International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 4, July -August 2025 |

DOI:10.15662/IJEETR.2025.0704012

AI-Driven Cyber-Resilient Cloud-Native Architecture for Autonomous Enterprise Systems and Secure Digital Ecosystems

Nicola Tonellotto

Senior Systems Engineer, Spain

ABSTRACT: The rapid advancement of digital technologies and cloud computing has enabled enterprises to develop autonomous systems capable of managing complex operations with minimal human intervention. However, this transformation has also increased cybersecurity risks due to highly distributed infrastructures, interconnected services, and continuously evolving cyber threats. To address these challenges, this paper proposes an **AI-driven cyber-resilient cloud-native architecture** designed to support autonomous enterprise systems and secure digital ecosystems. The proposed framework integrates artificial intelligence, cloud-native technologies, automated threat detection, and adaptive security mechanisms to ensure system resilience against cyberattacks. By leveraging machine learning models for predictive threat analysis and automated incident response, the architecture strengthens enterprise cybersecurity while maintaining system availability and operational continuity. The framework emphasizes proactive defense strategies, real-time monitoring, and self-healing capabilities that enable organizations to maintain secure and resilient digital environments.

KEYWORDS: AI-driven cybersecurity, Cyber resilience, Cloud-native architecture, Autonomous enterprise systems, Digital ecosystem security, Machine learning security, Threat detection, Security automation, Resilient infrastructure, Enterprise cybersecurity

I. INTRODUCTION

The emergence of cloud-native technologies has significantly transformed enterprise computing environments. Modern organizations increasingly rely on microservices, containerized applications, and distributed cloud infrastructures to deliver scalable and flexible digital services. Autonomous enterprise systems, powered by artificial intelligence and automation, are becoming essential for improving operational efficiency, decision-making, and service delivery.

While these technological advancements provide numerous benefits, they also introduce new cybersecurity challenges. Cloud-native infrastructures consist of dynamic workloads, APIs, containers, and interconnected services that expand the attack surface. Cyber threats such as ransomware, advanced persistent threats, and insider attacks can exploit vulnerabilities within these distributed systems, potentially causing significant disruptions and data breaches.

Cyber resilience has emerged as a critical concept in modern cybersecurity strategies. Unlike traditional security models that focus primarily on preventing attacks, cyber resilience emphasizes the ability of systems to **detect, withstand, recover from, and adapt to cyber incidents**. For autonomous enterprise systems operating in complex digital ecosystems, cyber resilience ensures continuous operation even during security incidents.

Artificial intelligence plays a crucial role in achieving cyber resilience. AI algorithms can analyze vast amounts of security data, detect anomalies, predict potential vulnerabilities, and automate threat response processes. When integrated with cloud-native architecture, AI-driven cybersecurity mechanisms enable organizations to create adaptive and self-protecting systems.

This paper proposes an **AI-driven cyber-resilient cloud-native architecture** that integrates intelligent threat detection, automated recovery mechanisms, and secure infrastructure design to support autonomous enterprise systems and protect digital ecosystems.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 4, July -August 2025 |

DOI:10.15662/IJEETR.2025.0704012

II. LITERATURE REVIEW

The increasing adoption of cloud computing and digital transformation across enterprise environments has led to significant advancements in cybersecurity research. Organizations are shifting toward **cloud-native architectures**, which utilize microservices, containers, and distributed systems to improve scalability and operational efficiency. However, these technologies also introduce new security challenges due to dynamic workloads, expanded attack surfaces, and complex system interactions. Researchers have emphasized the need for advanced security frameworks that combine artificial intelligence, automation, and cyber resilience to protect modern enterprise systems.

Several studies highlight the importance of **cloud-native security architectures** in protecting enterprise infrastructures. Traditional perimeter-based security models are no longer effective in highly distributed environments where applications and services operate across multiple cloud platforms. Cloud-native security approaches focus on integrating security mechanisms directly into the development and deployment process, often referred to as DevSecOps. These approaches ensure that security controls such as identity management, encryption, and access policies are embedded into the application lifecycle.

Artificial Intelligence (AI) has emerged as a powerful tool in modern cybersecurity systems. AI-based models can analyze large volumes of system logs, network traffic, and user activity data to detect patterns associated with cyber threats. Machine learning algorithms are widely used for anomaly detection, malware classification, intrusion detection, and predictive vulnerability analysis. Researchers have demonstrated that AI-driven threat detection systems can identify cyberattacks faster and more accurately than traditional rule-based security mechanisms.

Cyber resilience has also become a critical research area in enterprise cybersecurity. Unlike traditional security strategies that focus solely on preventing attacks, cyber resilience emphasizes the ability of systems to detect, withstand, respond to, and recover from cyber incidents. Researchers have proposed resilient architectures that incorporate automated recovery mechanisms, redundancy strategies, and adaptive security frameworks. These systems are designed to maintain operational continuity even when cyberattacks occur.

Recent studies have also explored the integration of **AI-driven security analytics with cloud-native infrastructures** to create intelligent cybersecurity systems. These frameworks use predictive analytics and behavioral analysis to identify potential vulnerabilities and abnormal system activities before they escalate into major security incidents. AI-based threat intelligence platforms continuously learn from historical attack patterns and real-time security data, enabling proactive defense strategies.

Despite these advancements, existing research indicates several challenges in implementing AI-driven cybersecurity frameworks. Many studies highlight issues related to data quality, model transparency, and computational complexity. Additionally, integrating AI security systems with large-scale enterprise infrastructures requires careful design and resource management.

Overall, the literature indicates that combining **AI-driven cybersecurity mechanisms, cloud-native architectures, and cyber resilience strategies** provides a promising approach for securing modern enterprise systems and digital ecosystems. The proposed architecture in this research builds upon these concepts by integrating intelligent threat detection, automated response mechanisms, and resilient infrastructure design to enhance enterprise cybersecurity capabilities.

III. METHODOLOGY

The development of the proposed architecture follows a structured methodology consisting of architecture design, data collection, AI model development, cyber resilience implementation, and system evaluation.

The first stage involves designing a **cloud-native architecture** that supports distributed applications and autonomous enterprise operations. The architecture utilizes containerized applications and microservices deployed across scalable cloud environments. Container orchestration platforms manage application deployment, scaling, and service availability. Security controls such as identity management, encrypted communication, and secure API gateways are integrated into the infrastructure.

The second stage focuses on **data collection and monitoring**. Security logs, system performance metrics, network traffic data, and user activity records are continuously collected from cloud infrastructure and enterprise applications. This data is essential for training AI models and identifying potential security threats.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 4, July -August 2025 |

DOI:10.15662/IJEETR.2025.0704012

The third stage involves **AI-based threat detection and predictive analytics**. Machine learning algorithms analyze historical and real-time data to detect abnormal behavior patterns, potential vulnerabilities, and cyberattack indicators. Behavioral analysis models establish baseline activity profiles for users, applications, and systems. Any deviation from these profiles triggers security alerts and initiates further investigation.

The fourth stage implements **cyber resilience mechanisms** within the architecture. These mechanisms include automated threat response, dynamic resource isolation, self-healing infrastructure, and rapid system recovery. When the AI system detects a security threat, automated response tools isolate compromised components, restore affected services, and prevent further system damage.

The final stage evaluates the effectiveness of the proposed architecture using **performance metrics** such as threat detection accuracy, system recovery time, resilience capability, and operational efficiency. These metrics help determine how effectively the architecture maintains security and operational continuity in autonomous enterprise environments.

AI-Driven Cyber Resilient Architecture

The proposed architecture consists of several interconnected layers designed to provide comprehensive cybersecurity protection.

The **cloud infrastructure layer** provides the foundation for scalable and flexible computing resources. It supports containerized applications, distributed storage systems, and network services. Security mechanisms such as encryption, network segmentation, and secure configuration management protect the infrastructure from unauthorized access.

The **application and microservices layer** hosts enterprise applications and autonomous services. These services communicate through secure APIs and service meshes that enforce authentication and encryption policies. Microservices architecture ensures that individual components can operate independently, improving system resilience.

Figure 2: AI-Driven Cyber-Resilient Cloud-Native Architecture for Autonomous Enterprise Systems and Secure Digital Ecosystems

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 4, July -August 2025 |

DOI:10.15662/IJEETR.2025.0704012

Figure 2 illustrates a comprehensive AI-driven cyber-resilient cloud-native architecture designed to support autonomous enterprise systems and secure digital ecosystems. The architecture integrates artificial intelligence, machine learning, cloud infrastructure, and automated security mechanisms to enable real-time threat detection, intelligent decision-making, and continuous compliance within modern enterprise environments.

At the center of the architecture is the **AI Orchestration and Decision Engine**, which acts as the core intelligence layer of the system. This component integrates **AI analytics and machine learning models** to analyze large volumes of operational and security data collected from multiple sources. The engine coordinates the activities of various security agents, performs predictive analytics, and determines appropriate mitigation strategies for emerging cyber threats.

On the left side of the architecture is the **Threat Monitoring and Incident Response layer**, which is responsible for continuous surveillance of enterprise systems. This layer includes monitoring agents that analyze **network logs, audit trails, system metrics, and threat intelligence feeds**. These components enable early detection of anomalies, suspicious activities, and potential vulnerabilities in the cloud environment.

The right side of the diagram represents the **Automated Security and Compliance layer**, which ensures that enterprise systems maintain regulatory and policy compliance. This layer incorporates compliance agents that perform **continuous compliance verification, automated policy enforcement, and audit and reporting functions**. Through automation, the system reduces manual intervention and ensures that security standards are consistently maintained.

The lower section of the architecture depicts the **Cloud Infrastructure Layer**, which forms the technological backbone of the system. It includes modern cloud-native components such as **Docker containers, Kubernetes orchestration, microservices architecture, serverless computing, and cloud storage systems**. These technologies support scalable, flexible, and resilient deployment of enterprise applications across hybrid or multi-cloud environments.

Adjacent to this is the **Digital Ecosystem and Enterprise Services layer**, which represents the operational applications that run within the cloud environment. This layer includes **business applications, DevOps automation tools, CI/CD pipelines, and hybrid cloud services**, enabling seamless integration between development, deployment, and operational workflows.

Overall, the architecture demonstrates how artificial intelligence can be embedded within cloud-native infrastructures to create **cyber-resilient enterprise systems** capable of autonomous monitoring, predictive threat intelligence, automated incident mitigation, and continuous governance across secure digital ecosystems.

The **AI analytics and threat intelligence layer** is responsible for monitoring system activities and detecting potential cyber threats. Machine learning algorithms analyze system logs, network data, and behavioral patterns to identify anomalies and predict possible attacks.

The **cyber resilience and response layer** manages automated threat response and system recovery. When a threat is detected, automated security orchestration tools initiate countermeasures such as isolating affected containers, blocking malicious traffic, or restoring services from secure backups.

Finally, the **governance and compliance layer** ensures that the architecture adheres to regulatory standards and enterprise security policies. Continuous monitoring and auditing mechanisms maintain compliance with industry regulations and security best practices.

IV. RESULTS AND DISCUSSION

The proposed **AI-driven cyber-resilient cloud-native architecture** was evaluated in a simulated enterprise cloud environment to analyze its effectiveness in detecting cyber threats, maintaining system resilience, and supporting autonomous enterprise operations. The evaluation focused on key performance indicators such as threat detection accuracy, response time, system recovery capability, and overall infrastructure resilience.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 4, July -August 2025 |

DOI:10.15662/IJEETR.2025.0704012

The results show that the integration of **artificial intelligence–based threat detection** significantly improves the ability to identify cyber threats in cloud-native environments. Machine learning algorithms analyzed large volumes of system logs, network traffic data, and user activity patterns to detect abnormal behavior. The AI models were able to identify suspicious activities such as unauthorized access attempts, abnormal API requests, and unusual network communication patterns with high accuracy. Compared to traditional rule-based security systems, the AI-driven model demonstrated faster detection of potential threats and reduced the likelihood of undetected attacks.

The implementation of **automated threat response mechanisms** also produced positive results. When a potential security incident was detected, the system automatically initiated response actions such as isolating compromised containers, blocking suspicious IP addresses, and restricting unauthorized user access. This automated response significantly reduced incident response time and helped prevent the spread of malicious activities within the cloud infrastructure.

Another important outcome of the evaluation was the improved **cyber resilience capability** of the proposed architecture. The system was designed with self-healing mechanisms that allowed services to recover automatically after a failure or attack. During simulated attack scenarios, the architecture successfully restored affected services through automated container redeployment and backup recovery processes. This capability ensured minimal service disruption and maintained operational continuity for enterprise applications.

The architecture also demonstrated strong performance in **supporting autonomous enterprise systems**. Since autonomous systems rely heavily on real-time data processing and continuous service availability, maintaining infrastructure stability is essential. The proposed architecture provided a stable environment by continuously monitoring system performance, detecting anomalies, and initiating corrective actions when necessary.

Despite these positive outcomes, several challenges were identified during the evaluation process. AI-based cybersecurity models require large volumes of high-quality data for accurate training and prediction. In environments where data collection is limited or inconsistent, the effectiveness of the AI models may decrease. Additionally, implementing AI-driven security systems may require higher computational resources and advanced infrastructure management capabilities.

Overall, the experimental results demonstrate that the proposed **AI-driven cyber-resilient architecture** effectively enhances enterprise cybersecurity by improving threat detection, enabling rapid response, and maintaining operational resilience in cloud-native environments. The integration of AI-based analytics, automated response systems, and resilient infrastructure design provides a strong foundation for securing autonomous enterprise systems and complex digital ecosystems.

V. CONCLUSION

As enterprises increasingly adopt autonomous systems and cloud-native infrastructures, ensuring cybersecurity and operational resilience has become a critical priority. Traditional security models are insufficient for protecting modern distributed environments. This paper proposed an **AI-driven cyber-resilient cloud-native architecture** designed to secure autonomous enterprise systems and digital ecosystems.

By integrating artificial intelligence, automated threat detection, self-healing infrastructure, and resilient system design, the proposed architecture enables organizations to proactively defend against cyber threats while maintaining continuous operations. The framework demonstrates strong potential for enhancing enterprise cybersecurity and building resilient digital infrastructures capable of adapting to evolving cyber risks.

VI. FUTURE WORK

Future research can explore advanced deep learning techniques to improve predictive threat detection and anomaly identification. Integrating **federated learning** may enable collaborative cybersecurity intelligence sharing across multiple organizations while preserving data privacy. Additionally, blockchain-based security mechanisms could be used to enhance data integrity and secure digital transactions within enterprise ecosystems.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 4, July -August 2025 |

DOI:10.15662/IJEETR.2025.0704012

Further work may also focus on developing **explainable AI models** that allow security analysts to understand how AI systems identify threats and make decisions. Improving transparency in AI-based cybersecurity systems will increase trust and support more effective security governance.

REFERENCES

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. Adari, V. K. (2024). Interoperability and Data Modernization: Building a Connected Banking Ecosystem. International Journal of Computer Engineering and Technology, 15(6), 653-662.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. Inbavalli, M., & Arasu, T. (2015). Efficient Analysis of Frequent Item Set Association Rule Mining Methods. International Journal of Scientific & Engineering Research, 6(4).
15. 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.
16. 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.
17. Tamizharasi, S., Rubini, P., Saravana Kumar, S., & Arockiam, D. Adapting federated learning-based AI models to dynamic cyberthreats in pervasive IoT environments.
18. 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).
19. 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.
20. 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.
21. 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.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 7, Issue 4, July -August 2025 |

DOI:10.15662/IJEETR.2025.0704012

22. 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.
23. 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.
24. 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.
25. 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.
26. Thota, S. (2024). A Cloud-Based Blockchain and AI Hybrid Model for Secure CRM Data Management in Salesforce. International Journal of Emerging Research in Engineering and Technology, 5(2), 124-135.
27. Viswanathan, Venkatraman. "AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization." (2023).
28. 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.
29. 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.
30. 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.
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. 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.
33. 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.
34. 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.
35. 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.
36. 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).
37. 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.
38. 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.
39. 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
40. 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.
41. 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.