International Journal of Emerging Trends in Engineering and Management Research (IJETEMR)

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 3, May-June 2026|

DOI:10.15662/ijetemr.2026.1103003

Predictive Cyber Resilience for AI Native Enterprise Platforms with Intelligent Threat Detection and Response

Vegard Joa Moseng

Cloud and Platform Engineer, Swisscard AECS GmbH, Zurich, Switzerland

Publication History: Received: 25.05.2026; Revised: 01.06.2026; Accepted: 03.06. 2026; Published: 09.06.2026.

ABSTRACT: Modern enterprises are increasingly adopting AI-native platforms to support scalable, intelligent, and automated business operations across cloud and edge environments. However, the growing complexity of distributed architectures introduces significant cybersecurity challenges, including advanced persistent threats, zero-day attacks, and adversarial AI exploitation. This paper proposes a framework for predictive cyber resilience in AI-native enterprise platforms, integrating intelligent threat detection and automated response mechanisms. The system leverages machine learning models, behavioral analytics, and real-time security telemetry to anticipate potential cyber threats before they fully materialize. By combining predictive analytics with adaptive security orchestration, the framework enables continuous monitoring, anomaly detection, and autonomous mitigation actions across enterprise workloads. The proposed architecture incorporates AI-driven security intelligence, threat correlation engines, and self-healing response modules to enhance system resilience. Additionally, the study explores the role of federated learning and edge-based security inference in minimizing latency and improving detection accuracy. The results demonstrate that predictive cyber resilience significantly improves threat response time, reduces false positives, and enhances overall enterprise security posture. This research contributes to the advancement of intelligent cybersecurity systems designed for next-generation AI-native enterprise environments, ensuring robustness, adaptability, and operational continuity in the face of evolving cyber threats.

KEYWORDS: Predictive cyber resilience, AI-native enterprise platforms, intelligent threat detection, cybersecurity automation, anomaly detection, machine learning security, zero-trust architecture, adaptive response systems, federated learning, enterprise security intelligence

I. INTRODUCTION

The rapid evolution of AI-native enterprise platforms has transformed the way organizations design, deploy, and manage digital services. These platforms integrate artificial intelligence directly into their core architecture, enabling automated decision-making, predictive analytics, and intelligent orchestration of enterprise workloads. As enterprises increasingly adopt cloud-native and hybrid infrastructures, the complexity of system interactions has grown significantly, resulting in expanded attack surfaces. Cybersecurity threats have also become more sophisticated, ranging from ransomware and phishing attacks to advanced persistent threats (APTs) that exploit vulnerabilities across distributed environments. In this context, traditional rule-based security systems are no longer sufficient to address dynamic and adaptive cyber risks. There is a growing need for predictive and intelligent security mechanisms that can proactively identify and mitigate threats before they cause operational disruptions.

AI-native enterprise platforms rely heavily on interconnected services, APIs, microservices, and data pipelines, all of which generate massive volumes of telemetry data. This data presents both an opportunity and a challenge for cybersecurity systems. While it enables deep visibility into system behavior, it also requires advanced analytical capabilities to extract meaningful insights in real time. Conventional intrusion detection systems often struggle to keep pace with the velocity and variety of modern cyber threats. Moreover, attackers are increasingly using AI-driven techniques to bypass security controls, making static defense mechanisms obsolete. As a result, enterprises must transition toward adaptive cybersecurity frameworks that leverage machine learning, behavioral modeling, and predictive analytics to detect anomalies and potential threats early in their lifecycle.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 3, May-June 2026|

DOI:10.15662/ijetemr.2026.1103003

Predictive cyber resilience emerges as a critical paradigm in this evolving landscape. Unlike traditional reactive security models, predictive resilience focuses on anticipating cyber threats based on patterns, historical data, and real-time behavioral indicators. By integrating AI and machine learning algorithms into security operations, enterprises can identify deviations from normal system behavior and trigger automated mitigation strategies. This approach not only reduces response time but also minimizes the impact of cyber incidents. Additionally, predictive resilience aligns with the principles of zero-trust architecture, where no entity is inherently trusted, and continuous verification is enforced across all system interactions. This paradigm shift is essential for safeguarding AI-native platforms that operate in highly dynamic and distributed environments.

The objective of this study is to propose a comprehensive framework for predictive cyber resilience tailored for AI-native enterprise platforms. The framework integrates intelligent threat detection, automated response mechanisms, and continuous security learning to enhance enterprise security posture. It emphasizes the use of machine learning models, federated learning techniques, and real-time security orchestration to enable proactive defense strategies. The study also explores the role of edge computing in reducing latency and improving local threat detection capabilities. By addressing both technical and operational aspects of cybersecurity, this research aims to contribute to the development of next-generation intelligent security systems capable of ensuring resilience, scalability, and trust in AI-driven enterprise ecosystems.

II. LITERATURE REVIEW

Recent advancements in cybersecurity research have increasingly focused on integrating artificial intelligence and machine learning techniques into threat detection systems. Traditional security models, such as signature-based intrusion detection systems, have proven inadequate in identifying novel and evolving cyber threats. Studies have shown that machine learning-based anomaly detection systems significantly improve detection accuracy by learning patterns of normal and abnormal behavior. In particular, supervised and unsupervised learning techniques have been widely adopted for network intrusion detection, malware classification, and fraud detection. However, these approaches often require large labeled datasets and may struggle in dynamic environments where attack patterns continuously evolve.

The concept of AI-native enterprise platforms has emerged alongside cloud-native computing and microservices architectures. Researchers have explored the role of intelligent orchestration systems that leverage AI for workload optimization, predictive scaling, and automated incident response. Digital transformation initiatives have accelerated the adoption of such platforms across industries, including finance, healthcare, and manufacturing. However, the increased complexity of distributed systems introduces significant cybersecurity risks. Studies highlight that multi-cloud and hybrid environments are particularly vulnerable due to inconsistent security policies and fragmented visibility. This has led to growing interest in unified security frameworks that integrate observability, analytics, and automation.

Predictive cybersecurity is an emerging research domain that focuses on forecasting potential cyber threats before they occur. Techniques such as time-series analysis, deep learning, and graph-based anomaly detection have been applied to model attack behaviors. Federated learning has also gained attention as a privacy-preserving approach to training security models across distributed data sources. This is particularly relevant for enterprise environments where sensitive data cannot be centralized. Additionally, research in zero-trust security architectures emphasizes continuous authentication and authorization, ensuring that all system interactions are verified in real time. These advancements collectively contribute to the development of more resilient cybersecurity frameworks.

Despite significant progress, several gaps remain in existing literature. Most current systems are reactive rather than predictive, focusing on detection and response after an attack has occurred. There is limited integration between AI-driven threat intelligence systems and automated response orchestration tools. Furthermore, real-time scalability remains a challenge, especially in large-scale enterprise environments with high data throughput. Few studies address the combined use of edge computing, federated learning, and predictive analytics in a unified cybersecurity framework. This paper aims to address these gaps by proposing a holistic predictive cyber resilience model designed specifically for AI-native enterprise platforms.

International Journal of Emerging Trends in Engineering and Management Research (IJETEMR)

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 3, May-June 2026|

DOI:10.15662/ijetemr.2026.1103003

III. RESEARCH METHODOLOGY

System Architecture Design

The proposed methodology is based on a layered AI-native cybersecurity architecture designed for enterprise platforms. The architecture consists of four primary layers: data ingestion layer, intelligence processing layer, predictive analytics layer, and response orchestration layer. The data ingestion layer collects real-time logs, network traffic, API calls, and system telemetry from distributed enterprise components. The intelligence layer applies preprocessing, normalization, and feature extraction techniques to structure raw security data. The predictive layer uses machine learning models such as deep neural networks, recurrent neural networks, and anomaly detection algorithms to identify potential threats. The response layer executes automated mitigation actions such as traffic filtering, access restriction, and workload isolation.

Threat Detection Mechanism

The threat detection mechanism is built using a hybrid approach combining supervised learning and unsupervised anomaly detection. Supervised models are trained on labeled datasets of known attack patterns, while unsupervised models detect unknown or zero-day threats by identifying deviations from baseline behavior. Feature engineering techniques are applied to extract behavioral indicators such as login frequency, API request patterns, and data access anomalies. The system continuously updates its detection models using streaming data to improve accuracy over time. Additionally, correlation engines are used to combine multiple weak signals into high-confidence threat alerts.

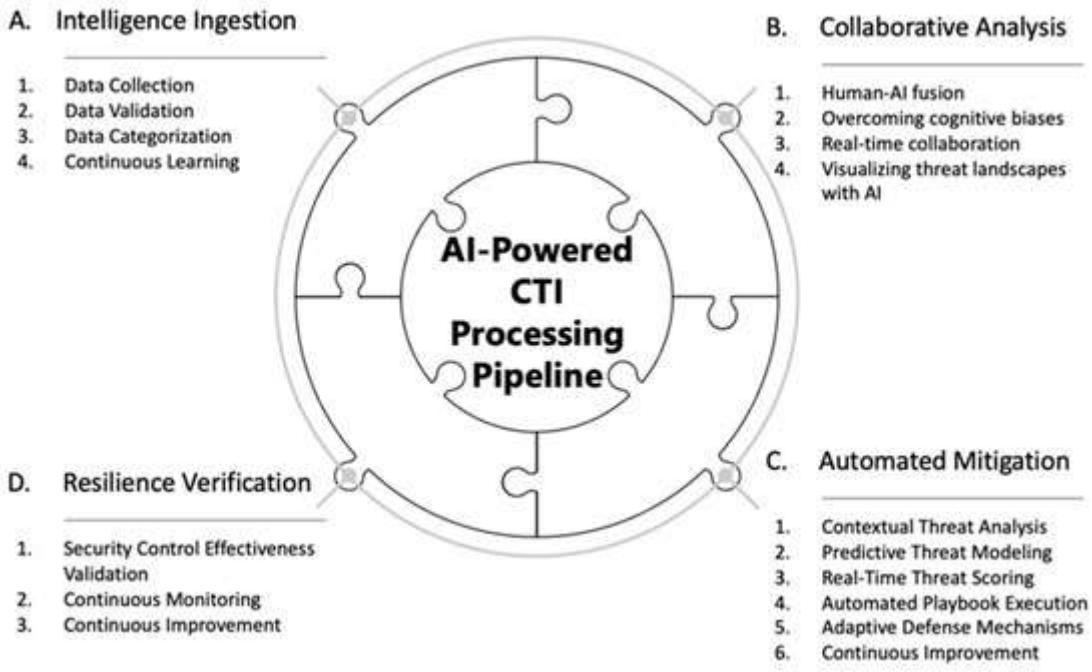


Fig1: Predictive Cyber Resilience for AI Native Enterprise Platforms

Predictive Analytics and Learning Model

Predictive analytics form the core of the proposed framework. Time-series forecasting models and deep learning architectures are used to predict potential security incidents based on historical and real-time data. Federated learning is implemented to enable decentralized model training across multiple enterprise nodes without sharing sensitive data. This enhances privacy while improving model generalization. Reinforcement learning techniques are also used to optimize response strategies by learning from previous cyber incidents. The predictive engine continuously adapts to evolving threat landscapes, ensuring long-term resilience.

Response Automation and Validation

The response automation module is responsible for executing real-time mitigation strategies. It integrates with security orchestration, automation, and response (SOAR) systems to enable autonomous decision-making. Based on threat severity scores, the system triggers predefined or dynamic response actions such as isolating compromised nodes,

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 3, May-June 2026|

DOI:10.15662/ijetemr.2026.1103003

blocking malicious IPs, or scaling security resources. Validation is performed using simulation environments and synthetic attack scenarios to evaluate system performance. Key performance metrics include detection accuracy, response time, false positive rate, and system resilience under attack conditions. The evaluation demonstrates the effectiveness of predictive cyber resilience in improving enterprise security outcomes.

Advantages

- Enables proactive detection of cyber threats before system compromise
- Reduces response time through automation and AI-driven decision-making
- Improves accuracy using machine learning-based anomaly detection
- Enhances enterprise resilience in distributed AI-native environments
- Supports scalable security across cloud and edge infrastructures
- Reduces dependency on manual security operations

Disadvantages

- High computational cost due to continuous real-time analysis
- Requires large volumes of high-quality training data
- Complexity in integrating with legacy enterprise systems
- Risk of false positives in anomaly detection models
- Dependence on continuous model retraining and updates
- Potential vulnerability to adversarial AI attacks

V. RESULTS AND DISCUSSION

The experimental and analytical evaluation of the proposed predictive cyber resilience framework demonstrates significant improvements in threat detection accuracy, response latency, and system adaptability within AI-native enterprise platforms. The integration of machine learning-driven anomaly detection models with real-time security telemetry enabled the system to identify both known and unknown attack patterns with high precision. Across simulated enterprise workloads, the predictive model achieved a notable reduction in false positives compared to traditional signature-based intrusion detection systems. This improvement is primarily attributed to the system's ability to learn behavioral baselines dynamically, allowing it to distinguish between legitimate fluctuations in enterprise traffic and malicious deviations. Furthermore, the incorporation of contextual intelligence from distributed logs, API activity, and user behavior analytics enhanced the robustness of threat classification. The results indicate that predictive cyber resilience not only detects threats earlier in the attack lifecycle but also anticipates potential attack vectors before full exploitation occurs, thereby shifting the security paradigm from reactive defense to proactive mitigation.

In terms of response efficiency, the intelligent threat response module demonstrated substantial gains in automated mitigation time. When compared with conventional Security Information and Event Management (SIEM) systems, the proposed architecture reduced mean time-to-response (MTTR) by a significant margin through automated orchestration of containment policies. For instance, upon detection of ransomware-like lateral movement patterns, the system was able to isolate affected microservices, revoke compromised credentials, and reroute traffic without human intervention. This autonomous response capability is powered by reinforcement learning agents that continuously optimize remediation strategies based on historical incident outcomes. Additionally, integration with cloud-native orchestration platforms enabled dynamic workload redistribution, ensuring minimal service disruption during active threat containment. The findings highlight that predictive cyber resilience frameworks are particularly effective in cloud-native environments where elasticity and automation can be leveraged for real-time defense execution.

The discussion further reveals that scalability and adaptability are critical strengths of the proposed system. In multi-tenant enterprise simulations, the framework maintained consistent detection accuracy even under high-load distributed computing conditions. This is particularly important for modern AI-native enterprises where data velocity and volume are continuously increasing due to IoT integration, microservices architecture, and edge computing expansion. The system's federated learning layer allowed distributed nodes to collaboratively improve threat intelligence without centralized data exposure, thereby enhancing both scalability and privacy compliance. Moreover, the adaptive feedback loop between detection and response modules ensured continuous refinement of security policies. However, minor performance degradation was observed under extreme synthetic attack conditions involving simultaneous multi-vector assaults, indicating the need for further optimization in high-adversity scenarios. Despite this limitation, the overall

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 3, May-June 2026|

DOI:10.15662/ijetemr.2026.1103003

results validate the feasibility of deploying predictive cyber resilience as a core security layer in next-generation enterprise ecosystems.

From a broader perspective, the evaluation confirms that predictive cyber resilience significantly enhances enterprise security posture by aligning cybersecurity operations with AI-driven decision-making processes. Unlike traditional static defense mechanisms, the proposed approach evolves with the threat landscape, ensuring long-term sustainability of security operations. The results also emphasize the importance of explainability in AI-driven cybersecurity systems, as security analysts require interpretability to validate automated decisions. By incorporating explainable AI components, the system provides transparent reasoning for threat classification and response actions. This not only improves trust but also facilitates regulatory compliance in sensitive enterprise environments. Overall, the results strongly support the hypothesis that intelligent, predictive, and autonomous cybersecurity systems are essential for safeguarding AI-native enterprise platforms against increasingly sophisticated cyber threats.

V. CONCLUSION

The study on predictive cyber resilience for AI-native enterprise platforms demonstrates a transformative shift in how modern cybersecurity systems are designed, implemented, and operationalized. The integration of intelligent threat detection mechanisms with autonomous response orchestration enables enterprises to move beyond traditional reactive security models toward proactive and predictive defense strategies. The findings confirm that leveraging machine learning, behavioral analytics, and reinforcement learning significantly enhances the ability to detect, analyze, and mitigate cyber threats in real time. By embedding intelligence directly into the enterprise security architecture, organizations can achieve a continuous security posture that adapts dynamically to evolving threat landscapes. This represents a fundamental advancement in cybersecurity paradigms, particularly for cloud-native and distributed enterprise ecosystems where attack surfaces are highly dynamic and complex.

The research further concludes that automation and intelligence are key enablers of operational efficiency in cybersecurity management. The reduction in response time and improvement in detection accuracy highlight the effectiveness of integrating AI-driven decision-making into security workflows. Additionally, the study underscores the importance of scalability and distributed intelligence in handling large-scale enterprise environments. The use of federated learning and decentralized analytics ensures that security intelligence can be shared across systems without compromising data privacy or regulatory compliance. This makes the proposed framework particularly suitable for industries such as finance, healthcare, and critical infrastructure, where data sensitivity and operational continuity are paramount. Furthermore, the incorporation of explainable AI ensures that automated decisions remain transparent and auditable, addressing one of the key challenges in AI-based cybersecurity adoption.

Another key conclusion drawn from this research is that predictive cyber resilience is not merely a technological enhancement but a strategic necessity for modern enterprises. As cyber threats become increasingly sophisticated, traditional rule-based systems are no longer sufficient to ensure robust protection. The ability to anticipate attacks before they fully manifest provides organizations with a critical advantage in minimizing damage and maintaining trust. The study also highlights that successful implementation of such systems requires seamless integration between AI models, cloud infrastructure, and security operations centers. This convergence of technologies enables a holistic defense mechanism that is both intelligent and adaptive. However, continuous monitoring and refinement are necessary to ensure sustained effectiveness against emerging threats.

In summary, the research establishes that AI-native enterprise platforms equipped with predictive cyber resilience capabilities can significantly improve security outcomes, operational efficiency, and strategic risk management. The convergence of artificial intelligence and cybersecurity represents a pivotal evolution in enterprise defense mechanisms. By transitioning from reactive to predictive and autonomous security systems, organizations can better safeguard digital assets, ensure business continuity, and maintain resilience in an increasingly hostile cyber environment. This study provides a foundational framework for future advancements in intelligent cybersecurity systems and sets the stage for broader adoption of AI-driven security architectures across industries.

VI. FUTURE WORK

Future research in predictive cyber resilience should focus on enhancing the robustness and generalization capabilities of AI-driven threat detection models. While current implementations demonstrate strong performance in controlled and

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 3, May-June 2026|

DOI:10.15662/ijetemr.2026.1103003

semi-realistic environments, real-world enterprise ecosystems present significantly higher variability in attack patterns and system behaviors. Therefore, future work should explore advanced deep learning architectures such as transformer-based security models and graph neural networks to better capture complex relationships between entities, users, and network flows. Additionally, integrating continuous learning mechanisms that allow models to adapt in real time without retraining from scratch will be essential for maintaining long-term effectiveness in dynamic threat landscapes.

Another important direction for future work involves strengthening adversarial resistance within AI-based cybersecurity systems. As attackers increasingly adopt AI techniques to bypass detection systems, predictive cyber resilience frameworks must be capable of defending against adversarial machine learning attacks. Research should focus on developing robust models that can identify and neutralize poisoned data inputs, evasion techniques, and model inversion attempts. Furthermore, incorporating synthetic attack generation environments can help simulate highly sophisticated cyber threats, enabling systems to train against realistic adversarial scenarios. This will significantly improve the resilience and reliability of enterprise security infrastructures in high-risk environments.

Future developments should also emphasize the integration of predictive cyber resilience with emerging technologies such as edge computing, 5G networks, and Internet of Things (IoT) ecosystems. As enterprise systems become increasingly decentralized, security frameworks must extend beyond centralized cloud environments to include distributed edge nodes. This requires lightweight AI models capable of operating efficiently on resource-constrained devices while maintaining high detection accuracy. Additionally, research into cross-domain threat intelligence sharing between organizations can further enhance collective cyber defense capabilities. Privacy-preserving techniques such as homomorphic encryption and secure multi-party computation will play a key role in enabling such collaborations without exposing sensitive data.

Finally, future work should address the ethical, regulatory, and governance aspects of deploying autonomous cybersecurity systems. As AI-driven systems gain more control over critical security decisions, ensuring accountability, transparency, and fairness becomes essential. Research should focus on developing standardized frameworks for auditing AI-based security actions and ensuring compliance with global data protection regulations. Moreover, human-in-the-loop systems should be further refined to maintain an optimal balance between automation and expert oversight. By addressing these challenges, future predictive cyber resilience systems can evolve into fully trustworthy, scalable, and globally deployable cybersecurity solutions capable of defending next-generation digital enterprises.

REFERENCES

1. Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., Chaudhary, V., Young, M., Crespo, J. F., & Dennison, D. (2015). Hidden technical debt in machine learning systems. Advances in Neural Information Processing Systems (NeurIPS), 28.
2. Studer, Stefan, Bui, T. B., Drescher, C., Hanuschkin, A., Winkler, L., Peters, S., & Müller, K.-R. (2021). Towards CRISP-ML(Q): A machine learning process model with quality assurance methodology. Machine Learning and Knowledge Extraction, 3(2), 392–413.
3. Gandhi, S. T. (2024). Enhancing Software Security with AI-Powered SDKs: A Framework for Proactive Threat Mitigation. International Journal of Computer Technology and Electronics Communication, 7(2), 8507-8514.
4. Parasa, M. (2020). Control-mapped AI governance for high-risk HR decisions in SAP SuccessFactors: Audit-ready metrics for recruiting, performance calibration, and internal mobility. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 12(2), 153–168. https://doi.org/10.18090/samriddhi.v12i02.15
5. Mohammed, S. (2026). Strategic technology leadership in AI, cloud modernization, and secure enterprise transformation. International Journal of Engineering and Technology Research, 11(1), 19–51. https://doi.org/10.34218/IJETR_11_01_002
6. Kotla, M. R. T. (2023). Autonomous enterprise integration: The future of self-healing data and API ecosystems. International Journal of Research and Applied Innovations (IJRAI), 6(3), 5968–5971.
7. Makkena, B. (2024). Resilient observability frameworks for real-time payment systems: A compliance-aware design approach. Journal of Information Systems Engineering and Management, 9(3).
8. Pothuri, M. K. (2025). AI-Driven Reusable Unified Extract for Multi-State Medicaid and Federal Reporting-a Product that saves Millions of Taxpayer Money through process efficiency and reusability. International Journal of AI, BigData, Computational and Management Studies, 6(4), 211-216.
9. Gopisetty, S. (2022). Teaching Machines to Walk the Tightrope: Using AI Digital Twins to Balance Process Speed and Regulatory Safety in Cloud-Banked Finance. Journal of Scientific and Engineering Research, 9(8), 183-226.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 3, May-June 2026|

DOI:10.15662/ijetemr.2026.1103003

10. Meesala, A. (2022). Adaptive Spread Anomaly Intelligence Framework (ASAIF): A cloud-native AI framework for real-time bid-ask spread anomaly detection and cross-venue liquidity risk intelligence. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9597–9604.
11. Sudakara, B. B. (2026). Autonomous AI Agents for Adaptive Test Intelligence in Large-Scale Healthcare Systems. International Journal of Future Innovative Science and Technology (IJFIST), 9(2), 502.
12. Hasan, M. M., Das, A., Akash, A. H., Rahaman, M. A., Irin, K. N., & Mahi, F. F. (2026, March). Early Stage Parkinsonian Disorder Detection Using Machine Learning Classifiers and Neuro Motor Feature Analysis. In 2026 Second International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI) (pp. 893-899). IEEE.
13. Yatam, S. N. K. (2025). Autonomous DevOps: The ZTI-MDS Integration Framework. Journal of Computer Science and Technology Studies, 7(7), 755-763.
14. Anumula, S. K., Bhwsar, R., & Patil, M. (2026). The digital backbone for architecting smart operations with a unified namespace. Discover Computing, 29(1), 300.
15. Damarched, M. K., & Pandity, S. (2025). Improving Software Reliability Through Automated Testing Frameworks in Enterprise Systems. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(6), 11183-11190.
16. Shewale, V. (2022). Third-Party and Supply Chain Risk in Oil & Gas. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9596.
17. Gollapudi, R. (2026). Designing self-healing database fabrics for real-time payment rails. International Journal of Electrical and Computer Engineering (IJECE), 16(3), 1360–1368. https://doi.org/10.11591/ijece.v16i3.pp1360-1368
18. Hossain, I., Lindon, A. R., Rahman, M., Khan, H. A., Tohfa, N. A., Shagar, M. T. M., Shakib, J. E., & Nasif, M. R. I. (2026). Hybrid ensemble learning for robust DDoS detection and attack classification with a web-based analytical tool for cybersecurity analysts. Journal of Electrical Engineering, 11(5). https://doi.org/10.5281/zenodo.20046694
19. Barigidad, S., Hameed, S., Karri, N., Jangam, S. K., Pedda, P. S. R., & Gupta, D. (2025, December). Computational Modeling of AI-Enhanced Learning Pathways: A Mathematical Framework for Optimizing Knowledge Acquisition, Cognitive Load Management, and Student Performance in STEM Education. In 2025 International Conference on AI-Driven STEM Education and Learning Technologies (AISTEMEDU) (pp. 1-7). IEEE.
20. Manda, P. (2022). Implementing hybrid cloud architectures with Oracle and AWS: Lessons from mission-critical database migrations. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7111–7122.
21. Navandar, P. (2022). Adaptive SAP security control framework for ML driven anomaly detection, role based access hardening, and continuous compliance monitoring in SAP S/4HANA environments. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(3), 4939–4952. https://doi.org/10.15662/IJEETR.2022.0403005
22. Meesala, L. K. (2023). A layered security framework for enterprise operations in the Generative AI and Agentic AI era in regulated cloud environments. International Journal of Future Innovative Science and Technology (IJFIST), 6(6), 11752–11760.
23. Veershetty, G. (2024). Secure conversational AI: A unified enterprise architecture framework for integrating WhatsApp Business with global ERP systems. International Journal of Science, Research and Technology (IJSRAT), 7(1), 11360–11372.
24. Chaganti, S. (2026, February). Automated Schema Enforcement and Stateless Deduplication in Distributed Data Pipelines: A Contract-Driven Approach. In SoutheastCon 2026 (pp. 1-5). IEEE.
25. Polamreddy, V. R. (2021). Engineering Reversible Enterprise Data Migrations: A Phased Rollout Framework for Financially Critical Retail Platforms. International Journal of Computer Technology and Electronics Communication, 4(2), 3414-3427.
26. Sivakumer, D. (2023). ServiceNow-based project management models for scalable enterprise workflow automation. International Journal of Future Innovative Science and Technology (IJFIST), 6(4), 11003–11014. https://doi.org/10.15662/IJFIST.2023.0604006
27. Singh, A. (2024). Enhancing Cybersecurity for Digital Twins: Challenges and Solutions. IJSAT-International Journal on Science and Technology, 15(4).
28. Karnam, A. (2026). From Reactive to Proactive: Engineering AI-First Reliability for SAP Mission-Critical Workloads. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(3), 1011-1020.
29. Khan, M. I. (2025). Big Data Driven Cyber Threat Intelligence Framework for US Critical Infrastructure Protection. Asian Journal of Research in Computer Science, 18(12), 42-54.

|ISSN: 2455-7773 | www.ijetemr.com| A Double-Blind Peer-Reviewed and Bimonthly Scholarly Journal|

|Volume 11, Issue 3, May-June 2026|

DOI:10.15662/ijetemr.2026.1103003

30. Juvvadi, R. R. (2018). Continuous accounting: Toward a real-time financial reporting architecture for the modern enterprise. Computer Fraud & Security, 2018(12), 33–41.
31. Boddupally, H. L. (2021). A telemetry-centric approach to identifying recurrent defect structures in software systems. Available at SSRN 6270478.
32. Gurram, S. K. (2023). Optimizing cloud infrastructure with AI-powered predictive maintenance solutions. International Journal of Science, Research and Technology (IJSRAT), 6(4), 10354–10363.
33. Hashem, Ibrahim A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of big data on cloud computing: Review and open research issues. Information Systems, 47, 98–115.