



Cloud-First Compliance Data Meets Governance

Dimitris Plexousakis
Asst Professor

Abstract

Translated into English, the Ukrainian fifteenth-century account of the life of Saint Nicholas Chernogorsky reflects the development of post-Byzantine hagiography. The narrative—considered to be a translation, but more often viewed as an imitation—has been cultivated not only by linguists and historians, but also by hagiographers and folklorists. The life of Saint Nicholas Chernogorsky, between Latinizations and Ostrogization, represents a renaissance in old belated hagiography. The question arises to what extent these elements of Latinizations, as well as Neo-Greek aspects and east-European influences, ought to be emphasized in this Redaction X of Radziwiłł's Bychowiec Chronicle and consequently its authorship and dating, medial functions, stylistics and sources.

The fifteenth-century life of Saint Nicholas Chernogorsky translated from Greek affirms the Greek-Old Slavonic axis of post-Byzantine hagiography. Even if the work is considered an imitation rather than a translation—something that would overcome its relations to the Bychowiec Chronicle—the hagiographer's choice nevertheless represents a renaissance of old belated hagiography. The thematic climax of the narrative can be defined as the pursuit of a saintly ideal, altered by an ostrogization in accord with political amalgamation.

Keywords : Cloud-Native Data Platform, Intelligent Governance, Financial Crime Compliance, Money Laundering, Counter-Terrorism Financing, Sanctions, Fraud Management, Transaction Monitoring, Screening, Intelligence, Risk Management.

<H1> Introduction

Cloud-native data platforms, designed expressly for the demands of distributed applications, can transform the financial crime compliance landscape—Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), sanctions controls, fraud detection, and the associated data-gathering capabilities—by reducing costs, enhancing scalability, and enabling advanced analytics. Combined with an intelligent governance framework that implements a policy-driven, model-based, and centralized design, such platforms deliver a comprehensive and cohesive solution and provide a sound rationale for transformation. Governance addresses the establishment of an operational framework, and complaints policy within the organization—setting the context within which advanced analytics can be implemented.

Financial crime compliance is normally seen as a necessary evil, generating substantial operational costs but offering limited competitive advantage. Although risk-based practices have helped to reduce cost and improve efficiency, the effectiveness of financial crime compliance remains a concern for regulators and financial organizations alike. The emergence of cloud-native data platforms—data management environments designed expressly for the demands of distributed applications—now offers the potential to transform the economics of compliance by reducing costs, enhancing scalability, and enabling advanced analytics for anomaly detection, natural language processing, and network analytics.

<H1> Foundations of Financial Crime Compliance



Financial Crime Compliance encompasses four primary domains: Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), sanctions, and fraud. Financial institutions are subject to a complex web of national and supranational regulations and play a key role in preventing financial crime by detecting and reporting suspicious activity. Despite the importance of effective compliance, paradoxically, compliance departments are entrusted with the generation of ever-growing false positive alerts. Financial Crime Compliance is fundamentally an exercise in risk management, requiring the prioritization of limited resources against the risks of reputation loss, revenue loss, regulatory breach, and criminal sanction.

Financial Crime compliance consists of four domains: anti-money laundering, counter-terrorist financing, sanctions compliance, and fraud prevention. The global financial industry is subject to a complex web of regulations, issued by national and supranational authorities, supported by the Financial Action Task Force, money laundering task forces, and political organizations such as the European Union. Financial institutions operating in jurisdictions vulnerable to financial crime are required to implement robust financial crime compliance programs. Non-financial organizations, including gatekeepers of the financial system, are subject to CTF regulatory requirements. The compliance departments of these organizations play a crucial role in the early stages of the detection process and are tasked with evaluating the suspicious activity of clients, applicants, parties against whom transactions are contemplated, and counterparties with whom clients intend to conduct a business relationship.

Table 1: Financial Crime Compliance Domains

Domain	Primary Objective
Anti-Money Laundering (AML)	Detect and report suspicious financial activity

Domain	Primary Objective
Counter-Terrorist Financing (CTF)	Prevent financing of terrorist activities
Sanctions Compliance	Ensure transactions do not involve sanctioned entities
Fraud Prevention	Detect and prevent fraudulent transactions

<H1> Cloud-Native Data Platforms: Concepts and Architectures

Cloud-native data platforms are characterized by the design and delivery of data services on cloud systems and infrastructures. Concepts and architectural choices underlying three key aspects of a cloud-native data platform—data management and interoperability, and scalability, reliability, and security—are summarized.

3.1 Data Management and Interoperability

The meaning of data, as expressed in its model, schema, structure, and metadata, is fundamental for an organization. It should be available in readily understandable and usable forms for identity resolution, and AML, CTF, and sanction compliance functions. Data needs to be standardized and made interoperable across use cases, enabling different types of data to be combined for richer analysis.

Standardized metadata provides a defining description of data sources, including details of the data's purpose, quality, and usage. It also supports data catalogue services, enabling users to find and access relevant data, while providing the necessary information for auditing, lineage definition, and risk assessment. Data lineage describes how data transforms as it flows through pipelines, applications, repositories, and services. Data cataloging automates and enriches the production of data catalogs and scales across all enterprise-



managed data. Common exchange formats, such as Avro or Parquet, run efficiently on cloud-native architectures and decouple data producers from data consumers.

<H2> Data Management and Interoperability

Compliance operations generate, manipulate, and analyze large amounts of data, data models designed for efficient storage, retrieval, and application. As these operations span at least the four domains of Sanctions, Anti-Money Laundering, Counter-Terrorist Financing, and Fraud, the data models must enable effective linking and cross-domain analysis—often called interoperability. Such standardization is further supported by the organization’s metadata registers (conceptual data model, data lineage and catalog) that provide natural language descriptions of business concepts, their definitions, synonyms, and controlling logics, relations between concepts or sources of concepts and governing authorities. It also covers standard formats for exchanging data—Common Data Format (CDF)—data quality evaluations—Common Data Quality Metrics (CDQM)—and data lineage/provenance description—Common Data Provenance Model (CDPM).

It is crucial to ensure that on-premise data repositories implement interoperability. Each schema in these stores, independent of its data model, is considered a dedicated repository for one logical business concept—the organization controls and governs the data in-house so that their quality is warranted. Data in Cloud-Native environments are stored in multi-tenant designs, leading to shared schema designs that undermine data ownership and therefore data quality. Such data become transactional data without deciding values to signify the correctness/validity of business concepts; the data required for compliance operations must always ensure that they are owned by the organizations to allow quality and business control. A governance policy therefore defines controls, level of probing and access approvals required based on the sensitivity of the business concept where lack of privacy is perceived—for Data Quality Management and Data Ownership Management.

<H1> Intelligent Governance Frameworks

Financial crime compliance operates in a complex regulatory environment, which is constantly evolving. Different areas are governed by different regulations, with authorities around the world updating them individually. However, financial institutions often derive and enforce compliance requirements from the same or similar regulations. Policy-driven governance frameworks formalize requirements by monitoring authoritative sources for updates and distilling them into machine-readable compliance rules. These rules are expressed in an abstract natural language, normalizing and harmonizing diverse semantics. Annotations capture the governance context to facilitate decision-making. Automated workflows ensure compliance processes are executed fully and appropriately, with audit trails providing evidence of completed activities.

In addition to financial crime compliance, intelligent policy-driven governance frameworks can support many other areas of regulatory compliance, including data protection, consumer protection, anti-money laundering, and anti-bribery. Individual organizations often govern, monitor, and manage compliance for these diverse areas independently, relying on different systems and engaged by different teams. Recognizing commonalities and synergies shared by the compliance domains can help organizations move toward more integrated governance frameworks without sacrificing their discipline-specific focus.

<H2>. Policy-Driven Compliance and Rule Normalization

Financial crime compliance must adapt and evolve as financial criminal activity and related regulations change. This is commonly achieved through the revision of policies and rules; however, the application of new policy versions rarely replaces, rather than supplements, the rules encoded within financial crime systems. The introduction of new rules that perform the same or overlapping operations as existing rules need to be correctly managed to avoid excessive false positive alerts. To reduce the risk of



compliance, an intelligent rule governance framework that encompasses the entire rule life cycle is thus required.

A policy-driven compliance approach constructs compliance rules derived from internal and external guidelines and acts as a central configuration management point for all rules applied throughout the compliance operation. To be genuinely policy driven, the underlying compliance rules must be automatically created, authorized, managed, and maintained, with the operation controlled and validated using a decision workflow and audit trail. An equally sophisticated solution is required for incoming compliance alerts. The normalization, deduplication, harmonization, and operations of compliance-related alerts—money laundering reporting officers’ and management investigations, transaction monitoring alerts, screening hits, and AML transaction monitoring alerts—should be closely aligned. This integrated handling entails a merged alert service that receives inputs from various systems but operates on a common alert set that executes consistent information-gathering processes, provides a unified investigation view, enables efficient organization and management of accumulated alerts, and generates consolidated reporting.

<H1> Integrating Cloud-Native Platforms into Compliance Operations

Although cloud-native platforms provide extensive new capabilities and support new functional domains, such capabilities alone are insufficient for effective financial crime compliance. The successful integration of these platforms into compliance operations is vital to capitalizing on the newly enabled capabilities, especially those involving advanced analytical techniques and artificial intelligence. Such integration comprises the specific processes, controls, governance elements, and business requirements that direct the cloud-native platforms to satisfy compliance needs. The processes that ingest data into the platforms, the quality of the ingested data, and the provenance information recorded in the platform must meet compliance requirements. Other aspects of the integration govern the application of advanced

analytics techniques for investigation and intelligence gathering.

Data ingestion into a cloud-native platform must satisfy two types of requirements: business/process requirements for the platform, and second, security and privacy concerns at the data’s source. The various business requirements for the platform need to be satisfied, often facilitated by technical features such as schema-on-read support. The control objectives need to be addressed through controls such as data quality checks during ingestion and provenance tracking from data sources through to the platform. Finally, such cloud-native techniques as distributed processing, combined with careful consideration during feature engineering, can ease the challenge of applying anomaly detection techniques.

<H2> Data Ingestion, Quality, and Provenance

Data ingestion encompasses processing and feeding data into a compliance system at rest. An ingestion pipeline defines the required processing and transforms either data at rest or in motion. Data-flow pipelines are a specific subtype of ingestion pipeline that ingests data transmitted from source A to destination B. A schema-on-read approach offers flexibility, allowing field definitions only at the time of use. Data quality checks verify that the current data conforms to expected standards. Provenance recording annotates data with its source and processing history, such as the applied addition of a column or alteration of data values. Such information aids in visualizing data lineage – usually a directed acyclic graph – enabling identification of all data products originating from a relevant input, all data products contributing to a relevant output, or all processing steps involved.

Data systems commonly offer end-to-end data lineage functionality, capturing ingest-to-archive provenance for data at rest and part of data in motion. Data lineage semantics capture necessary domain-specific concepts for formal or semi-formal representation. Data lineage can also denote an entity’s degree of alteration across different tips of



the lineage direction. Tamper-evidence guarantees that a system can detect if some data product has been modified. Complex data pipelines can inherently provide, or can be augmented to supply, these properties given real-time requirements. Business availability goals, business priority of compliance use cases, and data-source tampering evidence are the aspects that drive the need for data-flow real-timeness.

Table 2: Core Technology Capabilities and Benefits

Capability	Key Benefits
Cloud-Native Data Platform	Scalability, interoperability, cost efficiency
Intelligent Governance Framework	Policy-driven rules, auditability, rule lifecycle management
Advanced Analytics & AI	Anomaly detection, NLP, network analytics

<H1> Advanced Analytics and Artificial Intelligence in Compliance

A wide array of advanced analytics and AI techniques can enhance compliance operations, particularly in the detection of anomalous behaviour and the usage of naturally occurring language in exploring intelligence documents. Sophisticated anomaly detection capabilities that incorporate feature engineering and other non-standard methods can provide an important additional line of defence as supervised anomaly detection models often suffer from false-positive fatigue and the need to render a large number of alerts for human evaluation. A mixture of techniques for detection and evaluation of anomalies, especially supervised models, can mitigate these issues. Neural embedding-based generative networks that learn the fault distribution via normal class

instances are attractive in that they generate new samples from the learnt distribution, facilitating anomaly detection in logistic regression and other classifiers. In addition to their important intrinsic value, anomaly detection models also serve to guide interpretive analytics, particularly for graph data.

Compliance is heavily dependent on understanding, processing and applying large volumes of unstructured natural language text. This creates a high demand for NLP methods and solutions, all of which must conform to the requirements of compliance-sensitive applications. Operations such as named entity extraction, entity relationship extraction, sentiment and intention classification are central to the analytics on natural language data produced by regulatory-alerts, case notes, external threat intelligence data (sanctions lists, PEPs, negative news) etc. The fusion of such information is critical for understanding risk exposure. The automated reading of such documentation introduces an additional layer of risk that requires mitigation, namely model bias and explainability.

A well-planned deployment of advanced analytics and AI-based capabilities provides a strong foundation for improved performance in financial crime compliance going well beyond injective automation, enhancing both effectiveness at reasonable cost and support to skilled human resources.

<H2> Anomaly Detection and Network Analytics

Anomaly detection plays a vital role in financial crime compliance and risk management, leveraging supervised or unsupervised learning on multiple data types, including transactional, behavioral, alert, and risk network data. Detecting material anomalies from non-material or merely suspicious, and in a timely manner, remains a formidable challenge. For supervised methods, carefully designed features and up-to-date models are critical while addressing the class imbalance problem; for unsupervised methods, method evaluation and tuning demand special attention. Fake alerts generated by models deployed in production may exhaust analytical resources and impair detection



capabilities. Monitoring feature distributions and patterns with the support of human domain knowledge typically helps reinforce model performance. Network analytics provides query-based risk analysis for money flows in threat networks.

All money transfer activities within the considered period can be modeled as a graph comprising nodes and edges. The nodes represent the anti-money laundering (AML) entities (e.g. individuals, organizations, banks), and the edges capture the transaction records among these entities. Network analysis is conducted using two perspectives: network risk analysis and money flow analysis. Tools such as Sentimental Network Analysis and Stacked Edge Bundle can aid AML professionals to swiftly identify high-risk entities and suspicious transaction patterns embedded in huge amounts of money flows.

<H1> Conclusion

Both cloud-native platforms and intelligent governance frameworks enable granularity in policy decision-making that supports more effective compliance operations. Advanced analytics and artificial intelligence enhance the effectiveness of all financial crime domains; anomaly detection improves the identification of suspicious transactions, while natural language processing aids in the interpretation and extraction of intelligence from unstructured data sources.

In summary, Cloud-native data platforms and intelligent governance frameworks present an answer to key limitations in current Financial Crime Compliance (FCC) arrangements and operations in the banking sector. Cloud-native principles applied to data platforms improve the sharing of information within banks and between banks and other organizations, facilitate advanced analytics, and enable the application of artificial intelligence technologies. Intelligent governance frameworks align policy requirements with policy-delivering systems and support granular decision-making at all levels of the organization. However, integration of cloud-native data platforms and intelligent governance frameworks into FCC

operations is yet to be addressed. Cloud-native principles applied to data platforms improve the sharing of information within banks and between banks and other organizations, facilitate advanced analytics, and enable the application of artificial intelligence technologies. Intelligent governance frameworks align policy requirements with policy-delivering systems and support granular decision-making at all levels of the organization. However, integration of cloud-native data platforms and intelligent governance frameworks into FCC operations is yet to be addressed.

<H2> Future Trends

Financial crime remains a deep and persistent concern. Despite heavy investments in compliance operations, the effectiveness of detection and investigation has not improved drastically, and risk management at the enterprise level remains inadequate. Cloud-native data platforms enable quick and easy integration and advanced analytics, allowing for enhanced detection, network analysis, and intelligence gathering from a compliance perspective. However, the lack of aligned operations and quality governance poses challenges. The interplay between advanced analytics and artificial intelligence in compliance strikes an optimistic note for financial crime detection and responsible financial intermediation.

A trend toward technology-driven development in financial crime compliance support and service provision should improve the effectiveness and scalability of compliance operations. Emerging regulatory technologies are shifting the paradigm around regulatory compliance reporting and policy system management. Financial and securities sector regulators are supporting cloud innovation in financial services, including regulatory technology, by providing a technology-neutral approach to investigating and carrying out policy-driven solutions in a cloud-native manner. New generation natural language processing capabilities can transform structured and unstructured case investigation support and help through intelligence support, providing useful clues about future money flows through risk detection on sanctioned entities.



<H1> References

1. Akande, N. A., Olasehan, O. A., Oluwagbotemi, J. F., Duruemeruo, C. U., & Ani, S. (2023). AI-driven governance and zero trust automation for continuous cloud compliance and secure access. *Iconic Research and Engineering Journals*, 6(9), 545–559.
2. Alsousi, A., & Shah, A. (2022). Data governance for SME: Systematic literature review. *Journal of Information Systems and Digital Technologies*, 4(2).
3. Chaudhari, A. R., Gohil, B. N., & Rao, U. P. (2023). A review on cloud security issues and solutions. *Journal of Computer Security*, 31(4).
4. Mangalampalli, B. M. (2024). Transparent Intelligence Explainability Frameworks for AI-Driven Clinical Decision Support in Healthcare Business Intelligence. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 7(3), 10566-10579.
5. Espinha Gasiba, T., Andrei-Cristian, I., Lechner, U., & Pinto-Albuquerque, M. (2021). Raising security awareness of cloud deployments using infrastructure as code through cybersecurity challenges. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–8.
6. Ngesimani, N. L., Ruhode, E., & Harpur, P.-A. (2022). Data governance in healthcare information systems: A systematic literature review. *South African Journal of Information Management*, 24(1), Article a1475.
7. Naguib, H. M., Kassem, H. M., & Abou Naem, A. E.-H. M. (2024). The impact of IT governance and data governance on financial and non-financial performance. *Future Business Journal*, 10, Article 15.
8. Mattaparthi, R. (2024). Transformer-Based Fault Diagnosis for Large-Scale Standby Power Generators: Partial Discharge Pattern Recognition at Hyperscale Data Center Installations. *Journal of Computational Analysis and Applications (JoCAAA)*, 33(08), 8781-8799.
9. Naik, S. (2023). Cloud-based data governance: Ensuring security, compliance, and privacy. *The Eastasouth Journal of Information System and Computer Science*, 1(1), 69–87.
10. Parast, F. K., Sindhav, C., Nikam, S., Yekta, H., & others. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, 114, 102580.
11. Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, 217, 109358.
12. Ukeje, N., Gutiérrez, J. A., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. *International Journal of Information Security*, 23, 1459–1475.
13. Loganathan, R., & Kolla, S. H. (2024). Harnessing generative AI for adaptive risk policy generation in multi-regulatory data center environments. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 15(3), 505-515.
14. Shahane, R. (2022). Enhancing data governance in multi-cloud environments: A focused evaluation of Microsoft Azure's capabilities and integration strategies. *Journal of Computational Analysis and Applications*, 30(2), 536–548.
15. Jayaram, Y. (2023). Data governance and content lifecycle automation in the cloud for secure, compliance-oriented data operations. *International Journal of AI, BigData, Computational and Management Studies*, 4(3), 124–133.
16. Pentyala, D. K. (2023). Cloud-based solutions for AI-enhanced data governance and assurance. *International Journal of Engineering and Computer Science*, 12(8), 25815–25834.
17. Perumal, A. P., Deshmukh, H., Chintale, P., Desaboyina, G., & Najana, M. (2022). Implementing zero trust architecture in financial services cloud environments in Microsoft Azure security framework. *International Journal of Circuit, Computing and Networking*, 3(2), 75–80.



18. Faragallah, O. S. (2021). AI-enabled financial data governance using a secure cloud-based framework for enterprise compliance and automation. *International Journal of Research Publications in Engineering, Technology and Management*, 4(5).
19. Kolla, S. H., & Peddi, R. K. (2024). Designing Governance-Aligned GenAI Pipelines Using Small Language Models for Enterprise Workflow Intelligence. *International Journal of Science, Research and Technology*, 7(6), 13256-13268.
20. Ogeawuchi, J. C., Akpe, E. E., Abayomi, A. A., Agboola, O. A., Ejiole, O., & Owoade, S. (2022). Systematic review of advanced data governance strategies for securing cloud-based data warehouses and pipelines. *International Research in Engineering Journals*, 6(1).
21. Reddy, M. S. (2024). Advancing data security and privacy in cloud computing: A systematic literature review of challenges and innovations. *International Journal of Computer Applications and Information Technology*, 2024.
22. Khoda Parast, F., Sindhav, C., Nikam, S., Yekta, H., & others. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, 114, 102580.
23. Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, 217, 109358.
24. Chaudhari, A. R., Gohil, B. N., & Rao, U. P. (2023). A review on cloud security issues and solutions. *Journal of Computer Security*, 31(4).
25. Reddy, V. A. R. (2024). Generative Intelligence for Healthcare Claims Processing and Personalized Benefits Management. *International Journal of Advanced Engineering Science and Information Technology (IJAESIT)*, 7(3), 14099.
26. Ukeje, N., Gutiérrez, J. A., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. *International Journal of Information Security*, 23, 1459–1475.
27. Naguib, H. M., Kassem, H. M., & Abou Naem, A. E.-H. M. (2024). The impact of IT governance and data governance on financial and non-financial performance. *Future Business Journal*, 10, Article 15.
28. Gasiba, T. E., Lechner, U., & Pinto-Albuquerque, M. (2021). Security awareness and secure infrastructure-as-code practices for cloud deployments. *Proceedings of the International Conference on Availability, Reliability and Security*, 1–8.
29. Ngesimani, N. L., Ruhode, E., & Harpur, P.-A. (2022). Data governance in healthcare information systems: A systematic literature review. *South African Journal of Information Management*, 24(1), Article a1475.
30. Alsousi, A., & Shah, A. (2022). Data governance for SME: Systematic literature review. *Journal of Information Systems and Digital Technologies*, 4(2).
31. Naik, S. (2023). Cloud-based data governance: Ensuring security, compliance, and privacy. *The Eastasouth Journal of Information System and Computer Science*, 1(1), 69–87.
32. Pentyala, D. K. (2023). Cloud-based solutions for AI-enhanced data governance and assurance. *International Journal of Engineering and Computer Science*, 12(8), 25815–25834.
33. Mangala, N. (2022). Real-Time Data Quality Monitoring and Gating Frameworks in Cloud-Based Data Pipelines. *International Journal of Research and Applied Innovations*, 5(6), 8197-8219.
34. Jayaram, Y. (2023). Data governance and content lifecycle automation in the cloud for secure, compliance-oriented data operations. *International Journal of AI, BigData, Computational and Management Studies*, 4(3), 124–133.
35. Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Computer Networks*, 217, 109358.
36. Perumal, A. P., Deshmukh, H., Chintale, P., Desaboyina, G., & Najana, M. (2022). Implementing zero trust architecture in financial services cloud environments in Microsoft Azure security framework. *International Journal of Circuit, Computing and Networking*, 3(2), 75–80.



37. Ukeje, N., Gutiérrez, J. A., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. *International Journal of Information Security*, 23, 1459–1475.
38. Naguib, H. M., Kassem, H. M., & Abou Naem, A. E.-H. M. (2024). The impact of IT governance and data governance on financial and non-financial performance. *Future Business Journal*, 10, Article 15.
39. Khoda Parast, F., Sindhav, C., Nikam, S., Yekta, H., & others. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, 114, 102580.
40. Mahadevan, S. (2024). Clouding the Future: Innovating Towards Net-Zero Emissions. *International Journal of Computing and Engineering*, 6(2), 17-23.
41. Analyzing transparency and malicious insiders prevention for cloud computing environment. (2024). *Computers & Security*, 137, 103622.
42. Cloud data leakage, security, privacy issues and challenges: Review. (2024). *Procedia Computer Science*, 242, 592–601.