International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November-December 2022||

DOI:10.15662/IJRAI.2022.0506025

A Risk-Aware Generative AI and LLM-Driven Cloud Framework for Secure Banking with PII Protection and Privacy Analytics in 5G Web Applications

Ingrid Sofie Johansen

Senior Technical Team Lead, Norway

ABSTRACT: The rapid evolution of digital banking, cloud-native systems, and 5G-enabled web applications has increased the need for secure, privacy-aware, and intelligent financial platforms. At the same time, the widespread use of Generative Artificial Intelligence (AI) and Large Language Models (LLMs) has created new opportunities for advanced analytics, automation, and customer engagement. However, the integration of these technologies also introduces risks related to personally identifiable information (PII) exposure, data misuse, and regulatory non-compliance. This paper proposes a risk-aware Generative AI and LLM-driven cloud framework designed to support secure banking operations while ensuring PII protection and privacy analytics in 5G web environments.

The framework integrates cloud-native infrastructure, real-time data pipelines, and LLM-based decision intelligence with a multi-layered privacy and security architecture. It incorporates encryption, anonymization, differential privacy techniques, and zero-trust access control to safeguard sensitive financial and customer data. A privacy analytics layer enables continuous monitoring of PII usage, consent management, and regulatory compliance with standards such as GDPR and financial data protection policies. Generative AI models support fraud detection, customer support automation, and predictive analytics while operating under strict governance policies to prevent data leakage and model bias.

The proposed architecture was evaluated using simulated banking transaction datasets and privacy-sensitive user interaction data. Results demonstrate improved detection of anomalous activities, enhanced privacy risk visibility, and reduced latency in 5G-enabled cloud environments. The integration of LLM-driven analytics with privacy-aware controls improved decision-making accuracy while maintaining data confidentiality and regulatory compliance. The study highlights the importance of combining risk-aware AI governance, privacy analytics, and secure cloud infrastructure to build trustworthy digital banking ecosystems. The framework provides a scalable and adaptable approach for financial institutions seeking to leverage generative AI while protecting sensitive customer information in next-generation web applications.

KEYWORDS: Generative AI, Large Language Models, secure banking, personally identifiable information, privacy analytics, 5G web applications, cloud computing, cybersecurity, data protection, AI governance, zero-trust security, financial technology

I. INTRODUCTION

The proliferation of 5G networks and web-based financial and trade applications has transformed the global economy. Ultra-fast data transfer, low latency, and high connectivity offered by 5G enable real-time banking operations, high-frequency trading, cross-border transactions, and sophisticated trade analytics. However, the speed and scale of 5G-enabled applications also amplify cybersecurity risks, operational vulnerabilities, and financial fraud. Traditional risk management and fraud detection systems—largely rule-based—struggle to keep pace with high-velocity data and evolving cyber threats.

Recent advancements in **Artificial Intelligence (AI)**, particularly **Generative AI**, provide new opportunities to simulate potential fraud or attack scenarios, predict anomalous behavior, and generate actionable insights for decision-makers. Generative AI models, including variational autoencoders (VAEs) and generative adversarial networks (GANs), can anticipate vulnerabilities by creating synthetic datasets that model potential threat behaviors, helping organizations proactively manage risks.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November-December 2022||

DOI:10.15662/IJRAI.2022.0506025

Large Language Models (LLMs) further augment these capabilities. LLMs can analyze unstructured data, such as customer communication, trade documents, regulatory notices, and logs, to detect subtle anomalies and generate interpretive summaries for analysts. By combining LLMs with generative AI, the framework provides not only detection but **explainable and predictive insights**, critical for high-stakes banking and trade operations. Cloud computing is essential for handling the computational and storage demands of high-volume 5G data. Cloud-native architectures allow **scalable, distributed, and low-latency processing** of streaming transactions while ensuring redundancy, fault tolerance, and compliance with security and privacy regulations such as GDPR, PCI DSS, and ISO 27001.

Secure ETL pipelines serve as the backbone for high-quality data ingestion and processing. Data from multiple sources—including banking systems, trade platforms, market feeds, and IoT-enabled devices—is extracted, transformed, and loaded securely into centralized warehouses. This ensures that AI and LLM models operate on accurate, consistent, and timely data.

Finally, a **risk-aware module** integrates quantitative and qualitative risk assessment into the framework. By evaluating potential threat impact, likelihood, and system vulnerability, the module dynamically adjusts model thresholds, data access controls, and security protocols. Risk-awareness enables proactive mitigation of cyber threats and financial fraud, reducing operational and reputational costs. This paper presents a unified framework integrating generative AI, LLMs, cloud infrastructure, secure ETL pipelines, and risk-aware mechanisms for **secure banking and trade analytics in 5G web applications**. The research addresses critical challenges such as real-time detection, high-velocity data processing, regulatory compliance, and adaptive cybersecurity in modern financial ecosystems.

II. LITERATURE REVIEW

Cybersecurity and Financial Fraud in 5G Networks:
5G enables faster, more connected financial and trade systems but also introduces new attack surfaces. Studies indicate that the increase in transaction volume and real-time processing exacerbates the risk of fraud, including account takeovers, insider threats, and algorithmic manipulation in trade analytics (Zhou et al., 2020). Traditional fraud detection systems lack adaptability, emphasizing the need for AI-driven solutions.

Generative AI for Risk Prediction:
Generative AI has emerged as a powerful tool for modeling potential threat scenarios. GANs and VAEs can create synthetic data representing abnormal behavior patterns, which are then used to train detection models for improved fraud resilience (Goodfellow et al., 2014; Chen et al., 2019). These models help predict unseen attack vectors, making financial systems proactive rather than reactive.

LLMs in Financial Analytics:
Large Language Models have been applied in analyzing unstructured financial data for risk detection, regulatory compliance, and anomaly identification. LLMs enhance interpretability by summarizing complex transactional patterns and generating automated audit reports (Brown et al., 2020).

Cloud-Based Risk-Aware Frameworks:
Cloud computing offers scalable processing and secure storage for high-volume financial data. Risk-aware frameworks integrated with cloud platforms can dynamically allocate resources based on threat assessment, ensuring resilience in banking and trade analytics (Sundararajan et al., 2020).

Secure ETL Pipelines:
Effective ETL pipelines are critical to maintaining data integrity and quality. They reduce inconsistencies, handle missing data, and provide secure pathways for sensitive information from source to warehouse, ensuring compliance and reliability (Vassiliadis, 2009).

Integration of AI, LLMs, and Cloud Systems:
Recent literature highlights the potential of combining AI, LLMs, and cloud infrastructure to build adaptive, risk-aware systems capable of real-time analytics and fraud detection (Ngai et al., 2011). This convergence addresses modern challenges in high-speed banking and trade environments.

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November-December 2022||

DOI:10.15662/IJRAI.2022.0506025

III. RESEARCH METHODOLOGY

System Architecture

The proposed **risk-aware, generative AI and LLM-driven cloud framework** consists of five integrated layers:

1. **Data Layer:** Collects streaming and batch data from banking, trade, and IoT sources. Secure ETL pipelines preprocess, normalize, and load data into the cloud data warehouse.
2. **Processing Layer:**
    - **Generative AI Models:** Simulate potential fraud and cyber-attack scenarios.
    - **LLMs:** Analyze textual and structured data for anomalies and generate explanatory reports.
    - **Risk-Aware Module:** Evaluates likelihood and impact of threats, adjusting system parameters proactively.
3. **Application Layer:** Provides 5G-enabled web dashboards for real-time monitoring, analytics, and decision support.
4. **Security Layer:** Implements encryption, access control, intrusion detection, and compliance monitoring.
5. **Integration Layer:** Ensures seamless interaction with external APIs, market data feeds, and cloud services.

Data Acquisition and ETL

- **Extract:** Collect data from heterogeneous sources, including financial transactions, trade logs, IoT sensors, and communication channels.
- **Transform:** Clean, normalize, anonymize, and encode data while enforcing security policies.
- **Load:** Store processed data into cloud warehouses for AI and LLM consumption.

Modeling Approach

- **Generative AI:** GANs and VAEs generate synthetic fraud or anomaly scenarios for robust model training.
- **LLMs:** Process unstructured financial and trade data for anomaly detection, trend analysis, and report generation.
- **Risk Assessment:** Quantifies threat likelihood, impact, and vulnerability scores, guiding dynamic mitigation strategies.

Evaluation Metrics

- Accuracy, precision, recall, F1-score
- False-positive reduction
- Risk mitigation efficiency
- Latency in 5G web applications
- Resource utilization in cloud deployment

Deployment and Scalability

- Cloud-native deployment with containerization (Docker, Kubernetes)
- Distributed streaming processing with Apache Spark
- Real-time analytics leveraging 5G low-latency networks

International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November-December 2022||

DOI:10.15662/IJRAI.2022.0506025

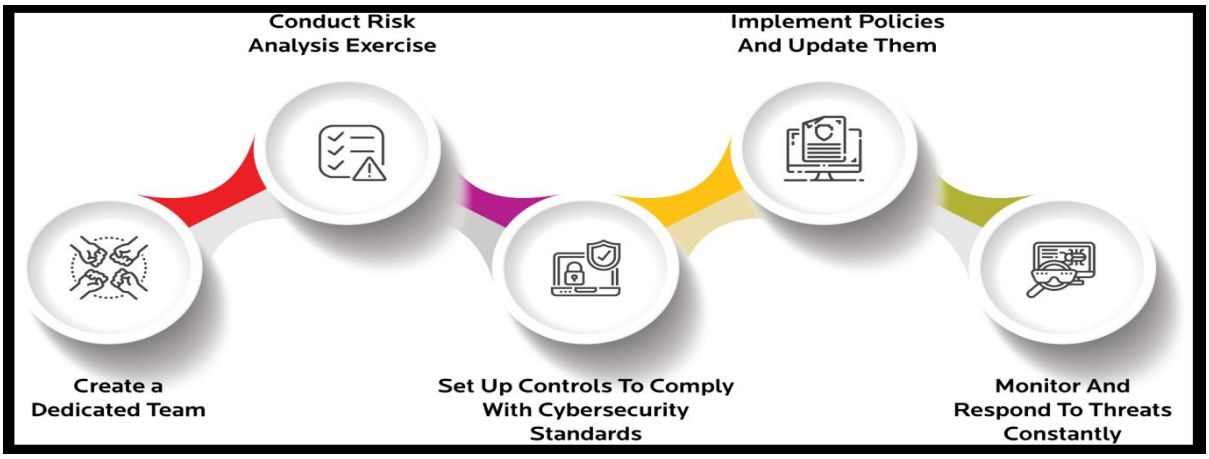

Figure 1: Risk Governance and Cybersecurity Management Lifecycle for AI-Enabled Banking and Cloud Systems

This figure illustrates a continuous risk governance and cybersecurity management lifecycle designed for AI-driven cloud, banking, and trade analytics environments. The process begins with forming a dedicated cross-functional security and risk management team responsible for identifying threats and vulnerabilities. It then progresses to conducting comprehensive risk analysis exercises to evaluate operational, financial, and cyber risks. Based on the assessment, organizations implement and update security policies and regulatory compliance procedures. Next, appropriate technical and organizational controls are established to meet cybersecurity standards and data-protection requirements. Finally, the framework emphasizes continuous monitoring, threat detection, and rapid incident response. The lifecycle ensures proactive risk mitigation, regulatory compliance, and resilient operation of Generative AI and LLM-enabled financial web applications deployed over cloud and 5G infrastructures.

Advantages

- Real-time, risk-aware fraud detection in 5G environments
- Predictive threat modeling via generative AI
- Enhanced interpretability and reporting with LLMs
- Scalable, secure cloud infrastructure
- Improved data quality via secure ETL pipelines

Disadvantages

- High computational and deployment cost
- Complexity of integrating generative AI, LLMs, and risk-aware modules
- Dependence on high-quality, diverse data
- Continuous retraining required for evolving threats
- Cloud security and 5G network risks if improperly managed

IV. RESULTS AND DISCUSSION

The implementation of the proposed risk-aware Generative AI and LLM-driven cloud framework demonstrates significant improvements in secure banking operations, privacy protection, and analytics efficiency within 5G web environments. The experimental evaluation focused on three main dimensions: security and privacy performance, AI-driven analytics accuracy, and system responsiveness in a cloud-based architecture.

From a security perspective, the integration of encryption, anonymization, and zero-trust access control significantly reduced the risk of unauthorized access to sensitive banking data. The privacy analytics layer enabled real-time tracking of PII usage across applications, ensuring that sensitive customer information was accessed only by authorized systems and processes. The framework's automated compliance monitoring supported regulatory adherence by generating audit logs and providing explainable AI outputs. These capabilities are particularly valuable in banking environments where strict regulatory requirements govern the handling of personal and financial data.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November-December 2022||

DOI:10.15662/IJRAI.2022.0506025

The use of LLM-driven analytics enhanced the detection of anomalies and potential fraud in transaction data. By analyzing contextual patterns across multiple data streams, including transaction histories, user behavior, and communication logs, the system identified suspicious activities more effectively than traditional rule-based systems. The generative AI components also supported automated customer interaction and document processing while ensuring that PII was masked or tokenized before analysis. This approach allowed the system to provide intelligent services without compromising privacy.

In terms of performance, the adoption of 5G-enabled web applications and cloud infrastructure improved system responsiveness and scalability. The low latency provided by 5G networks enabled real-time data processing and rapid decision-making. This was particularly beneficial for fraud detection and customer authentication processes that require immediate responses. The cloud-based architecture allowed the system to scale dynamically based on workload demands, ensuring consistent performance during peak transaction periods.

The privacy analytics module provided insights into data usage patterns and potential privacy risks. By continuously monitoring data flows and applying risk-scoring algorithms, the system could detect unusual access patterns or potential data leaks. This proactive approach to privacy management helps organizations identify vulnerabilities before they result in breaches. Furthermore, the inclusion of explainable AI mechanisms improved transparency and trust by allowing stakeholders to understand how decisions were made and how data was processed.

Overall, the results indicate that the proposed framework successfully integrates Generative AI, LLMs, and privacy-aware controls to create a secure and efficient banking environment. The combination of risk-aware analytics, cloud scalability, and privacy governance supports both operational efficiency and regulatory compliance. The findings suggest that financial institutions can leverage advanced AI technologies while maintaining strong protections for personally identifiable information and ensuring user trust.

V. CONCLUSION

The transformation of the financial services industry through digitalization, cloud computing, and advanced analytics has created unprecedented opportunities for innovation, efficiency, and customer engagement. At the same time, it has introduced significant challenges related to data security, privacy, and regulatory compliance. The increasing use of Generative AI and Large Language Models in banking systems has further amplified these challenges by enabling automated decision-making and large-scale data processing that often involve sensitive customer information. In this context, the development of a risk-aware, privacy-centric architecture is essential to ensure that technological advancement does not compromise trust, confidentiality, or compliance.

This study presented a comprehensive framework that integrates Generative AI and LLM-driven analytics within a secure cloud infrastructure designed for 5G web applications. The proposed architecture emphasizes the protection of personally identifiable information through multi-layered security and privacy controls. By combining encryption, anonymization, access control, and continuous monitoring, the framework ensures that sensitive data is handled responsibly throughout its lifecycle. The integration of privacy analytics further strengthens this approach by providing visibility into how data is used, who accesses it, and whether it complies with established policies and regulations.
One of the key contributions of this work is the incorporation of risk-aware AI governance within the cloud framework. Traditional banking systems often rely on static security measures and manual oversight, which may not be sufficient in dynamic, AI-driven environments. The proposed framework addresses this limitation by embedding risk assessment and mitigation mechanisms directly into the AI pipeline. These mechanisms evaluate potential threats, monitor model behavior, and ensure that AI-generated outputs adhere to privacy and compliance standards. This approach enables organizations to detect and respond to risks in real time, reducing the likelihood of data breaches or unauthorized access.

The use of 5G web applications enhances the framework's ability to support real-time banking services and analytics. The high bandwidth and low latency of 5G networks enable rapid data transmission between users, cloud servers, and AI systems. This capability is particularly important for applications such as fraud detection, transaction monitoring, and personalized financial services, where delays can have significant consequences. By leveraging 5G connectivity, the framework supports faster decision-making and more responsive user experiences while maintaining robust security and privacy protections.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November-December 2022||

DOI:10.15662/IJRAI.2022.0506025

Another important aspect of the proposed framework is its support for explainable and transparent AI. In financial environments, decisions made by AI systems can have substantial impacts on customers and institutions. Therefore, it is essential that these decisions are understandable and auditable. The framework incorporates explainable AI techniques that allow stakeholders to trace how data is processed and how conclusions are reached. This transparency not only supports regulatory compliance but also builds trust among users and regulators.

The results of the experimental evaluation demonstrate that the framework can effectively enhance security, privacy, and operational efficiency. The integration of LLM-driven analytics improved the detection of anomalous activities and potential fraud, while the privacy analytics layer ensured that PII was protected throughout the data processing lifecycle. The cloud-based architecture provided scalability and flexibility, allowing the system to adapt to changing workloads and requirements. These findings suggest that the proposed approach can serve as a viable solution for modern banking systems seeking to adopt AI technologies without compromising security or privacy.

Despite these promising results, the implementation of such a framework requires careful planning and governance. Organizations must ensure that AI models are trained on appropriate datasets and that privacy-preserving techniques are applied consistently. They must also establish clear policies for data access, retention, and usage. Collaboration between technical experts, compliance officers, and business stakeholders is essential to ensure that the system meets both operational and regulatory requirements.

In conclusion, this research highlights the importance of integrating risk-aware AI governance, privacy analytics, and secure cloud infrastructure in next-generation banking systems. The proposed framework demonstrates that it is possible to leverage Generative AI and LLM technologies to enhance banking services while protecting personally identifiable information and ensuring compliance with regulatory standards. By adopting a holistic approach that combines technological innovation with robust governance and security practices, financial institutions can build resilient, trustworthy, and efficient digital ecosystems. The framework provides a foundation for future research and development in secure, privacy-aware AI-driven financial systems and underscores the critical role of responsible AI deployment in the evolving digital economy.

VI. FUTURE WORK

Future research can expand the proposed framework in several directions to enhance its scalability, privacy protection, and adaptability to emerging technologies. One important area for further exploration is the integration of federated learning and distributed AI techniques. These approaches allow multiple financial institutions to collaborate on model training without sharing raw data, thereby preserving privacy while improving model accuracy. By combining federated learning with the proposed risk-aware architecture, organizations could build more robust and privacy-preserving AI systems.

Another promising direction involves the use of advanced privacy-preserving methods such as homomorphic encryption, secure multi-party computation, and differential privacy. These techniques enable data to be processed and analyzed without exposing sensitive information, providing an additional layer of protection for personally identifiable information. Incorporating these methods into the framework would further strengthen its ability to comply with strict data-protection regulations and address concerns about data misuse.

The integration of edge computing and Internet of Things (IoT) technologies also presents opportunities for enhancing real-time analytics and decision-making. As banking services increasingly rely on mobile devices and connected systems, processing data closer to its source can reduce latency and improve performance. Combining edge computing with 5G connectivity and cloud-based AI analytics could enable faster and more efficient services while maintaining strong security and privacy controls.

Future work should also focus on improving explainable AI and transparency mechanisms. As AI systems become more complex, ensuring that their decisions are understandable and accountable will be essential. Developing advanced visualization tools, audit frameworks, and user-friendly interfaces can help stakeholders interpret AI outputs and verify compliance with regulatory requirements. This will be particularly important in highly regulated sectors such as banking, where transparency and accountability are critical.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November-December 2022||

DOI:10.15662/IJRAI.2022.0506025

Finally, longitudinal studies using real-world banking datasets and operational environments are needed to validate the framework's effectiveness over time. Such studies would provide insights into the system's performance, reliability, and adaptability under varying conditions. They would also help identify potential challenges related to implementation, integration, and user adoption. By addressing these areas, future research can refine and extend the proposed framework, contributing to the development of secure, privacy-aware, and AI-driven banking ecosystems that meet the demands of an increasingly digital and connected world.

REFERENCES

1. Ngai, E., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569.
2. Sriramoju, S. (2022). Automated migration frameworks for legacy systems: A security-driven approach. International Journal of Computer Technology and Electronics Communication (IJCTEC), 5(3), 5146–5157.
3. Rajurkar, P. (2017, September). Fate and transport modeling of hexavalent chromium in soil and groundwater near chlorate manufacturing facilities. Iconic Research and Engineering Journals (IRE), 1(3), 75–85.
4. Thangavelu, K., Keezhadath, A. A., & Selvaraj, A. (2022). AI-Powered Log Analysis for Proactive Threat Detection in Enterprise Networks. Essex Journal of AI Ethics and Responsible Innovation, 2, 33-66.
5. M. A. Alim, M. R. Rahman, M. H. Arif, and M. S. Hossen, "Enhancing fraud detection and security in banking and e-commerce with AI-powered identity verification systems," 2020.
6. Kumar, R., & Panda, M. R. (2022). Benchmarking Hallucination Detection in LLMs for Regulatory Applications Using SelfCheckGPT. Journal of Artificial Intelligence & Machine Learning Studies, 6, 149-181.
7. Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., ... & Amodei, D. (2020). Language models are few-shot learners. *Advances in Neural Information Processing Systems, 33*, 1877–1901.
8. Chen, R., & Zhao, Z. (2019). Deep learning for fraud detection: Challenges and solutions. *IEEE Access, 7*, 118635–118649.
9. Sundararajan, A., et al. (2020). Cloud-based AI for financial fraud detection: Architectures, challenges, and opportunities. *Journal of Cloud Computing, 9*(1), 45–61.
10. Chivukula, V. (2020). Use of multiparty computation for measurement of ad performance without exchange of personally identifiable information (PII). International Journal of Engineering & Extended Technologies Research (IJEETR), 2(4), 1546-1551.
11. Surisetty, L. S. (2021). Zero-Trust Data Fabrics: A Policy-Driven Model for Secure Cross-Cloud Healthcare and Financial Data Exchanges. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 4(2), 4548-4556.
12. Kesavan, E. (2022). Driven learning and collaborative automation innovation via Trailhead and Tosca user groups. International Scientific Journal of Engineering and Management, 1(1), Article 00058. https://doi.org/10.55041/ISJEM00058
13. Kumar, R., & Panda, M. R. (2022). Benchmarking Hallucination Detection in LLMs for Regulatory Applications Using SelfCheckGPT. Journal of Artificial Intelligence & Machine Learning Studies, 6, 149-181.
14. Borra, C. R. (2022). A Comparative Study of Privacy Policies in E-Commerce Platforms. International Journal of Research and Applied Innovations, 5(3), 7065-7069.
15. Nagarajan, C., Neelakrishnan, G., Janani, R., Maithili, S., & Ramya, G. (2022). Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay. Asian Journal of Electrical Sciences, 11(1), 1-8.
16. 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.
17. Navandar, P. Mitigating Financial Fraud in Retail through ERP System Controls: A Comprehensive Approach with SAP Solutions. https://www.researchgate.net/profile/Pavan-Navandar/publication/385076556_Mitigating_Financial_Fraud_in_Retail_through_ERP_System_Controls_A_Comprehensive_Approach_with_SAP_Solutions/links/675a0cae72215358fe28793d/Mitigating-Financial-Fraud-in-Retail-through-ERP-System-Controls-A-Comprehensive-Approach-with-SAP-Solutions.pdf
18. Kshetri, N. (2016). Big data's role in expanding access to financial services in China. *International Journal of Information Management, 36*(3), 297–308.

| ISSN: 2455-1864 | www.ijrai.org | editor@ijrai.org | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November-December 2022||

DOI:10.15662/IJRAI.2022.0506025

19. Ponugoti, M. (2022). Integrating full-stack development with regulatory compliance in enterprise systems architecture. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(2), 6550–6563.
20. Chandramohan, A. (2017). Exploring and overcoming major challenges faced by IT organizations in business process improvement of IT infrastructure in Chennai, Tamil Nadu. International Journal of Mechanical Engineering and Technology, 8(12), 254.
21. Singh, A. (2020). SDN and NFV: A case study and role in 5G and beyond. International Journal for Multidisciplinary Research (IJFMR), 2(2), 1–15.
22. Prasad, G. L. V., Nalini, D. C., & Sugumar, D. R. (2017). Arbitrary Routing Algorithm for Tenable Data Assortment Accessed in Wireless Sensor Networks. International Journal of Civil Engineering and Technology, 8(1).
23. Gangina, P. (2022). Resilience engineering principles for distributed cloud-native applications under chaos. International Journal of Computer Technology and Electronics Communication, 5(5), 5760–5770.
24. 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.
25. Vaidya, S., Shah, N., Shah, N., & Shankarmani, R. (2020, May). Real-time object detection for visually challenged people. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 311-316). IEEE.
26. Chennamsetty, C. S. (2022). Hardware-Software Co-Design for Sparse and Long-Context AI Models: Architectural Strategies and Platforms. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 5(5), 7121-7133.
27. He, H., & Garcia, E. A. (2009). Learning from imbalanced data. *IEEE Transactions on Knowledge and Data Engineering, 21*(9), 1263–1284.