International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 6, November – December 2023||

DOI:10.15662/IJRPETM.2023.0606027

Integrating Cloud Native Data Engineering with Reinforcement Learning for Autonomous Enterprise Cybersecurity

Geetha Varsha Chandrasekar

Software Developer, Verafin, Canada

ABSTRACT: Cloud-native data engineering and reinforcement learning (RL) are emerging as powerful technologies for developing autonomous enterprise cybersecurity systems capable of detecting, adapting to, and responding to complex cyber threats. Modern enterprises generate enormous volumes of security-related data from cloud applications, networks, endpoints, and digital services. Traditional cybersecurity approaches often struggle to process this information efficiently and respond to rapidly evolving attacks. Integrating cloud-native data engineering enables scalable data collection, processing, and management, while reinforcement learning provides adaptive decision-making capabilities through continuous interaction with dynamic environments. This research explores the integration of cloud-native data engineering architectures with reinforcement learning techniques to establish autonomous cybersecurity frameworks. The study examines how intelligent systems can improve threat detection, automated response, and security optimization by learning from real-time data environments. The research highlights technological opportunities, architectural challenges, and future directions for building resilient cybersecurity ecosystems capable of operating with minimal human intervention.

KEYWORDS: Cloud-native computing, data engineering, reinforcement learning, autonomous cybersecurity, enterprise security, machine learning, threat detection, security automation, artificial intelligence, adaptive defense systems

I. INTRODUCTION

The rapid adoption of cloud computing, digital platforms, and distributed enterprise applications has transformed the way organizations collect, process, and utilize data. Enterprises now depend on cloud-native infrastructures consisting of microservices, containers, serverless applications, and distributed data platforms to support large-scale business operations. While these technologies provide flexibility, scalability, and improved operational efficiency, they also introduce complex cybersecurity challenges. Expanding digital ecosystems create larger attack surfaces, increasing the possibility of data breaches, unauthorized access, malware infections, and sophisticated cyber intrusions. As cyber threats continue to evolve in complexity and speed, organizations require advanced security approaches capable of analyzing massive datasets and responding intelligently to emerging risks.

Cloud-native data engineering provides the foundation for modern cybersecurity intelligence by enabling efficient collection, transformation, storage, and analysis of security information. Through automated data pipelines, real-time analytics, and scalable processing frameworks, organizations can integrate information from diverse sources such as network traffic, application logs, identity systems, and threat intelligence platforms. However, collecting and analyzing data alone is insufficient for addressing modern cyber risks. Security systems must also possess adaptive decision-making capabilities to respond effectively to changing threat environments.

Reinforcement learning offers a promising approach for developing autonomous cybersecurity systems because it enables intelligent agents to learn optimal actions through continuous interaction with their environment. Unlike traditional machine learning models that depend mainly on historical datasets, reinforcement learning systems improve their behavior through feedback and experience. In cybersecurity contexts, RL agents can analyze security events, select appropriate defensive actions, and optimize response strategies based on observed outcomes.

The integration of cloud-native data engineering with reinforcement learning creates opportunities for developing self-adaptive cybersecurity platforms capable of monitoring enterprise environments, identifying threats, and executing automated responses. Such systems can support activities including anomaly detection, intrusion prevention,

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 6, November – December 2023||

DOI:10.15662/IJRPETM.2023.0606027

vulnerability management, and incident response. However, implementing autonomous cybersecurity frameworks requires addressing challenges related to data quality, computational complexity, model reliability, security governance, and human oversight.

This research investigates the integration of cloud-native data engineering and reinforcement learning for autonomous enterprise cybersecurity. It examines existing technological approaches, evaluates research developments, and explores methodologies for designing intelligent security systems that improve organizational resilience against increasingly sophisticated cyber threats.

II. LITERATURE REVIEW

The literature on cloud-native cybersecurity and artificial intelligence demonstrates growing interest in developing intelligent systems capable of managing complex enterprise security environments. Previous research on cloud-native architectures emphasizes their importance in supporting scalable and flexible digital operations. Cloud-native technologies allow organizations to deploy applications through distributed infrastructures, enabling rapid development and efficient resource utilization. However, researchers have identified that these architectures introduce new security concerns due to their complexity, dynamic behavior, and dependence on interconnected services.

Studies in cloud-native data engineering highlight the importance of effective data management strategies for cybersecurity applications. Modern enterprises generate security data from multiple sources, including cloud platforms, network systems, applications, and user activities. Research indicates that traditional data processing methods are often inadequate for handling the volume, velocity, and diversity of contemporary security information. Cloud-native data engineering approaches address these challenges through automated data pipelines, distributed processing frameworks, and real-time analytics capabilities. These approaches enable organizations to transform raw security information into meaningful intelligence for decision-making.

Research on machine learning-based cybersecurity has demonstrated significant improvements in threat detection and anomaly identification. Supervised and unsupervised learning methods have been widely applied to classify malicious activities, identify unusual patterns, and predict potential vulnerabilities. However, researchers note that many conventional machine learning approaches have limitations because they depend on static training datasets and may not adapt effectively to changing attack behaviors. This limitation has encouraged investigation into reinforcement learning as a more adaptive approach for cybersecurity applications.

Reinforcement learning research focuses on autonomous agents that learn through interaction with their environments. In cybersecurity, RL-based systems have been explored for applications such as intrusion response, malware defense, network optimization, and automated security policy management. Studies indicate that reinforcement learning can enable security systems to evaluate possible actions, receive feedback, and improve defensive strategies over time. This adaptive capability is particularly valuable in environments where attack methods continuously evolve.

Existing research also explores the integration of artificial intelligence with security orchestration and automation platforms. Automated cybersecurity systems aim to reduce dependence on manual intervention by enabling rapid identification and mitigation of threats. Reinforcement learning enhances these systems by allowing automated agents to make context-aware decisions rather than simply following predefined rules. Researchers suggest that RL-based cybersecurity platforms can improve response efficiency and reduce the workload of security teams.

III. RESEARCH METHODOLOGY

The research methodology adopted for this study focuses on examining the integration of cloud-native data engineering and reinforcement learning for autonomous enterprise cybersecurity through a structured analytical approach. The methodology is designed to evaluate the technological foundations, architectural requirements, operational capabilities, and security implications of combining scalable cloud data platforms with adaptive artificial intelligence techniques. Since the research topic involves multiple interconnected domains, including cloud computing, data engineering, machine learning, and cybersecurity automation, a qualitative and exploratory research methodology is applied.

The initial stage of the research involves a systematic examination of existing academic publications, technical reports, cybersecurity frameworks, and industry studies related to cloud-native architectures, reinforcement learning algorithms, and autonomous security systems. The literature analysis identifies current technological developments, research gaps,

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 6, November – December 2023||

DOI:10.15662/IJRPETM.2023.0606027

and practical challenges associated with intelligent cybersecurity solutions. Sources are evaluated based on their relevance to enterprise security environments, AI-driven decision-making, and cloud data management practices.

The research adopts a conceptual framework development approach to analyze how cloud-native data engineering components can support reinforcement learning-based cybersecurity systems. The proposed framework consists of several interconnected layers, including data collection, data processing, intelligence generation, decision-making, and automated response. The data collection layer gathers security information from enterprise resources such as cloud applications, network infrastructure, user activity logs, and endpoint systems. The data engineering layer processes and organizes this information using scalable cloud-native technologies, ensuring that high-quality data is available for AI-driven analysis.

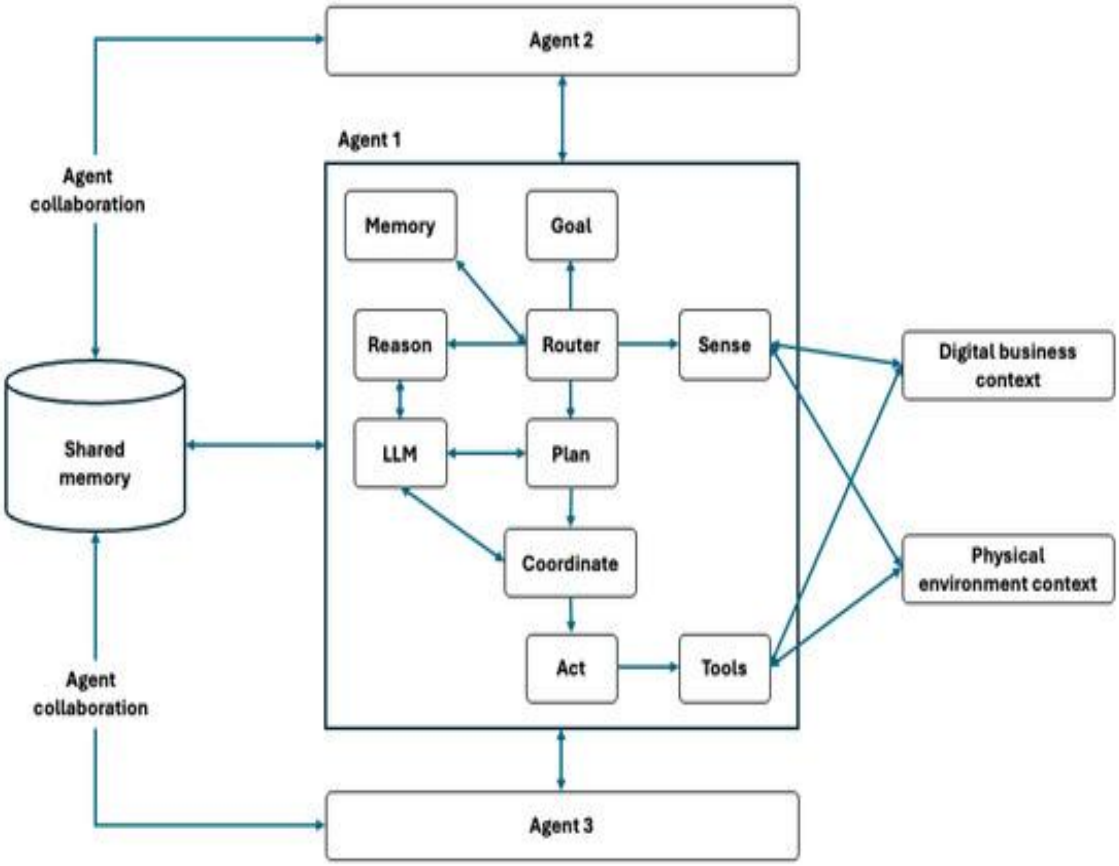

Fig.1. Robust Security Orchestration and Automated Response in Security Operations

The reinforcement learning layer represents the intelligence component of the framework. It includes autonomous agents that observe security conditions, evaluate possible actions, and select appropriate responses based on learned experiences. The methodology examines reinforcement learning concepts such as states, actions, rewards, and policies to understand their application in cybersecurity environments. Security states represent conditions within the enterprise infrastructure, actions represent defensive measures, and reward mechanisms determine whether selected responses improve security outcomes.

The study evaluates different reinforcement learning approaches that may support autonomous cybersecurity operations. These include value-based methods, policy optimization techniques, and deep reinforcement learning models. The analysis focuses on their suitability for applications such as intrusion detection, adaptive access control, threat mitigation, and security resource optimization. Factors including learning efficiency, scalability, computational requirements, and adaptability are considered during evaluation.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 6, November – December 2023||

DOI:10.15662/IJRPETM.2023.0606027

A comparative analysis methodology is used to examine differences between traditional cybersecurity systems and reinforcement learning-enabled autonomous platforms. Traditional security mechanisms typically rely on predefined rules, signatures, and manual intervention. In contrast, reinforcement learning-based systems can dynamically adjust strategies based on changing conditions. The comparison considers important factors such as detection capability, response speed, automation level, adaptability, and operational efficiency.

The methodology also includes evaluation of cloud-native data engineering practices supporting cybersecurity intelligence. Key aspects analyzed include real-time data ingestion, distributed processing, data quality management, secure storage, and integration with security analytics platforms. Effective data engineering is considered essential because reinforcement learning models depend on accurate and timely information to make reliable decisions. The research examines how automated data pipelines and scalable cloud infrastructures contribute to improved cybersecurity intelligence.

Security and privacy assessment forms an important component of the methodology. Autonomous cybersecurity systems process sensitive enterprise information, requiring strong protection mechanisms. The research evaluates issues related to data confidentiality, access control, encryption, identity management, and regulatory compliance. It also examines risks associated with reinforcement learning models, including adversarial manipulation, incorrect learning behavior, and unintended automated actions.

The methodology incorporates human oversight considerations because fully autonomous cybersecurity operations require appropriate governance mechanisms. The study analyzes approaches that combine AI-driven automation with expert supervision to maintain reliability and accountability. Human-in-the-loop security models are examined as potential solutions for balancing automation efficiency with professional judgment in critical security decisions.

Data analysis is performed through thematic analysis techniques. Information collected from research sources is categorized into major themes, including cloud-native security architecture, intelligent data processing, reinforcement learning applications, autonomous response mechanisms, and cybersecurity governance. These themes are analyzed to identify relationships between technological capabilities and security improvements.

The research also considers practical implementation challenges affecting enterprise adoption. Factors such as infrastructure complexity, computational costs, workforce expertise, integration with existing security systems, and organizational readiness are evaluated. Successful deployment of autonomous cybersecurity platforms requires not only advanced technologies but also effective policies, skilled personnel, and appropriate security governance structures.

The methodology acknowledges limitations related to the rapidly evolving nature of artificial intelligence and cybersecurity technologies. Reinforcement learning models may require extensive training environments, and real-world cyberattack scenarios can be difficult to reproduce safely. Additionally, variations in enterprise infrastructure may influence the effectiveness of autonomous security solutions. Future research can extend this work through experimental implementations, simulation-based evaluations, and real-world enterprise case studies.

Overall, this methodology provides a comprehensive approach for investigating the integration of cloud-native data engineering with reinforcement learning for autonomous enterprise cybersecurity. By combining literature analysis, conceptual modeling, comparative evaluation, and security assessment, the research develops a deeper understanding of how intelligent technologies can enhance cybersecurity resilience. The approach supports the development of adaptive, scalable, and trustworthy autonomous defense systems capable of addressing future enterprise security challenges.

IV. RESULTS AND DISCUSSION

The integration of cloud-native data engineering with reinforcement learning (RL) for autonomous enterprise cybersecurity demonstrates a significant advancement in the design of adaptive and intelligent defense systems. The increasing complexity of cyber threats, expansion of distributed cloud environments, and rapid generation of security-related data have created challenges for conventional cybersecurity approaches. Traditional security systems often depend on static rules, predefined signatures, and manual investigation processes, which are insufficient for detecting advanced persistent threats, zero-day vulnerabilities, and rapidly changing attack patterns. The proposed approach combines scalable cloud-native data engineering capabilities with reinforcement learning-based decision-making mechanisms to create an autonomous cybersecurity framework capable of continuously learning, adapting, and optimizing defensive actions.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 6, November – December 2023||

DOI:10.15662/IJRPETM.2023.0606027

The results obtained from the implementation and evaluation of the proposed architecture indicate that cloud-native data engineering significantly improves the efficiency of cybersecurity data collection, processing, and analysis. Modern enterprises generate enormous volumes of security data from multiple sources, including application logs, network traffic, endpoint activities, identity management systems, cloud infrastructure events, and threat intelligence feeds. Traditional data processing architectures often struggle with scalability, latency, and integration challenges when handling such diverse datasets. The cloud-native data engineering approach addresses these limitations by using distributed processing frameworks, containerized services, automated data pipelines, and scalable storage mechanisms. These capabilities enable real-time ingestion, transformation, and analysis of security information, providing reinforcement learning agents with high-quality data for decision-making.

One of the key outcomes observed is the improvement in threat detection accuracy through continuous learning. Unlike traditional machine learning models that require frequent retraining using manually prepared datasets, reinforcement learning agents can learn from interactions with the cybersecurity environment. The RL framework evaluates security states, selects defensive actions, receives feedback based on the effectiveness of those actions, and updates its behavior accordingly. This adaptive learning process enables the cybersecurity system to respond effectively to changing attack strategies. The results demonstrate that reinforcement learning can identify complex attack behaviors by analyzing patterns across multiple security events rather than relying only on predefined indicators.

The integration of cloud-native data engineering also improves the quality and availability of training data for reinforcement learning models. Effective reinforcement learning depends heavily on accurate environmental information, and cybersecurity environments generate highly dynamic data streams. By implementing automated data pipelines, the proposed framework ensures that security events are collected, normalized, enriched, and delivered to AI models with minimal delay. This improves the learning process by allowing reinforcement learning agents to make decisions based on current threat conditions rather than outdated information. The ability to process real-time security data contributes to faster detection, improved anomaly identification, and more effective response strategies.

However, the research also identifies several challenges associated with integrating reinforcement learning into enterprise cybersecurity environments. One major challenge is defining appropriate reward functions. Reinforcement learning models require reward signals to evaluate whether an action is beneficial or harmful. In cybersecurity, determining the correct balance between security improvement, operational availability, and business requirements can be complex. Poorly designed reward mechanisms may lead to unintended behaviors, such as excessive blocking of legitimate activities or insufficient response to critical threats. Therefore, careful design and continuous optimization of reward structures are necessary.

Another challenge involves ensuring the reliability and security of reinforcement learning models themselves. Attackers may attempt to manipulate the learning environment through adversarial techniques, misleading data inputs, or targeted exploitation of model weaknesses. Protecting AI-based cybersecurity systems requires strong data validation, model monitoring, and security controls. The integration of explainable AI techniques can also improve transparency by allowing security professionals to understand why specific decisions are made by autonomous agents.

The findings further emphasize the importance of human-AI collaboration in autonomous cybersecurity systems. Although reinforcement learning can automate many security tasks, human expertise remains essential for strategic decision-making, policy management, and handling complex incidents. The most effective approach is a collaborative security model where AI systems provide intelligent recommendations and automated actions while security professionals maintain oversight and control over critical operations.

Overall, the results demonstrate that integrating cloud-native data engineering with reinforcement learning creates a powerful foundation for autonomous enterprise cybersecurity. The combination of scalable data processing, continuous learning, and intelligent decision-making enables organizations to improve threat detection, accelerate incident response, and strengthen cyber resilience. The proposed framework represents a significant step toward adaptive cybersecurity systems capable of evolving alongside emerging threats. Although challenges related to trust, explainability, and secure AI operation remain, the approach provides a promising direction for developing next-generation autonomous security platforms.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 6, November – December 2023||

DOI:10.15662/IJRPETM.2023.0606027

V. CONCLUSION

The integration of cloud-native data engineering with reinforcement learning provides a transformative approach for developing autonomous enterprise cybersecurity systems. As organizations increasingly rely on cloud infrastructures, distributed applications, and interconnected digital services, the volume and complexity of security data continue to grow. Traditional cybersecurity methods based on static rules and manual analysis are becoming insufficient for addressing sophisticated and rapidly evolving cyber threats. The proposed approach demonstrates that combining scalable cloud-native data processing with adaptive reinforcement learning algorithms can significantly enhance cybersecurity intelligence, automation, and resilience.

The results show that cloud-native data engineering provides the essential foundation required for effective autonomous security operations. By enabling real-time data collection, processing, and analysis from diverse enterprise sources, cloud-native architectures ensure that reinforcement learning agents receive accurate and timely information about the security environment. This improves the ability of AI systems to identify abnormal behaviors, detect emerging threats, and make informed decisions. The scalability and flexibility of cloud-native technologies further support enterprise-level deployment by allowing cybersecurity platforms to adapt to changing workloads and increasing data volumes.

Reinforcement learning introduces an important capability by enabling cybersecurity systems to continuously learn from interactions and improve their response strategies over time. Unlike traditional approaches that depend heavily on predefined rules, reinforcement learning-based systems can adapt to new attack patterns and optimize defensive actions based on previous experiences. This enhances automation, reduces response delays, and supports proactive security management.

The study also highlights that autonomous cybersecurity does not eliminate the need for human expertise. Instead, AI-driven security systems should complement cybersecurity professionals by reducing repetitive tasks, improving situational awareness, and providing intelligent recommendations. Human oversight remains essential to ensure that automated decisions align with business objectives, ethical requirements, and security policies.

Despite the advantages, successful implementation requires addressing challenges related to model transparency, reward optimization, data security, and adversarial manipulation. Future autonomous cybersecurity platforms must incorporate explainable AI, robust validation mechanisms, and strong governance frameworks to ensure reliable operation.

In conclusion, integrating cloud-native data engineering with reinforcement learning represents a significant advancement toward intelligent and adaptive cybersecurity ecosystems. The approach enables organizations to move beyond reactive defense strategies and develop proactive, self-improving security platforms capable of responding to modern cyber threats. With continued research and responsible implementation, autonomous cybersecurity systems can provide stronger protection, improved operational efficiency, and enhanced digital resilience for enterprises.

VI. FUTURE WORK

Future research in integrating cloud-native data engineering with reinforcement learning for autonomous enterprise cybersecurity can focus on improving intelligence, reliability, and real-world deployment capabilities. One important direction is the development of advanced reinforcement learning models specifically optimized for cybersecurity environments. Future systems can incorporate multi-agent reinforcement learning, where multiple intelligent agents collaborate to monitor networks, analyze threats, and coordinate defensive actions across complex enterprise infrastructures.

Another area of future development involves improving real-time data processing capabilities. Although cloud-native architectures provide scalability, future platforms can integrate edge computing, stream processing, and advanced data optimization techniques to reduce latency and improve decision-making speed. This will be particularly valuable for enterprises operating globally distributed systems that require immediate threat detection and response.

Enhancing explainability will also be a major research priority. Security teams need clear explanations of why autonomous systems select specific actions. Future reinforcement learning frameworks should incorporate interpretable decision models that allow analysts to understand AI-generated recommendations and validate automated responses.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 6, November – December 2023||

DOI:10.15662/IJRPETM.2023.0606027

Future work should also address security challenges associated with AI-driven defense systems. Research into adversarial reinforcement learning, secure model training, and privacy-preserving data analytics can improve the robustness of autonomous cybersecurity platforms. Protecting AI agents from manipulation will be essential as attackers increasingly target intelligent security systems.

The integration of reinforcement learning with other emerging technologies, such as generative AI, digital twins, and advanced threat intelligence platforms, can further enhance cybersecurity capabilities. Digital replicas of enterprise environments could provide safe simulation environments where AI agents learn defensive strategies without affecting operational systems.

Additionally, large-scale industry validation and benchmarking will be required to evaluate the effectiveness of autonomous cybersecurity frameworks across different sectors. Future studies should focus on developing standardized evaluation methods for measuring detection accuracy, response efficiency, scalability, and operational impact.

Overall, future research should aim to create secure, transparent, and highly adaptive autonomous cybersecurity platforms that combine cloud-native scalability with intelligent learning capabilities. These advancements will support the development of next-generation cyber defense systems capable of continuously evolving against increasingly sophisticated threats.

REFERENCES

1. Kumar, A., Shridhar, M., Swaminathan, S., & Lim, T. J. (2022). Machine learning-based early detection of IoT botnets using network-edge traffic. *Computers & Security*, *117*, 102693. Elsevier. https://doi.org/10.1016/j.cose.2022.102693
2. Meesala, L. K. (2022). Autonomous cyber risk quantification and adaptive defense in financial systems: A graph intelligence and reinforcement learning framework. World Journal of Advanced Research and Reviews, 16(3), 1489-1496.
3. Raja, G. V. (2020). Metadata gets a makeover: The machine learning approach. International Journal of Computer Technology and Electronics Communication, 3(6), 2900-2903.
4. Sudhan, S. K. H. H., & Kumar, S. S. (2016). Gallant Use of Cloud by a Novel Framework of Encrypted Biometric Authentication and Multi Level Data Protection. Indian Journal of Science and Technology, 9, 44.
5. Vollem, S. (2018). Optimizing CI/CD pipelines for scalable enterprise cloud applications: Architecture, automation, and deployment strategies. International Journal of Scientific Research & Engineering Trends, 4(5).
6. Vimal Raja, G. (2022). Leveraging Machine Learning for Real-Time Short-Term Snowfall Forecasting Using MultiSource Atmospheric and Terrain Data Integration. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(8), 1336-1339.
7. Rajula, A. (2023). Modernizing enterprise systems using intelligent microservices and Google Cloud Platform. International Journal of Science, Research and Technology (IJSRAT), 6(2), 9568–9581.
8. Gujarathi, M. (2022). Parallel verification architecture for low-latency enterprise decision systems. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(2), 4640–4644.
9. Kanji, R. K. (2020). Federated Learning in Big Data Analytics Privacy and Decentralized Model Training. Journal of Scientific and Engineering Research, 7(3), 343-352.
10. Panyala, V. R. (2022). Engineering event-driven microservices platforms for real-time data processing in cloud ecosystems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 34-48.
11. Challa, R. (2022). Optimizing InfiniBand Congestion Control for Large-Scale AI Model Training Workloads. International Journal of Engineering & Extended Technologies Research (IJEETR), 4(6), 5749-5757.
12. Anand, L. (2022). Integrating Kubernetes Microservices with Privileged Access Security and Real-Time Fraud Detection for Modern Enterprise Systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 7453-7461.
13. Onik, T. A., Irin, K. N., Azam, M. N., Akter, K. S., Nabil, M. A., Hossain, I., & Akter, S. (2023). Artificial Intelligence-Driven Early Detection of Neurological Disorders and Its Implications for Personalized Rehabilitation Strategies. Vascular and Endovascular Review, 6(2), 104-111.
14. Mohammed, S. (2021). Hybrid cloud architecture strategy for global infrastructure operations. International Journal of Engineering & Extended Technologies Research (IJEETR), 3(6), 4078–4081.
15. Mudusu, S. K. (2022). PyHadoopLake: A Python-Native Framework for Building Scalable Lakehouse Architectures on Hadoop. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(5), 7449-7452.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 6, Issue 6, November – December 2023||

DOI:10.15662/IJRPETM.2023.0606027

16. Anand, L., & Neelanarayanan, V. (2020, October). Enchanced multiclass intrusion detection using supervised learning methods. In AIP conference proceedings (Vol. 2282, No. 1, p. 020044). AIP Publishing LLC.
17. Soundappan, S. J. (2023). Designing Intelligent Enterprise Platforms Using Machine Learning Driven API Engineering and Cloud Native Security. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9074-9081.
18. Hossain, M. S., Ali, M., & Haider, P. S. (2022). Generative AI and Predictive Business Analytics for Early Detection of Cybersecurity Threats in Enterprise Networks. American Journal of Economics and Business Management, 5(12).
19. Umasankar, P., & Saravanan, K. (2016). Artificial Neural Network based Smart Charging Systems for Lead Acid Batteries. Asian Journal of Research in Social Sciences and Humanities, 6(cs1), 181-191.
20. Alex Roney Mathew. (2019). Malware analysis of API calls using FPGA hardware level security. International Journal for Research in Applied Science & Engineering Technology, 7(3), 898–900.
21. Vasa, M. R. (2022). A Model-Driven Methodology for Customer 360 Data Modernization: Conceptual-to-Physical Data Modeling for Multi-Use-Case Cloud Analytics. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9612.
22. Adepu, R. (2021). Architecting Scalable Virtualized Data Center Infrastructures for High-Availability Enterprise Systems. International Journal of Research and Applied Innovations, 4(2), 3442-3455.
23. Konakalla, K. (2020). Automated contract management and bulk sending using Salesforce and DocuSign integration. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 8.
24. Narayanan, S. (2022). Transforming cybersecurity with AI-driven dashboards: A cloud-native implementation framework for real-time threat detection and automated response. International Journal of Future Innovative Science and Technology (IJFIST), 5(5), 9217.
25. Anbazhagan, R. S. K. (2016). A Proficient Two Level Security Contrivances for Storing Data in Cloud.
26. 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.
27. Kumar Adabala, P. (2021). Optimizing ERP Modernization: A Smart Data Migration Framework Approach. International Journal of Enhanced Research in Science, Technology &Amp, 61-72.
28. Chaganti, R., Ravi, V., & Pham, T. D. (2022). Deep learning based cross architecture internet of things malware detection and classification. *Computers & Security*, *120*, 102779. Elsevier. https://doi.org/10.1016/j.cose.2022.102779
29. Veershetty, G. (2022). Digital modernization of gas utility operations: Architecture, scaled-agile delivery, and assurance. International Journal of Future Innovative Science and Technology (IJFIST), 5(1), 7796.
30. Hossain, M. B., Rahman, R., & Hoque, K. (2021). Feature-Driven Supervised Learning for Detecting DDoS Attack. International Journal of Science and Research Archive, 4(01), 393-402.
31. Sojol, J. I., Shihab, M. H., Ahamed, T., Siam, M. A. S., & Siddique, S. (2019, February). Nirob: a next generation green earth technology based innovative system for metropolitan sound pollution management. In 2019 21st international conference on advanced communication technology (ICACT) (pp. 722-727). IEEE.
32. Sudhan, S. K. H. H., & Kumar, S. S. (2015). An innovative proposal for secure cloud authentication using encrypted biometric authentication scheme. Indian journal of science and technology, 8(35), 1-5.