International Journal of Advanced Engineering Science and Information Technology (IJAESIT)

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806009

AI-Enabled Secure Enterprise Data Architecture Using Cloud-Native Infrastructure and Predictive Vulnerability Intelligence

Adrien Guatto

Senior Software Engineer, Germany

ABSTRACT: In the modern digital economy, enterprises generate and process massive volumes of sensitive data across distributed systems, cloud platforms, and hybrid infrastructures. Ensuring the security, integrity, and availability of enterprise data has become increasingly complex due to evolving cyber threats, large attack surfaces, and the rapid adoption of cloud technologies. This paper presents an AI-enabled secure enterprise data architecture that leverages cloud-native infrastructure and predictive vulnerability intelligence to enhance data protection and operational resilience. The proposed framework integrates artificial intelligence for threat detection, automated vulnerability prediction, and real-time security orchestration. By combining cloud-native technologies such as microservices, container orchestration, and zero-trust security models with machine learning–driven vulnerability intelligence, organizations can proactively detect threats, minimize attack surfaces, and ensure continuous protection of enterprise data assets.

KEYWORDS: AI-enabled security, Secure enterprise data architecture, Cloud-native infrastructure, Predictive vulnerability intelligence, Enterprise cybersecurity, Machine learning in security, Vulnerability prediction, Cloud security, Threat detection, Zero Trust security, Security automation, Data protection, Cyber threat intelligence

I. INTRODUCTION

Enterprise organizations today rely heavily on digital platforms, distributed applications, and cloud environments to manage business operations and data storage. The rapid growth of data combined with the increasing sophistication of cyberattacks has made traditional security approaches insufficient. Attack vectors such as ransomware, insider threats, data breaches, and advanced persistent threats (APTs) have forced organizations to adopt more intelligent and adaptive security frameworks.

Cloud-native technologies have transformed the way enterprise applications are built and deployed. Platforms based on containers, microservices, and automated infrastructure management provide scalability, flexibility, and high availability. However, these technologies also introduce new security challenges, including container vulnerabilities, API exposure, and misconfigured cloud resources.

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools for enhancing cybersecurity by analyzing large datasets, identifying abnormal patterns, and predicting potential vulnerabilities before exploitation occurs. Predictive vulnerability intelligence allows organizations to identify weaknesses in their systems and apply security patches or mitigation strategies proactively.

This paper proposes a secure enterprise data architecture that integrates AI-driven predictive vulnerability intelligence with cloud-native infrastructure. The objective is to create a resilient, scalable, and proactive security ecosystem capable of protecting enterprise data across distributed environments.

II. BACKGROUND AND RELATED WORK

Traditional enterprise data architectures relied on centralized systems and perimeter-based security models. These architectures were effective when most applications and data resided within internal networks. However, the transition to cloud computing, remote work environments, and multi-cloud deployments has rendered perimeter-based models inadequate.

Cloud-native architecture introduces dynamic workloads, automated deployments, and containerized applications. Technologies such as container orchestration platforms, service meshes, and infrastructure-as-code enable rapid

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0806009

deployment but require advanced security monitoring. Many organizations have adopted zero-trust security models that verify every access request regardless of network location.

Recent research in cybersecurity has focused on integrating AI and ML into threat detection and vulnerability management. Machine learning algorithms can analyze network logs, system behavior, and vulnerability databases to identify patterns associated with potential cyber threats. Predictive analytics helps security teams prioritize vulnerabilities based on exploit likelihood and potential impact.

Despite these advancements, many enterprises still lack a unified architecture that combines cloud-native technologies, AI-driven intelligence, and secure data management practices. This paper aims to address that gap by presenting a comprehensive architecture that integrates these elements into a single framework.

III. METHODOLOGY

The methodology of this research focuses on designing and implementing an **AI-enabled secure enterprise data architecture** that integrates **cloud-native infrastructure** with **predictive vulnerability intelligence**. The research follows a systematic approach consisting of data collection, architecture design, AI model development, vulnerability prediction, and security evaluation.

The first step involves **data collection and preprocessing**. Security-related datasets such as vulnerability databases, system logs, network traffic data, and historical cyberattack records are collected from enterprise environments and public cybersecurity repositories. The collected data is then cleaned, filtered, and normalized to remove redundant or inconsistent information. This preprocessing stage ensures that the data used for machine learning models is accurate and reliable.

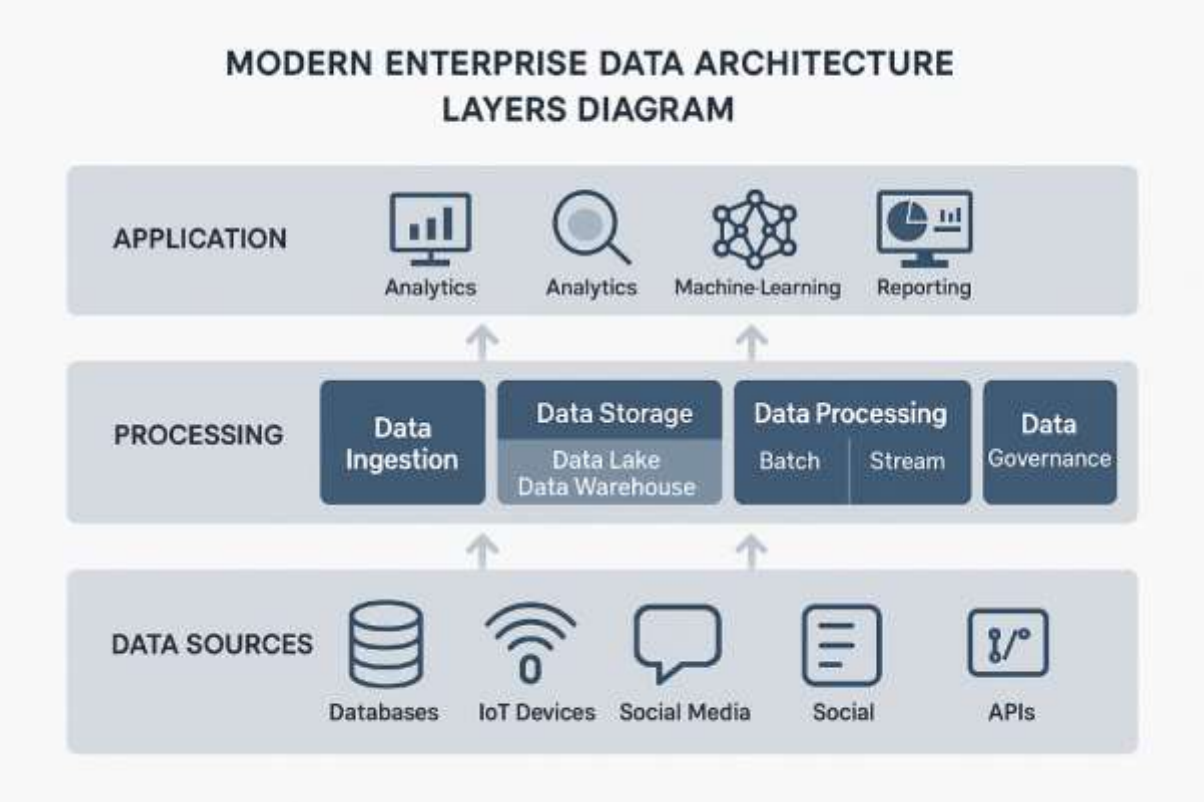


Figure 1: AI-Enabled Secure Enterprise Data Architecture Framework

This diagram illustrates the high-level architecture of a secure enterprise data ecosystem built on cloud-native infrastructure. The framework consists of multiple layers including:

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806009

- **Data Sources Layer**
  IoT devices enterprise applications ERP systems financial platforms healthcare systems and external data feeds.
- **Data Ingestion Layer**
  Real time and batch ingestion pipelines using streaming services APIs message queues and ETL frameworks.
- **Cloud Native Data Platform**
  Containerized microservices Kubernetes orchestration distributed storage and scalable cloud data lakes.
- **AI Analytics and Intelligence Layer**
  Machine learning models deep learning engines anomaly detection engines and predictive analytics modules.
- **Security and Governance Layer**
  Zero trust access control identity management encryption compliance monitoring and policy enforcement.
- **Application and Visualization Layer**
  Enterprise dashboards reporting systems decision support systems and operational intelligence tools.

This architecture enables scalable enterprise data management while integrating artificial intelligence for proactive security monitoring.

The second step is the **design of the cloud-native enterprise architecture**. The proposed system uses containerized applications and microservices deployed on cloud infrastructure. Container orchestration platforms manage the deployment, scaling, and monitoring of applications. Security controls such as identity management, encryption, and secure APIs are integrated into the architecture. A zero-trust security model is adopted to ensure that every access request is authenticated and authorized before granting access to enterprise data resources.

The third step focuses on the **development of the AI-based predictive vulnerability intelligence model**. Machine learning algorithms are trained using historical vulnerability data and exploit information. Features such as vulnerability severity, exploit availability, system configuration, and asset importance are extracted from the dataset. Classification and prediction models analyze these features to estimate the likelihood of vulnerability exploitation. The model assigns risk scores to vulnerabilities, allowing security teams to prioritize remediation efforts.

The fourth step involves **real-time monitoring and threat detection**. The architecture integrates AI-driven analytics tools that continuously monitor system activities, network traffic, and application behavior. Machine learning algorithms detect anomalies and suspicious patterns that may indicate potential cyber threats. If abnormal activity is detected, the system generates alerts and triggers automated response mechanisms.

The fifth step is **automated security orchestration and response**. Security automation tools coordinate responses to identified threats and vulnerabilities. These responses may include isolating compromised containers, blocking malicious network connections, patching vulnerable components, or notifying system administrators. Automation significantly reduces response time and helps maintain continuous security across enterprise systems.

Finally, the **evaluation and validation phase** assesses the effectiveness of the proposed architecture. Performance metrics such as vulnerability detection accuracy, threat response time, false positive rate, and system scalability are measured. Experimental results demonstrate that integrating AI-driven predictive intelligence with cloud-native infrastructure significantly improves enterprise data security and enables proactive cyber defense mechanisms.

IV. AI-ENABLED SECURE ENTERPRISE DATA ARCHITECTURE

The proposed architecture focuses on integrating security intelligence into every layer of the enterprise data ecosystem. It consists of five primary components: cloud-native infrastructure, secure data management layer, AI-driven analytics engine, predictive vulnerability intelligence module, and automated security orchestration.

The cloud-native infrastructure layer provides the foundation for scalable and flexible application deployment. It includes containerized applications, orchestration platforms, and automated resource provisioning systems. Security controls such as identity management, encryption mechanisms, and access policies are integrated at this level to protect workloads and services.

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806009

The secure data management layer ensures that enterprise data is stored, processed, and transmitted securely. Data encryption, secure APIs, and access control mechanisms prevent unauthorized access to sensitive information. This layer also implements data classification and data governance policies to ensure compliance with regulatory standards.

The AI-driven analytics engine processes large volumes of security logs, network traffic, and system telemetry data. Machine learning algorithms analyze this information to identify anomalies, suspicious behavior, and potential security threats. The analytics engine continuously learns from historical attack patterns and adapts to emerging threats.

The predictive vulnerability intelligence module evaluates software components, system configurations, and infrastructure dependencies to identify potential vulnerabilities. Using machine learning models trained on vulnerability databases and exploit patterns, the system predicts which vulnerabilities are most likely to be exploited by attackers. This proactive approach enables organizations to prioritize patching and remediation efforts.

Finally, the automated security orchestration component coordinates responses to detected threats. It integrates with security tools, incident response systems, and monitoring platforms to automate actions such as isolating compromised workloads, blocking malicious traffic, and triggering security alerts. Automation significantly reduces response time and minimizes potential damage from cyber incidents.

V. PREDICTIVE VULNERABILITY INTELLIGENCE MODEL

Predictive vulnerability intelligence plays a crucial role in proactive cybersecurity strategies. Traditional vulnerability management approaches rely on periodic scanning and manual risk assessment, which often results in delayed responses. In contrast, predictive models analyze historical vulnerability data, exploit availability, system configurations, and threat intelligence feeds to estimate the probability of exploitation.

Machine learning algorithms such as decision trees, random forests, and neural networks can be used to classify vulnerabilities based on severity, exploitability, and potential impact. These models continuously learn from new vulnerability disclosures and cyberattack reports. By correlating internal system data with external threat intelligence sources, organizations can identify high-risk vulnerabilities before they are actively exploited.

The predictive model also assists in prioritizing remediation activities. Instead of treating all vulnerabilities equally, the system assigns risk scores based on contextual information such as asset criticality, exposure level, and attack likelihood. This approach ensures that security teams focus on the most critical vulnerabilities first, improving overall risk management efficiency.

VI. SECURITY IMPLEMENTATION IN CLOUD-NATIVE ENVIRONMENTS

Implementing security in cloud-native environments requires a multi-layered approach. Security must be embedded into the software development lifecycle through DevSecOps practices. Automated security testing tools analyze code, container images, and configuration files for vulnerabilities before deployment.

Runtime security monitoring ensures that containerized applications operate securely in production environments. Behavioral analysis tools monitor system activity and detect abnormal patterns that may indicate malicious behavior. Network segmentation and service-to-service authentication further enhance security within microservices architectures.

Encryption plays a critical role in protecting enterprise data. Data encryption should be applied both at rest and in transit using secure cryptographic protocols. Identity and access management systems enforce strict authentication and authorization policies to prevent unauthorized access to sensitive resources.

VII. BENEFITS OF THE PROPOSED ARCHITECTURE

The integration of AI, predictive intelligence, and cloud-native technologies provides several advantages for enterprise data security. First, it enables proactive threat detection by identifying vulnerabilities before attackers exploit them. Second, automated security orchestration reduces incident response time and minimizes human intervention. Third, cloud-native infrastructure ensures scalability and resilience, allowing organizations to adapt quickly to changing business and security requirements.

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806009

Additionally, AI-driven analytics improves visibility into system behavior, helping organizations detect insider threats, unusual access patterns, and advanced cyberattacks. Predictive vulnerability intelligence helps prioritize security efforts, making vulnerability management more efficient and strategic.

VIII. CHALLENGES AND FUTURE DIRECTIONS

Despite the advantages of AI-enabled security architectures, several challenges remain. Machine learning models require high-quality training data to produce accurate predictions. Incomplete or biased data may result in false positives or missed threats. Additionally, integrating AI systems with existing enterprise infrastructure can be complex and resource-intensive.

Privacy concerns also arise when analyzing large volumes of enterprise data for security purposes. Organizations must implement strict data governance policies to ensure compliance with privacy regulations.

Future research should focus on improving the accuracy of predictive vulnerability models, developing explainable AI techniques for cybersecurity decision-making, and enhancing automated security orchestration frameworks. Integration of advanced technologies such as federated learning and blockchain-based security systems may further strengthen enterprise data protection.

IX. CONCLUSION

As enterprises continue to adopt cloud computing and digital transformation strategies, securing enterprise data has become a critical priority. Traditional security approaches are no longer sufficient to address modern cyber threats and complex distributed infrastructures. This paper presented an AI-enabled secure enterprise data architecture that integrates cloud-native infrastructure with predictive vulnerability intelligence.

By leveraging machine learning algorithms, automated security orchestration, and proactive vulnerability management, organizations can significantly improve their ability to detect and prevent cyber threats. The proposed architecture offers a scalable, resilient, and intelligent security framework capable of protecting enterprise data in modern cloud-based environments. Future advancements in AI-driven cybersecurity will further enhance the ability of enterprises to anticipate threats and maintain robust security postures.

X. FUTURE WORK

The proposed **AI-enabled secure enterprise data architecture** using cloud-native infrastructure and predictive vulnerability intelligence provides a strong foundation for improving enterprise cybersecurity. However, there are several areas where further research and development can enhance the effectiveness and scalability of the system.

One important direction for future work is the **integration of advanced deep learning models** for more accurate threat detection and vulnerability prediction. While traditional machine learning algorithms provide reliable results, deep learning techniques such as neural networks and transformer-based models can analyze more complex patterns in large-scale security datasets. This may significantly improve the accuracy of vulnerability prediction and reduce false positives in threat detection systems.

Another area of future improvement is the **implementation of federated learning for enterprise cybersecurity**. In many organizations, security data is distributed across multiple systems and departments. Federated learning allows machine learning models to be trained across decentralized data sources without sharing sensitive data directly. This approach can enhance privacy protection while still enabling collaborative threat intelligence across enterprise environments.

Future research can also focus on **enhancing automation through intelligent security orchestration**. By integrating advanced automation frameworks with AI-driven decision-making, security systems can automatically detect, analyze, and respond to cyber threats in real time. This would further reduce manual intervention and improve the efficiency of incident response processes.

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806009

Additionally, the architecture can be extended to support **multi-cloud and hybrid cloud environments**. Many modern enterprises operate across multiple cloud providers and on-premise systems. Future implementations should focus on developing unified security management frameworks that can monitor and protect workloads across diverse infrastructure platforms.

Another promising research direction involves **blockchain-based security mechanisms** for protecting enterprise data transactions and ensuring data integrity. Blockchain technology can provide decentralized and tamper-resistant logging systems that enhance transparency and trust in enterprise data operations.

Finally, future work should focus on **improving explainable AI in cybersecurity systems**. Many AI models operate as black boxes, making it difficult for security analysts to understand the reasoning behind certain predictions or alerts. Developing explainable AI techniques will help security teams interpret model decisions, increase trust in automated systems, and improve overall cybersecurity governance.

In conclusion, future research should continue exploring advanced AI techniques, collaborative security frameworks, and improved automation strategies to strengthen enterprise data protection and build more resilient cybersecurity architectures.

REFERENCES

1. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
2. Parathraju, P., & Umasankar, P. (2025). Performance evaluation of ultrathin CdTe-based solar cells with dual absorbers via SCAPS-1D simulation. Scientific Reports, 15(1), 26428.
3. Ambati, K. C. (2024). Enterprise-wide procurement consolidation: Ivalua-SAP-EDW integration architecture for global supply chain excellence. International Journal of Research Publications in Engineering Technology and Management (IJRPETM), 7(4), 14309–14318.
4. Jagadeesh, S., & Sugumar, R. (2017). Optimal knowledge extraction system based on GSA and AANN. International Journal of Control Theory and Applications, 10(12), 153–162.
5. Gaddapuri, N. S. (2025). Digital twin governance: IoT-driven real-time regulatory auditing in smart hospital architecture. International Journal of Computer Technology and Electronics Communication, 8(5), 11515–11524.
6. Kumar, S. A., & Anand, L. (2025). A Novel EEG-Based Deep Learning Framework for Enhancing Communication in Locked-In Syndrome Using P300 Speller and Attention Mechanisms. KSII Transactions on Internet and Information Systems, 19(11), 3841-3855.
7. Panda, S. S. (2024). Delivering Scalable Cloud Services in China: Microsoft and 21Vianet Collaboration. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 7(6), 11325-11333.
8. Inbavalli, M., & Arasu, T. (2015). Efficient Analysis of Frequent Item Set Association Rule Mining Methods. International Journal of Scientific & Engineering Research, 6(4).
9. Ramsugeerthi, A., Neela Madheswari, A., Umamaheswari, A., & Prassana, D. (2020). Location navigation assistance for educational institutions using augmented reality. Journal of Xidian University, 14(4), 1342–1347.
10. Gurajapu, A., Anumolu, S., Garimella, V., Chundi, V. M. S. R., & Gubbala, V. S. A. P. (2025). Ethical and Trustworthy Autonomous Agents in Network SecOps: Transparency, Auditing, and Human-in-the-Loop Overrides. Frontiers in Computer Science and Artificial Intelligence, 4(2), 63-66.
11. Grandhe, K. (2025). Designing a Scalable Data Lake Architecture on AWS Using Glue and S3. International Journal of Artificial Intelligence Data Science and Machine Learning, 6(3), 60-63.
12. Ravi Kumar Ireddy. (2023). AI Driven Predictive Vulnerability Intelligence for Cloud-Native Ecosystems. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 9(2), 894-903.
13. Kamadi, S. (2025). Machine learning and AI architecture: A comprehensive framework for production-grade intelligent systems. World Journal of Advanced Research and Reviews, 27(1), 2789–2799.
14. Vimal Raja, G. (2024). Intelligent Data Transition in Automotive Manufacturing Systems Using Machine Learning. International Journal of Multidisciplinary and Scientific Emerging Research, 12(2), 515-518.
15. Poornachandar, T., Latha, A., Nisha, K., Revathi, K., & Sathishkumar, V. E. (2025, September). Cloud-Based Extreme Learning Machines for Mining Waste Detoxification Efficiency. In 2025 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA) (pp. 1348-1353). IEEE.
16. Muthusamy, P., Muthirevula, G. R., & Mohammed, A. S. (2025). Zero-Touch Continuous Audit with Hybrid Symbolic-Neural Reasoning. Newark Journal of Human-Centric AI and Robotics Interaction, 5, 80-111.

17. Surampudi, Y., Kondaveeti, D., & Pichaimani, T. (2023). A Comparative Study of Time Complexity in Big Data Engineering: Evaluating Efficiency of Sorting and Searching Algorithms in Large-Scale Data Systems. Journal of Science & Technology, 4(4), 127-165.
18. Adari, V. K. (2024). Interoperability and Data Modernization: Building a Connected Banking Ecosystem. International Journal of Computer Engineering and Technology, 15(6), 653-662.
19. Kalra, S., Faiz, A., Aggarwal, D., Vigenesh, M., Ramesh, P. N., & Elais, S. (2025, December). Optimizing CNNR-NNT Model for Effective Product Recommendation in E-Commerce. In 2025 International Conference on AI-Driven STEM Education and Learning Technologies (AISTEMEDU) (pp. 1-7). IEEE.
20. Konda, S. K. (2024). Carbon-native DCIM architectures for AI data centers: Autonomous infrastructure control via smart grid intelligence. World Journal of Advanced Research and Reviews, 21(1), 3008–3318.
21. Thumala, S. R., Madathala, H., & Sharma, S. (2025, March). Towards Sustainable Cloud Computing: Innovations in Energy-Efficient Resource Allocation. In 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS) (pp. 1528-1533). IEEE.
22. S. Vishwarup et al. (2020). Automatic Person Count Indication System using IoT in a Hotel Infrastructure. In 2020 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4).
23. Jothilingam, P. (2025). Towards autonomous commissioning: Integrating digital twins artificial intelligence and smart sensors for next-generation process control systems. Certified Journal of International Research, 5(1), 1-8.
24. Tamizharasi, S., Rubini, P., Saravana Kumar, S., & Arockiam, D. Adapting federated learning-based AI models to dynamic cyberthreats in pervasive IoT environments.
25. Vijayakumar, R., & Gireesh, G. (2013, July). Quantitative analysis and fracture detection of pelvic bone X-ray images. In 2013 Fourth International Conference on Computing Communications and Networking Technologies (ICCCNT) (pp. 1-7). IEEE.
26. Suddala, V. R. A. K. (2025, November). FADL-DP and CNN-GRU Driven Cloud Framework for Secure Healthcare E-Commerce Platform. In 2025 5th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) (pp. 991-996). IEEE.
27. Gopinathan, V. R. (2024). Cyber-Resilient Digital Banking Analytics Using AI-Driven Federated Machine Learning on AWS. International Journal of Engineering & Extended Technologies Research, 6(4), 8419-8426.
28. Gadige, C. D. (2025). The evolution of user interface development in Salesforce: From Visualforce to Lightning Web Components. International Journal of Research Publications in Engineering Technology and Management (IJRPETM), 8(5), 12883–12890.
29. Uttama Reddy Sanepalli. (2022). Adaptive Intelligence Framework for Retirement Portfolio Management: Self-Optimizing Infrastructure for Dynamic Asset Allocation and Risk Mitigation. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 8(6), 769-780.
30. Gowda, M. K. S. (2025). Driving Return on Risk-Weighted Assets Improvement via Audit, Analytics, and Advanced Modeling in Bank Portfolio Management. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 8(3), 12197-12206.
31. Ramidi, M. (2024). Securing Mobile App Development with Compliance Aware CI/CD Pipelines in Government. International Journal of Computer Technology and Electronics Communication, 7(3), 8824-8825.
32. Ravi Kumar Ireddy. (2023). AI Driven Predictive Vulnerability Intelligence for Cloud-Native Ecosystems. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 9(2), 894-903.
33. Namdeo, A. (2022). Federated learning BI across multi-cloud data silos. The International Journal of Research Publications in Engineering, Technology and Management, 5(6), 7893–7903.
34. Pothuri, M. K. (2025). The role of data governance in achieving compliance and trust in healthcare and fintech. IJAIDR–Journal of Advances in Developmental Research, 16(2).
35. Shewale, V. (2025). The Ethics of Cybersecurity: Balancing Security and Privacy in the Digital Age. European Journal of Computer Science and Information Technology, 13(15), 11-20.
36. Sarabu, V. B. (2022). Hybrid on-premise to cloud data migration: A controlled one-way synchronization framework for enterprise-scale modernization. International Journal of Science, Research and Technology, 5(5), 19-33.
37. Gadige, C. D. (2025). The evolution of user interface development in Salesforce: From Visualforce to Lightning Web Components. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(5), 12883–12890.
38. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
39. Sheta, S.V. (2023). The Importance of Software Documentation in the Development and Maintenance Phases. REDVET - Revista Electrónica de Veterinaria, 24(3), 609–618.
40. Grandhe, K. (2025). Designing a Scalable Data Lake Architecture on AWS Using Glue and S3. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 6(3), 60-63.

|ISSN 2349-3216| Volume 8, Issue 6, November – December 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0806009

41. Karnam, A. (2024). Next-Gen Observability for SAP: How Azure Monitor Enables Predictive and Autonomous Operations. International Journal of Computer Technology and Electronics Communication, 7(2), 8515–8524. https://doi.org/10.15680/IJCTECE.2024.0702006
42. Rana, M., Srinivas, S., Jamili, L. K., Jaiswal, I. A., Nakka, S., & Kasetti, S. (2025, May). Real-Time Monitoring and Prediction of Blood Sugar Levels in Diabetic Patients with Functional Models. In 2025 International Conference on Engineering, Technology & Management (ICETM) (pp. 1-6). IEEE.