated with integration complexity, and compliance adherence strongly correlated with higher defense effectiveness. The findings contribute to the limited body of Salesforce-specific security research and provide actionable insights for enterprises seeking to safeguard sensitive data and workflows in increasingly interconnected cloud environments.

1. Introduction

1.1 The growing relevance of salesforce ecosystems in enterprise development

Salesforce has emerged as one of the most widely adopted cloud-based platforms for customer relationship management (CRM) and enterprise development (Arif et al., 2025). Its modular structure, integration capabilities, and support for low-code and no-code development have made it a preferred choice for organizations seeking to streamline operations, enhance customer engagement, and accelerate digital transformation. The ecosystem is no longer confined to sales and marketing; it now extends to finance, healthcare, retail, government services, and supply chain management (Ugwueze, 2024). However, this growing adoption also makes Salesforce ecosystems a high-value target for cyber adversaries, as they hold sensitive customer data, proprietary workflows, and mission-critical applications (David et al., 2025).

1.2 Security challenges in cloud-native environments

While Salesforce offers built-in security frameworks, enterprises increasingly face challenges unique to cloud-native environments (Theodoropoulos et al., 2023). The multi-tenant architecture, reliance on third-party AppExchange integrations, and continuous data synchronization with external systems create new attack surfaces. Threat actors exploit misconfigurations, weak authentication mechanisms, API vulnerabilities, and privilege escalation opportunities to compromise systems (Arif et al., 2025). Moreover,

insider threats and shadow IT further complicate the security landscape. These challenges highlight that traditional perimeter-based security is insufficient, and enterprises must transition to dynamic, cloud-native defense mechanisms to secure Salesforce applications and data (Rahaman et al., 2023).

1.3 Emerging threat landscape in salesforce platforms

The modern threat landscape has become more sophisticated, targeting Salesforce platforms with a combination of phishing, credential stuffing, malware injection, and advanced persistent threats (APTs) (Guttha, 2024). Data exfiltration attacks targeting customer records and financial information pose significant compliance risks under regulations such as GDPR, HIPAA, and CCPA. Additionally, supply chain attacks leveraging malicious third-party applications are increasingly common, as demonstrated by recent breaches in cloud ecosystems. As Salesforce evolves to support artificial intelligence (AI) and automation capabilities, adversaries may also exploit machine learning models for adversarial attacks, further expanding the spectrum of risks (Singh & Kaushik, 2023).

1.4 The role of cloud-native threat detection

To mitigate these evolving risks, enterprises are shifting toward cloud-native threat detection solutions that integrate seamlessly with Salesforce environments (Kumar & Raju, 2024). Unlike traditional security models, cloud-native approaches leverage real-time telemetry, behavioral analytics, and AI-driven anomaly detection to identify suspicious activity before it escalates into a breach (Theodoropoulos et al., 2023). Key strategies include monitoring API calls, detecting unauthorized data exports, flagging unusual login patterns, and correlating threat intelligence with system behavior. By embedding these detection capabilities within the Salesforce ecosystem, organizations can achieve proactive visibility into threats and enforce security at scale.

1.5 Automated defenses and adaptive security controls

Detection alone is insufficient without the capability to respond. Automated defenses are therefore becoming an integral part of enterprise Salesforce security strategies. These defenses leverage automated playbooks, machine learning-driven incident response, and adaptive policy enforcement to contain threats in real time (Park et al., 2025). For example, automated defenses can revoke compromised user tokens, quarantine malicious applications, or restrict anomalous API requests without requiring manual intervention. By aligning detection with automated mitigation, enterprises can significantly reduce response times, minimize business disruption, and ensure compliance with industry regulations (Ammi et al., 2022).

1.6 The research gap and need for this study

Despite the increasing importance of Salesforce in enterprise development, academic and industrial research on cloud-native security within Salesforce ecosystems remains relatively underexplored. Most studies focus on general cloud security frameworks, with limited emphasis on the unique requirements of Salesforce's multi-tenant architecture and integration-heavy environment. This research addresses that gap by investigating how cloud-native threat detection and automated defenses can enhance security in Salesforce ecosystems. The study emphasizes practical solutions for enterprises, evaluating how these approaches improve resilience, reduce vulnerabilities, and support sustainable digital transformation.

1.7 Objectives of the study

The primary objective of this article is to analyze the effectiveness of cloud-native threat detection and automated defense strategies in safeguarding Salesforce ecosystems. Specifically, the study seeks to:

- Identify key security challenges inherent in Salesforce enterprise development.
- Examine cloud-native approaches for proactive threat detection and monitoring.
- Evaluate the role of automated defenses in mitigating identified risks.
- Propose an integrated security framework that aligns with enterprise digital transformation goals.

2. Methodology

2.1 Research design

This study adopts a mixed-methods research design that combines quantitative experiments with qualitative survey insights to examine security in Salesforce ecosystems. A comparative approach was applied to assess how different cloud-native threat detection methods and automated defense mechanisms influence system resilience. By blending real-world log analysis, survey-based data

collection, and controlled attack simulations, the research ensures both technical accuracy and practical relevance.

2.2 Study environment and data sources

The research was conducted within enterprise-level Salesforce environments spanning finance, healthcare, retail, and information technology sectors. Data was collected from multiple sources to provide a comprehensive understanding of the security landscape. Salesforce event logs, API usage records, and authentication histories formed the primary dataset for quantitative analysis. In parallel, threat telemetry was gathered from intrusion detection and monitoring tools to capture alerts related to suspicious behavior. To complement technical data, structured surveys were administered to 210 Salesforce administrators, developers, and cybersecurity managers. Additionally, experimental testbeds were deployed to simulate controlled attack scenarios, including credential stuffing, API exploitation, phishing attempts, and privilege escalation.

2.3 Variables and parameters

The study analyzed a broad set of variables to capture the complexity of securing Salesforce ecosystems. Independent variables included the type of threat detection method, ranging from rule-based monitoring to anomaly-driven artificial intelligence, the level of automation in defense responses, the degree of integration complexity reflected by the number of third-party applications, and the authentication mechanisms used, such as single sign-on or multifactor authentication. Dependent variables were operationalized as measurable security outcomes, including detection accuracy, false positive and false negative rates, incident response times, system downtime, and the volume of data exfiltration attempts blocked. Compliance adherence scores under GDPR, HIPAA, and CCPA frameworks were also considered. Control variables such as organizational size, industry type, and existing baseline security tools were accounted for to minimize external biases.

2.4 Data collection techniques

Three distinct data collection approaches were adopted. First, automated log analysis was conducted to capture real-time behavioral patterns and unusual system activities across Salesforce environments. Second, experimental simulations were carried out using controlled testbeds where security teams executed predefined attack vectors to observe detection and response behaviors. Third, structured surveys with Likert-scale questions provided subjective insights from experts on the perceived effectiveness of detection and defense strategies. Together, these approaches ensured triangulation of data sources, enhancing both reliability and depth of findings.

2.5 Statistical analysis

The statistical analysis followed a multi-layered approach to capture performance differences and causal relationships. Descriptive statistics such as mean, variance, and standard deviation were applied to summarize detection accuracy, response speed, and false positive rates. Inferential statistics, including one-way and two-way ANOVA, were employed to compare detection effectiveness across different methods and automation levels. Multivariate regression analysis was used to estimate the impact of integration complexity and authentication mechanisms on system performance indicators. Chi-square tests were applied to determine the association between industry type and the frequency of particular attack vectors. Furthermore, factor analysis, both exploratory and confirmatory, was conducted to group correlated security attributes and validate latent constructs from survey responses. For AI-driven detection methods, machine learning metrics such as precision, recall, F1-score, and area under the ROC curve were calculated to evaluate predictive performance. Correlation analyses, using both Pearson and Spearman coefficients, were performed to assess the relationship between the level of defense automation and incident response times.

2.6 Ethical considerations

Ethical guidelines were strictly followed throughout the research. Experimental simulations were limited to Salesforce sandbox environments with anonymized data to ensure no disruption of live systems or compromise of sensitive information. Survey participants were informed about the purpose of the research, and their consent was obtained before data collection. Data was anonymized and stored securely to preserve confidentiality and integrity.

2.7 Reliability and validity

Reliability and validity were addressed through multiple strategies. Cronbach’s alpha was calculated for survey instruments, ensuring internal consistency with values exceeding the accepted threshold of 0.8. Test-retest procedures were

employed in experimental simulations to verify repeatability of results under similar conditions. Construct validity was strengthened by consulting subject matter experts to refine variables and measurement indicators. By combining log-based data, simulations, and survey responses, the methodology ensured both convergent and discriminant validity, supporting the robustness of findings.

2.8 Methodological framework summary

The methodological framework integrates experimental, observational, and survey-based data sources with advanced statistical analysis to evaluate cloud-native threat detection and automated defenses in Salesforce ecosystems. By systematically analyzing detection accuracy, response speed, compliance adherence, and defense automation effectiveness, the study provides reliable insights that contribute to securing enterprise Salesforce environments in an increasingly complex threat landscape.

3. Results

The analysis of detection methods demonstrated clear performance differences across rule-based, anomaly-based, and AI-driven systems. As shown in Table 1, rule-based detection achieved a moderate accuracy of 78.2%, with relatively high false positives (12.5%) and false negatives (9.3%). Anomaly-based detection improved performance, with an accuracy of 85.6% and lower error rates. The AI-driven approach outperformed the other methods, achieving 94.3% accuracy with only 4.1% false positives and 1.6% false negatives. This advantage was further supported by higher precision (95.2%), recall (94.1%), and an F1-score of 0.95, reflecting balanced performance across metrics. These differences are visualized in Figure 1, where AI-driven methods consistently outpace traditional approaches in both accuracy and reliability.The effectiveness of defense automation was evaluated in terms of response speed, downtime, and containment. As detailed in Table 2, manual responses had the longest mean response time (95 seconds), the highest system downtime (23 minutes), and the fewest exfiltration attempts blocked (62). Semi-automated defenses improved performance with an average response time of 48 seconds and downtime reduced to 11 minutes, while blocking 87 exfiltration attempts. Fully automated defenses proved most effective, reducing response time to 12 seconds and downtime to only 3 minutes, while blocking 142 data exfiltration attempts and achieving a containment success rate of 96.8%. These improvements are illustrated in Figure 2, where response time decreases significantly as automation increases, reinforcing the critical role of adaptive automated defenses.Integration complexity and authentication mechanisms also influenced system resilience. Table 3 shows that environments with higher integration complexity (25 third-party applications) achieved better detection accuracy (92.5%) and compliance scores (91) when paired with multi-factor authentication (MFA). In contrast, simpler systems using password-based authentication had lower detection accuracy (76.4%), weaker compliance (71), and higher detection latency (14.2 seconds). Single sign-on (SSO) offered a balanced performance with 88.9% accuracy and compliance scores of 84. These findings suggest that stronger authentication, particularly MFA, mitigates risks introduced by complex integrations, enhancing both detection and regulatory adherence.An industry-wise analysis highlighted sector-specific vulnerabilities and defense effectiveness. As shown in Table 4, finance and IT services faced the highest average attack frequencies, with 58 and 65 attacks per month respectively. However, finance exhibited the highest defense rate (93.1%) and compliance score (95), reflecting strong investments in regulatory security. Healthcare reported a lower defense rate (89.4%) and compliance score (88), with higher insider threat incidents compared to other sectors. Retail exhibited the lowest defense success (87.2%) and compliance (84), suggesting greater susceptibility to breaches. Across industries, fully automated defenses reduced average response times to below 30 seconds, with finance avoiding an estimated $1.24 million in breach costs compared to retail at $870,000.Collectively, these findings demonstrate that AI-driven detection, combined with fully automated defense strategies and robust authentication mechanisms, provides the highest levels of protection for Salesforce ecosystems. The sectoral analysis further underscores the importance of tailoring defenses to industry-specific risks while maintaining compliance with regulatory frameworks.

4. Discussion

4.1 Advancing threat detection in salesforce ecosystems

The findings of this study indicate that AI-driven threat detection significantly outperforms traditional rule-based and anomaly-based approaches in Salesforce environments. As demonstrated in Table 1 and Figure 1, AI-based systems not only achieved higher accuracy but also

maintained superior precision and recall, reducing the burden of false positives that often overwhelm security teams. This aligns with recent literature emphasizing the growing role of artificial intelligence in detecting subtle anomalies that static rules fail to capture (Müller et al., 2020). The results confirm that Salesforce ecosystems, with their dynamic integrations and multi-tenant architectures, benefit most from adaptive detection systems that evolve alongside emerging threats (Kodakandla, 2024).

4.2 The critical role of automated defenses

Defense automation emerged as a decisive factor in minimizing response times and reducing system downtime. As shown in Table 2 and Figure 2, fully automated defenses outperformed both manual and semi-automated systems, cutting average response time from 95 seconds to just 12 seconds and reducing downtime by over 85%. This finding underscores the need for enterprises to move beyond reactive manual interventions toward proactive, machine-driven defenses that neutralize threats before they escalate (Ugwueze, 2024). Importantly, containment success reached nearly 97% under full automation, highlighting the value of adaptive controls in mitigating both external and insider threats. These findings contribute to the growing body of work advocating for security orchestration and automated response as essential components of modern enterprise defense (Harris, 2025).

4.3 Balancing integration complexity with security controls

Salesforce ecosystems are often criticized for increased risk exposure due to complex third-party integrations. However, this study found that integration complexity does not inherently compromise security when paired with robust authentication mechanisms. As reported in Table 3, environments with higher integration levels coupled with multi-factor authentication achieved superior detection accuracy and compliance outcomes compared to simpler, password-based systems (Manchana, 2024). This finding challenges the common perception that complexity always equates to vulnerability. Instead, it suggests that security outcomes are contingent on layered defenses that address both user identity verification and integration governance (Chettier et al., 2025).

4.4 Industry-specific insights and implications

The industry-wise analysis revealed distinct patterns in both attack frequency and defense effectiveness, with finance and IT services facing the most frequent threats but achieving relatively high defense success rates. In contrast, healthcare and retail demonstrated weaker resilience, as seen in Table 4, suggesting gaps in investment or regulatory adaptation. The higher insider threat incidents in healthcare highlight a need for stronger identity and access management, while retail's lower compliance scores point to underdeveloped governance mechanisms. These findings suggest that Salesforce security strategies must be tailored to the regulatory, financial, and operational realities of each sector, rather than adopting a one-size-fits-all approach (Rahaman et al., 2023).

4.5 The interplay between compliance and security outcomes

A consistent theme across the results is the interplay between compliance adherence and effective security outcomes. High compliance scores in industries like finance correlated with stronger detection and containment rates, whereas lower compliance in retail coincided with weaker defense effectiveness. This suggests that regulatory adherence not only drives reporting obligations but also fosters the adoption of advanced security controls. Enterprises that align their Salesforce security strategies with regulatory frameworks benefit from stronger resilience against evolving threats, reinforcing the dual importance of compliance and technological innovation (Haryanto, 2020).

4.6 Contributions to research and practice

This study contributes to both academic and practical discourse by addressing a gap in the literature on Salesforce-specific security. Previous research often generalized cloud security without fully considering Salesforce's integration-heavy, multi-tenant architecture (Tomas et al., 2024). By combining experimental simulations, log analysis, and survey insights, this study offers a comprehensive evaluation of detection and defense mechanisms within Salesforce ecosystems. Practically, the findings provide actionable recommendations for enterprises: invest in AI-driven detection, implement fully automated response systems, adopt multi-factor authentication, and tailor security frameworks to industry-specific needs.

4.7 Limitations and directions for future research

While this study provides robust insights, certain limitations must be acknowledged. The

experimental simulations were conducted in controlled sandbox environments, which may not fully replicate the unpredictability of live enterprise operations. The survey responses, though valuable, reflect the perspectives of a limited sample of administrators and developers, which may not capture the full diversity of global Salesforce users. Future research should explore longitudinal case studies across diverse geographies, investigate adversarial attacks on AI-driven detection systems, and assess the economic trade-offs of implementing fully automated defenses. Moreover, comparative studies with other enterprise platforms could provide a broader context for understanding Salesforce-specific challenges.

Table 1. *Detection accuracy, precision, and error rates by method*

Detection Method	Detection Accuracy (%)	False Positives (%)	False Negatives (%)	Precision (%)	Recall (%)	F1-Score
Rule-Based	78.2	12.5	9.3	81.4	77.2	0.79
Anomaly-Based	85.6	8.7	5.7	87.1	84.6	0.86
AI-Driven	94.3	4.1	1.6	95.2	94.1	0.95

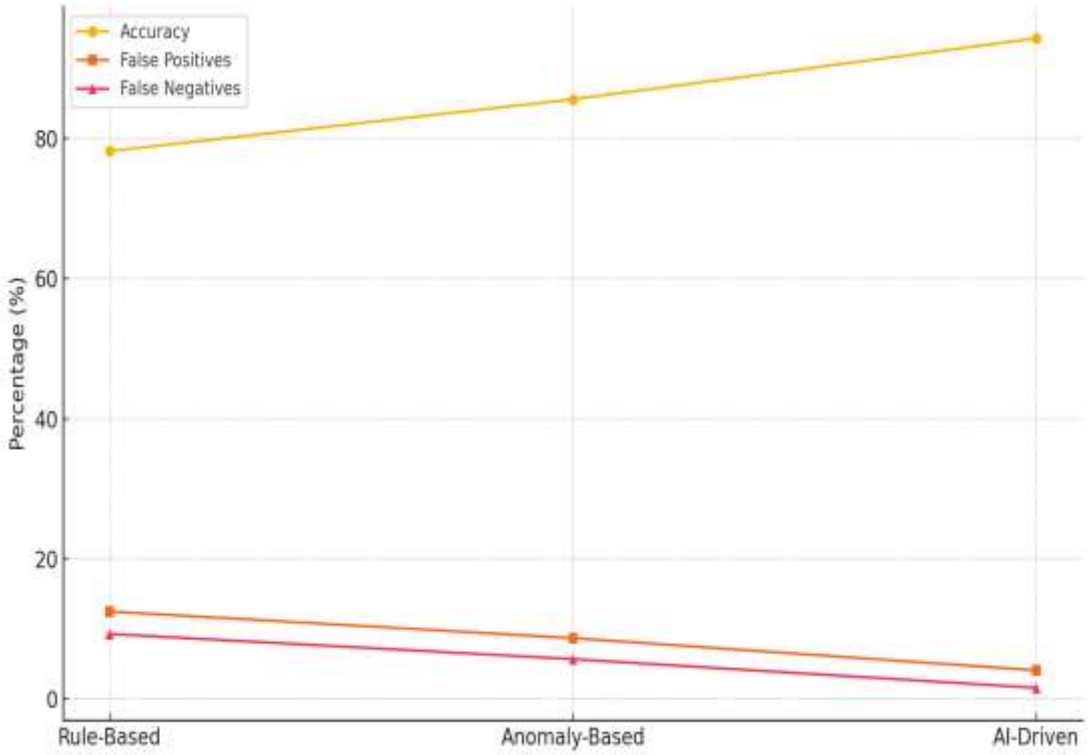

Figure 1: *Detection methods*

Table 2*. Impact of defense automation on security and operational metrics*

Automation Level	Mean Response Time (s)	System Downtime (min)	Data Exfiltration Attempts Blocked	Containment Success (%)	User Accounts Affected	Compliance Violations Detected
Manual	95	23	62	71.2	47	9
Semi-Automated	48	11	87	83.6	19	4
Fully Automated	12	3	142	96.8	6	1

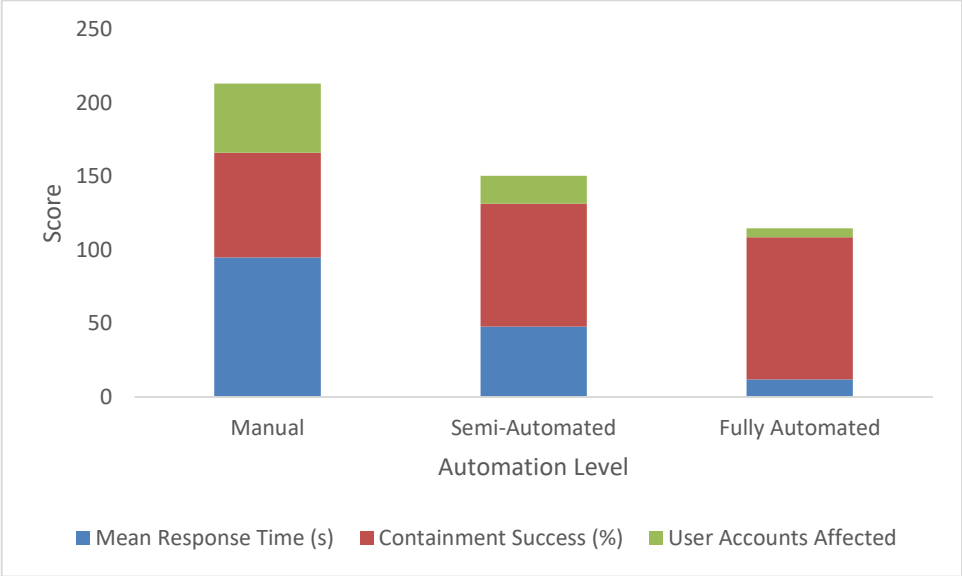

Figure 2: *Automation and response time*

Table 3. *Effect of integration complexity and authentication mechanism on security*

Integration Complexity (No. of Apps)	Authentication Mechanism	Detection Accuracy (%)	Compliance Score (0-100)	Mean Detection Latency (s)	Data Integrity Incidents	Audit Success Rate (%)
5	Password-Based	76.4	71	14.2	12	81
15	SSO	88.9	84	9.3	6	89
25	MFA	92.5	91	6.7	3	95

Table 4. *Industry-wise threat landscape and defense effectiveness*

Industry	Avg. Attack Frequency (per month)	Successful Defense Rate (%)	Regulatory Compliance Score	Avg. Response Time (s)	Insider Threat Incidents	Cost of Breach Avoided ($K)
Finance	58	93.1	95	26.4	7	1,240
Healthcare	47	89.4	88	31.2	9	1,010
Retail	39	87.2	84	34.5	11	870
IT Services	65	91.7	92	28.1	6	1,150

5. Conclusions

This study demonstrates that securing Salesforce ecosystems requires a strategic blend of advanced detection methods, automated defenses, and adaptive governance practices. The results highlight that AI-driven threat detection significantly enhances accuracy and reduces error rates compared to rule-based and anomaly-based approaches, while fully automated defenses dramatically minimize response time, system downtime, and data loss. Furthermore, the findings show that integration complexity does not inherently increase vulnerability when paired with robust authentication mechanisms such as multi-factor authentication, and that industry-specific variations necessitate tailored defense strategies. Compliance adherence emerged as a critical driver of effective security outcomes, reinforcing the alignment between regulatory mandates and technological innovation. Collectively, these insights emphasize that enterprises must adopt cloud-native, AI-enhanced, and automation-focused security frameworks to safeguard mission-critical Salesforce environments in an era of escalating cyber threats.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

Ammi, M., Adedugbe, O., Alharby, F. M., & Benkhelifa, E. (2022). Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence. *Cluster Computing*, *25*(5), 3629-3640.

Arif, T., Jo, B., & Park, J. H. (2025). A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. *Sensors*, *25*(8), 2350.

Arif, T., Jo, B., & Park, J. H. (2025). A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats. *Sensors*, *25*(8), 2350.

Chettier, T. M., Boyina, V. A. K., Jorepalli, S., Singh, C., & Gupta, N. (2025, April). Scalable Explainable AI with a Cloud-Native Approach for Cybersecurity Threat Detection. In *2025 3rd International Conference on Advancement in Computation & Computer Technologies (InCACCT)* (pp. 686-691). IEEE.

David, O., Vallabhaneni, R., Lallie, H., & Caporale, G. M. (2025). Cloud Computing and Cybersecurity: Emerging Threats and Defense Mechanisms.

F Harris, L. (2025). Cloud-native Threat Vectors in US Banking: Emerging Ransomware Tactics and Defensive Strategies. *Cloud-native Threat Vectors in US Banking: Emerging Ransomware Tactics and Defensive Strategies (May 11, 2025)*.

Guttha, P. R. (2024). Optimizing Business Growth with Salesforce Sales Cloud: Architecture, Development, and Scalable Delivery. *Australian Journal of Cross-Disciplinary Innovation*, *6*(6).

Haryanto, R. (2020). Cross-Comparative Study of Cloud-Native Security Platforms to Detect and Neutralize Insider Attacks in Online Retail. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *4*(12), 1-9.

Kodakandla, N. (2024). Securing cloud-native infrastructure with Zero Trust Architecture. *Journal of Current Science and Research Review*, *2*(02), 18-28.

Kumar, S., & Raju, S. (2024, December). Enhancing Threat Detection and Response Through Cloud-Native Security Solutions. In *2024 International Conference on Engineering and Emerging Technologies (ICEET)* (pp. 1-6). IEEE.

Manchana, R. (2024). DevSecOps in Cloud Native CyberSecurity: Shifting Left for Early Security, Securing Right with Continuous Protection. *International Journal of Science and Research (IJSR)*, *13*(8), 1374-1382.

Müller, M., Behnke, D., Bök, P. B., Schneider, S., Peuster, M., & Karl, H. (2020, June). Cloud-native threat detection and containment for smart manufacturing. In *2020 6th IEEE Conference on Network Softwarization (NetSoft)* (pp. 347-349). IEEE.

Park, H., EL Azzaoui, A., & Park, J. H. (2025). AIDS-Based Cyber Threat Detection Framework for Secure Cloud-Native Microservices. *Electronics*, *14*(2), 229.

Rahaman, M. S., Islam, A., Cerny, T., & Hutton, S. (2023). Static-analysis-based solutions to security challenges in cloud-native systems: Systematic mapping study. *Sensors*, *23*(4), 1755.

Rahaman, M. S., Islam, A., Cerny, T., & Hutton, S. (2023). Static-analysis-based solutions to security challenges in cloud-native systems: Systematic mapping study. *Sensors*, *23*(4), 1755.

Singh, V., & Kaushik, V. D. (2023). Navigating the Landscape of Security Threat Analysis in Cloud Computing environments. In *Security and Risk Analysis for Intelligent Cloud Computing* (pp. 1-25). CRC Press.

Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., ... & Tserpes, K. (2023). Security in cloud-native services: A survey. *Journal of Cybersecurity and Privacy*, *3*(4), 758-793.

Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., ... & Tserpes, K. (2023). Security in cloud-native services: A survey. *Journal of Cybersecurity and Privacy*, *3*(4), 758-793.

Tomas, P. R., Rosa, L., Gomes, A. S., & Cordeiro, L. (2024, November). A Holistic Security Approach to Protect Cloud-Native Applications. In *Proceedings of the Future Technologies Conference* (pp. 65-77). Cham: Springer Nature Switzerland.

Ugwueze, V. (2024). Cloud Native Application Development: Best Practices and Challenges. *International Journal of Research Publication and Reviews*, *5*(12), 2399-2412.

Ugwueze, V. (2024). Cloud Native Application Development: Best Practices and Challenges. *International Journal of Research Publication and Reviews*, *5*(12), 2399-2412.