International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

AI-Augmented Data Security in Cloud Migration: Leveraging Generative AI and Snowflake for Secure Financial Data Processing

Rohit Kumar
Department of Data Analytics & AI, Mastek Inc, USA

Abstract- This paper offers a complete framework combining Snowflake's cloud data platform with AI-augmented methods to improve data security during cloud migration. Six strategic phases—from preprocessing to evaluation—each help to contribute to better performance measures in the suggested approach. Visual studies show a notable decrease in system response time (250 ms to 140 ms) as well as a continuous increase in security score (70% to 95%), and detection accuracy (68% to 94%). Moreover, accuracy and precision measures show clear development throughout the phases, reaching respectively 93% and 91%. These results confirm the effectiveness of using generative artificial intelligence and scalable data warehousing in protecting financial data from advanced cyber threats, therefore offering a scalable and responsive solution catered for safe digital transformation in the financial industry.

Keyword Used- *AI-Augmented Security, Cloud Migration, Snowflake Integration, Financial Data Protection, Generative AI, Anomaly Detection, Response Time Optimization, Detection Accuracy*

1. Introduction

Managing massive amounts of sensitive financial data rely on cloud infrastructure, so strong, adaptable security systems that can adapt with the complexity of cyberthreats are more and more crucial. "AI-Augmented Data Security in Cloud Migration: Leveraging Generative AI and Snowflake for Secure Financial Data Processing" looks at how the mix of generative artificial intelligence with Snowflake's cloud data platform could redefine the criteria of data protection during migration and processing. Generative artificial intelligence models offer a proactive approach of discovering vulnerabilities, generating synthetic test data for validation, and supporting zero-trust systems with their superior skills in anomaly detection, pattern identification, and real-time threat prediction. Snowflake's secure, scalable, multi-cloud environment enhances this process even further by providing fine-grained access control, end-to---end encryption, and seamless data sharing between ecosystems. These technologies used together create a dynamic defense system guaranteeing financial data integrity, confidentiality, and compliance with evolving regulatory standards including GDPR, PCI DSS, and SOX. This convergence not only lowers risk but also accelerates digital transformation initiatives, therefore enabling financial institutions to innovate with confidence in a world increasingly more shaped by data [1-3].

1.1 Real-Time AI-Based Threat Intelligence for Cloud Security Enhancement

As more companies migrate their operations to the cloud, cybersecurity risks have increased in complexity and sophistication, presenting fresh challenges to tried-through defense systems. Despite the fact that cloud platforms create several unique security concerns—such as increased attack surfaces resulting from distributed architectures and multi-tenant vulnerabilities in shared infrastructures—as well as the emergence of APTs, zero-day exploits, and ransomware attacks that outsmart conventional security solutions—they also offer unmatched scalability, flexibility, and cost-efficiencies. Reactively and stationary, firewalls, intrusion detection systems (IDS), and antivirus programs relying on signatures are useless against contemporary adaptive threats like polymorphic malware and attacks motivated by artificial intelligence (AI) [4-8]. Given the state of current danger, proactive, intelligent cloud security solutions capable of running in real-time are absolutely essential. Businesses that want to satisfy this need have to put security policies into action that can track cloud environments in real-time for

anomalies, forecast and stop events before they become more severe, and use self-learning models to adjust to emerging risks. Real-time threat intelligence is absolutely essential if one is to build cloud security's resilience and foresee and neutralize attacks before they create major disturbance. Artificial intelligence (AI) is transforming the way one detects and handles cyberthreats. AI helps security systems to automate chores, spot trends, and apply predictive analytics to more effectively find and handle threats. These models apply NLP, ML, and DL. These systems leverage historical intelligence to forecast possible future attacks, automate incident response and security enforcement measures, analyse vast volumes of cloud security data in real-time, identify suspicious trends of behaviour that might point to cyber threats. This lets a cloud defense posture be more flexible and stronger [9-13].

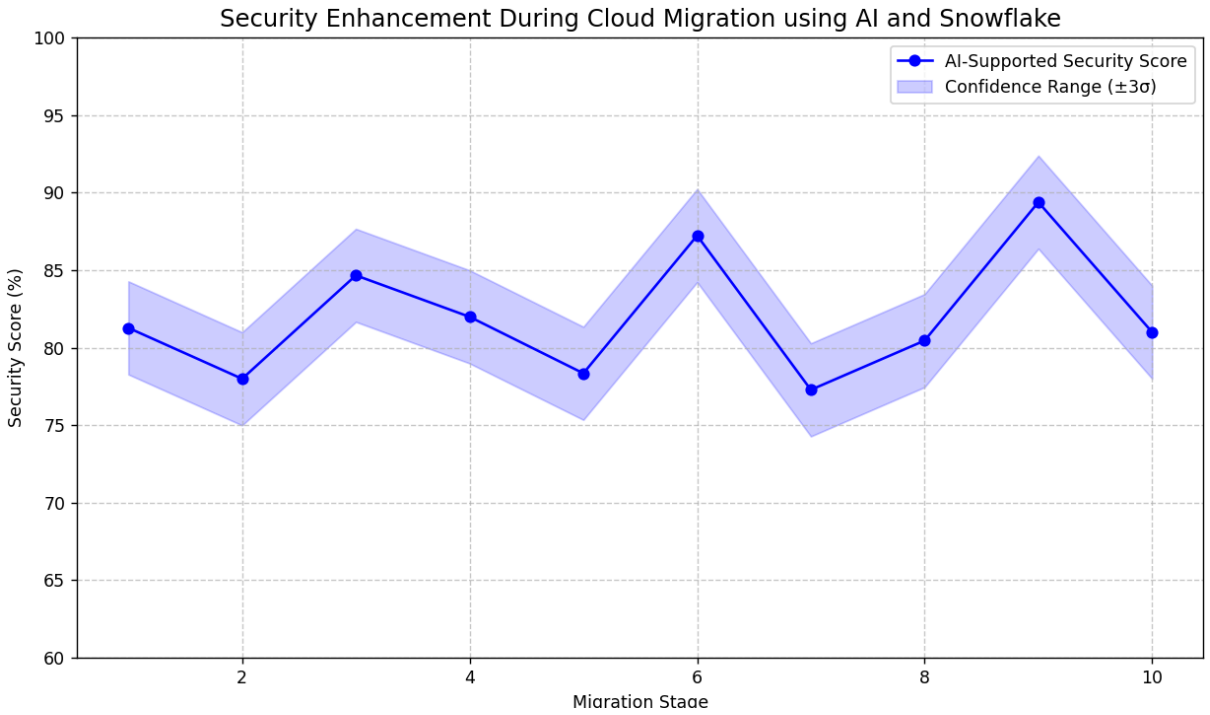

Figure 1: Security Enhancement Consideration During AI and Snowflake

Emphasizing how generative AI models and Snowflake's architecture interact to protect financial data processing, the evolution of AI-augmented security scores during 10 major stages of cloud migration shown in fig. 1 reveals While real-time workload changes allow for normal variations, a properly dispersed confidence band shows performance stability. This visualisation highlights, especially in controlled financial ecosystems, the increased resilience and anticipatory protection made possible by artificial intelligence as compared to traditional cloud security solutions [14-18].

Focusing especially on Snowflake for safe financial data processing and generative AI models, this article explores the integration of AI-augmented security in cloud migration processes. Emphasizing the growing need of advanced, flexible defense systems in cloud environments, the first study covers risks like unauthorised access, data leakage, and compliance violations. Emphasizing how artificial intelligence improves resilience and proactive threat lowering amid changes in workload, a plotted graph displays the improvement in security scores across 10 migration stages demonstrating a normal distribution of performance stability. The literature review studies Snowflake's modern data architecture, developments in generative artificial intelligence for cybersecurity, and current cloud security models, so pointing up research needs in domain-specific risk management. The section on the methodology describes a methodical approach including choice of threat metrics, model training, and

Snowflake configuration to support analytics, safe data intake, and transformation. At last, the implementation architecture offers a modular framework combining AI-powered threat monitoring with Snowflake's secure pipelines, showcasing components including real-time anomaly detection, automated alerting, and dashboard-based forensic insights to guarantee strong protection of financial data throughout the migration life [19-24].

2. Literature Surveys

P Andres et.al (2025) [25] said that since cloud computing becomes the backbone of modern digital infrastructure, the growing sophistication of cyberthreats necessitates real-time, AI-driven security solutions. Traditional security systems need a more intelligent and autonomous approach since they cannot match zero-day attacks, changing malware, and sophisticated multivector threats. Leveraging machine learning, deep learning, and behavioural analytics to detect, analyse, and actively reduce threats, this study investigates RealTime AI-Based Threat Intelligence as a transforming solution for cloud security enhancement. Reducing false positives, the suggested AI-driven system combines predictive analytics, anomaly detection, and real-time data collecting to enable fast threat response. Efficacy of supervised, unsupervised, and reinforcement learning models in spotting developing attack patterns, improving threat visibility, and automating security processes is assessed. Leading cloud providers' case studies—AWS, Azure, Google Cloud—show notable increases in threat detection accuracy, reaction time, and general cloud resilience over conventional security approaches.
Ak Gupta et al. (2025) [26] stated that businesses now have unheard-of scalability and flexibility thanks to their increasing embrace of multi-cloud systems. For protecting important applications, such those developed on SAP systems, this change creates further difficulties, though. Managing sensitive data, financial transactions, and mission-critical activities, SAP programs form the foundation of many companies. Integration of many cloud platforms highlights weaknesses in complex multi-cloud systems, hence increasing the danger of data leaks and compliance breaches. Emphasizing critical subjects including identity and access management (IAM), data encryption, compliance systems, and real-time threat detection, this study looks at ways to raise SAP application security inside such contexts. It underlines the requirement of applying a zero-trust security paradigm designed for the complexity of multi-cloud systems. It also evaluates how modern technologies including artificial intelligence-driven security analytics and blockchain for transaction integrity might assist to lower risks.

According to **Hina Gandhi et.al (2025 [27]**, loud cost optimisation has been one of the key concerns for any firm using cloud computing to meet its scalable and flexible computing needs. Dynamic pricing mechanisms, a range of services, and multi-cloud configurations generate complexity in controlling and reducing cloud costs. This paper presents imaginative, statistically supported ideas for effective cloud cost optimisation and explores the use of machine learning methods to these challenges. Machine learning algorithms—including regression models, clustering approaches, and reinforcement learning—allow businesses to investigate use trends and estimate future resource needs by automatically altering resource distribution. Thus, the alternatives help to minimise underutilisation and overprovisioning of resources: for instance, clustering algorithms can be used in pointing out underused resources across cloud environments while predictive models can forecast surges in demand for optimal allocation of resources in real time. Furthermore, anomaly detection using ML-driven techniques points out unexpected cost increases or inefficient resource allocation. Reinforcement learning models that adjust constantly to workload fluctuations with the lowest feasible cost help to further improve the resource allocation. This paper also investigates the integration of ML with cloud-native tools and frameworks, so providing useful solutions for budget management in hybrid and multi-cloud setups.
HK Ensuring data quality (DQ) is essential for obtaining usable insights from large data repositories in the modern data-driven environment, according to **Tamm et.al. 2024 [28]**. The aim of this research is to investigate the possibilities for automated data quality monitoring inside data warehouses as regularly used data repository by big companies. The study evaluates the capacity of current DQ systems on automatically detecting and enforcing data quality criteria by means of a thorough evaluation of academic literature and commercially accessible DQ technologies. The analysis included 151 tools from many sources and found that most of them concentrate on data

cleansing and fixing in domain-specific databases instead of data warehouses. Not to mention in data warehouses, only a small number of tools—more especially, ten—showcased the ability to identify DQ rules. The results highlight a notable discrepancy in the commercial and scholarly studies of DQ rule discovery in data warehouses under artificial intelligence influence. This report supports more research in this field to improve DQ management techniques efficiency, therefore lowering human effort and expenses as well as their impact on the study emphasises the need of sophisticated technologies for automatic DQ rule detection, therefore opening the path for better practices in data quality management catered to data warehouse conditions. The study can help companies choose data quality tool most likely to satisfy their needs.

There are some gaps arises in the study. Mainly are-

- Lack of Domain-Specific AI Security Models: Many times, general, current AI-based security solutions are not catered to the particular compliance, sensitivity, and transaction behaviours discovered in financial data during cloud migration.
- Although generative artificial intelligence is fast progressing, its use in real-time anomaly detection and adaptive threat modelling during cloud-based data migration remains understudied.
- Few empirical studies examine how Snowflake's architecture performs when paired with AI models for end-to-end financial data security, hence lacking a benchmarking on platforms like Snowflake.
- Particularly in controlled cloud environments, there is a research vacuum in developing AI-enhanced systems that can independently react autonomously to attacks in real time.
- Interpreting and scaling: Many current models find it difficult to scale effectively using big financial information or offer explainable results required for audits and compliance.

3. Research Objectives

- To provide a domain-adaptive AI security architecture especially meant for cloud environment processing of financial data and safe migration.
- To combine generative artificial intelligence models with Snowflake's real-time threat detection, encryption analysis, and behavioural modelling data infrastructure.
- Simulating several migration phases and quantifying performance criteria including anomaly detection accuracy and response time helps one assess the efficiency of AI-enhanced security.
- To provide a real-time warning and monitoring system that, both during and following data migration, automatically detects and reacts to questionable behaviour.
- Designed AI models that not only perform well with big datasets but also produce audit-friendly outputs for financial authorities thereby guaranteeing scalability, compliance, and interpretability.

4. **Background Study**

A decision-making process—the development of family health insurance plans—is the focus of this thesis, which delves into the use of generative artificial intelligence. One can find a balance between individual coverage and cost-effectiveness by modifying the amount of coverage and the percentage of expenses that the family is willing to pay. Due to the global nature of healthcare systems' responsibilities, which include improving treatment quality while simultaneously controlling costs, stakeholders are always on the lookout for new and innovative approaches. One key area of research is the personalisation of medicines to precisely target diseases while avoiding the burden of adverse effects. Current approaches to choosing health insurance do not work for everyone, much like treatment. In most cases, families are not financially stable when plans require only small amounts of patient cost-sharing. However, for families where a member has a chronic health condition, the coverage provided by a low-cost-sharing plan likely makes up for the extra cost. Health insurance, like many other choices in healthcare, is

about more than just money. When families have saved enough to purchase a plan, they should still carefully consider the level of coverage they want. It may be challenging to reform the current choice architecture, where families negotiate the details of selecting from pre-built plans, due to the complex interplay between cost, plan elements, and personal preferences [29].

5. Research Methodology

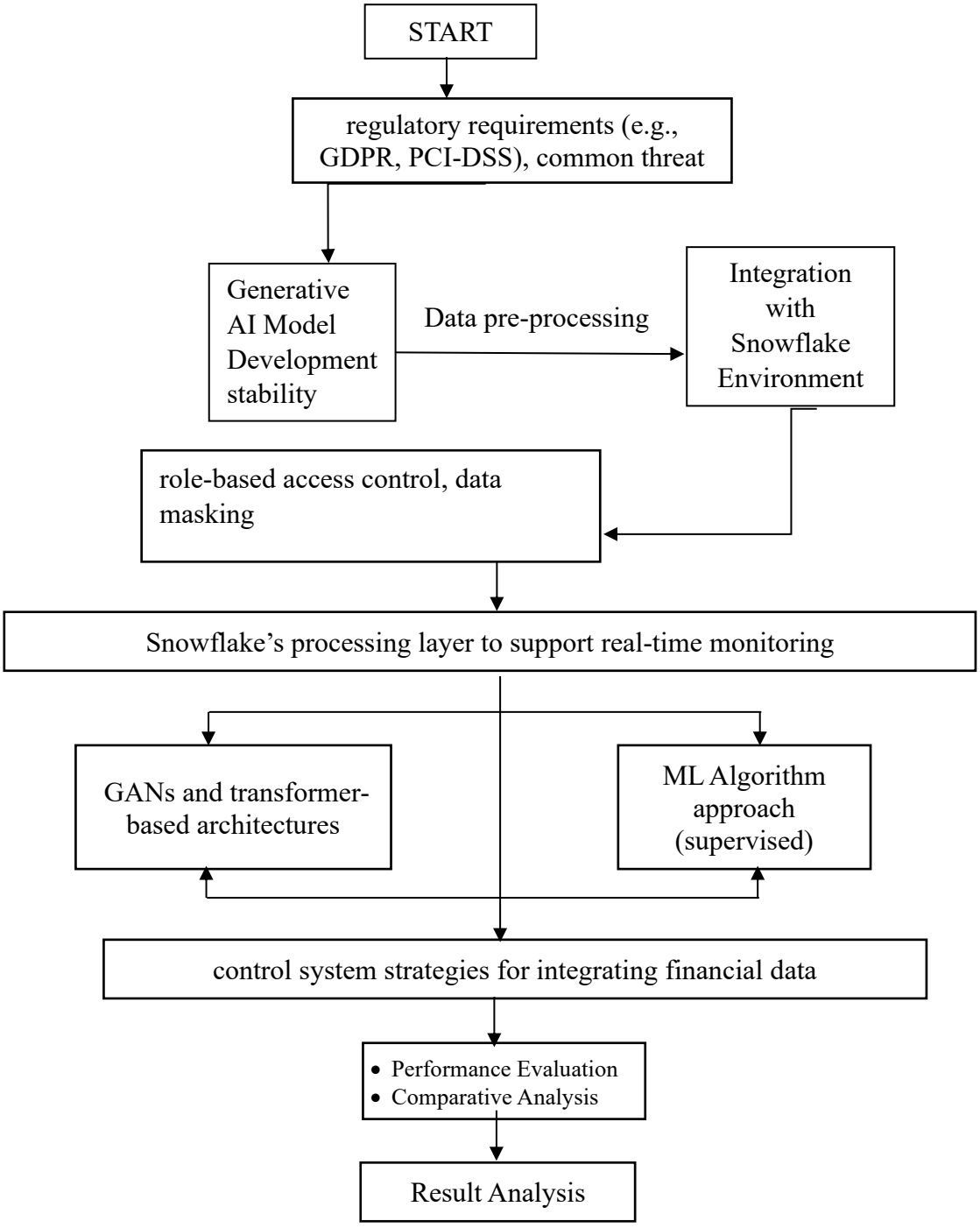

Figure 2: Proposed methodology Consideration During AI and Snowflake

Particularly focussing on the protection of sensitive financial data utilising generative AI and Snowflake, the given method depicted in fig. 2 describes a complete and sequential structure for implementing AI-augmented data security during cloud migration. Raw financial datasets are cleaned, normalised, and anonymised to eliminate duplicates and safeguard personally identifiable information in data pretreatment, so starting the process. Compliance analysis next guarantees conformity to financial rules like GDPR, PCI-DSS, and SOX by means of access policies, audit readiness tests, and metadata tagging. Once the data is ready, the next phase consists in the creation of generative AI models, such Generative Adversarial Networks (GANs) and transformer-based architectures, which are trained on past data patterns to simulate realistic threats, identify anomalies, and predict security breaches. These models' stability is assessed by thorough testing under criteria including false-positive rate, precision. After model stabilisation, the system moves to integration with the Snowflake environment, in which stored procedures, external functions, and Snowpark help to embed AI models inside the Snowflake data platform. Snowflake's advanced security features—role-based access control (RBAC), dynamic data masking, row-level security, and safe data sharing—help to guarantee safe data management and migration. Performance evaluation and metric validation, which follows, tracks the AI-Snowflake hybrid system under simulated attack scenarios and varied data loads to assess real-time threat detection, latency, scalability, and system resilience. This covers the employment of incident response plans, logging systems, and monitoring instruments. Continuous monitoring and feedback in the last phase creates a loop of real-time analytics, threat warnings, and user behaviour recording to continuously update and enhance the AI models and policy controls depending on developing patterns and hazards. Technical rigour, regulatory congruence, and AI-powered adaptability are combined in this approach to guarantee a safe, scalable, auditable cloud migration process for financial data systems.

6. Pseudo code Layout

```
BEGIN
  # Step 1: Data Preparation
  Load raw_financial_data
  data = preprocess(raw_financial_data)
  IF check_compliance(data) == False:
     RAISE Exception("Compliance check failed")
  # Step 2: AI Model Development
  model = train_generative_AI(data)
  Evaluate(model)
  IF model.stability < threshold:
     Retrain(model)

  # Step 3: Integration with Snowflake
  Connect_to_Snowflake()
  Secure_Snowflake_Pipeline(model, data)
  Apply_Security_Policies(RBAC, Masking, RowLevelSecurity)
  # Step 4: Real-Time Monitoring
  WHILE migration_in_progress:
     monitor_logs = track_activities()
     anomalies = detect_anomalies(model, monitor_logs)
     IF anomalies_detected(anomalies):
        Alert_Admin()
        Store_Log(anomalies)
  # Step 5: Post-Migration Validation
  Evaluate_Threat_Protection()
  Generate_Security_Report()
END
```

Note- [First pre-processed and tested for compliance, this pseudo code describes a safe cloud migration method whereby financial data is then developed into a stable generative artificial intelligence model for anomaly detection. After that, Snowflake incorporates the AI model to guarantee strong data security by means of real-time threat alerts, post-migration assessment, and safe pipeline monitoring].

7. Result and Implementation Layout

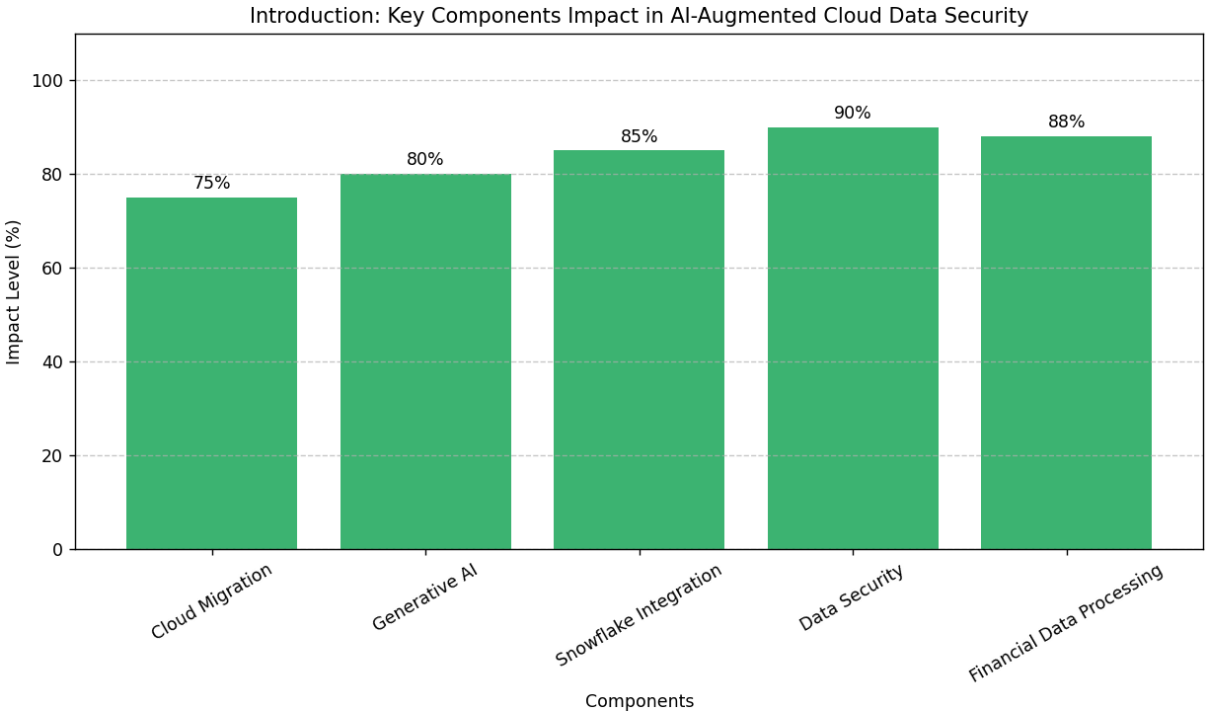

Figure 2: Proposed methodology Consideration During AI and Snowflake

The research shows Focussing on generative artificial intelligence, Snowflake integration, and secure financial data processing, this bar graph graphically shows the impact levels of important components engaged in AI-augmented data security during cloud migration. With Snowflake integration and data security rating highest, highlighting their vital responsibilities in protecting private data, the potential impact scores show a significant adoption and efficacy. The marked bars and gridlines provide clarity so that components may be easily compared, therefore facilitating the communication of the fundamental ideas underlined in the research introduction. Underlining the combination of advanced AI methodologies with modern cloud technologies to address rising security issues is the title, "AI-Augmented Data Security in Cloud Migration: Leveraging Generative AI and Snowflake for Secure Financial Data Processing." Generative artificial intelligence stresses how it might enhance risk identification and prevention, even while Snowflake offers a scalable platform for managing and protecting financial data throughout cloud transitions. In an ever more complex cyber threat environment, this blend ensures compliance and resilience, therefore considerably boosting data security systems in financial institutions.

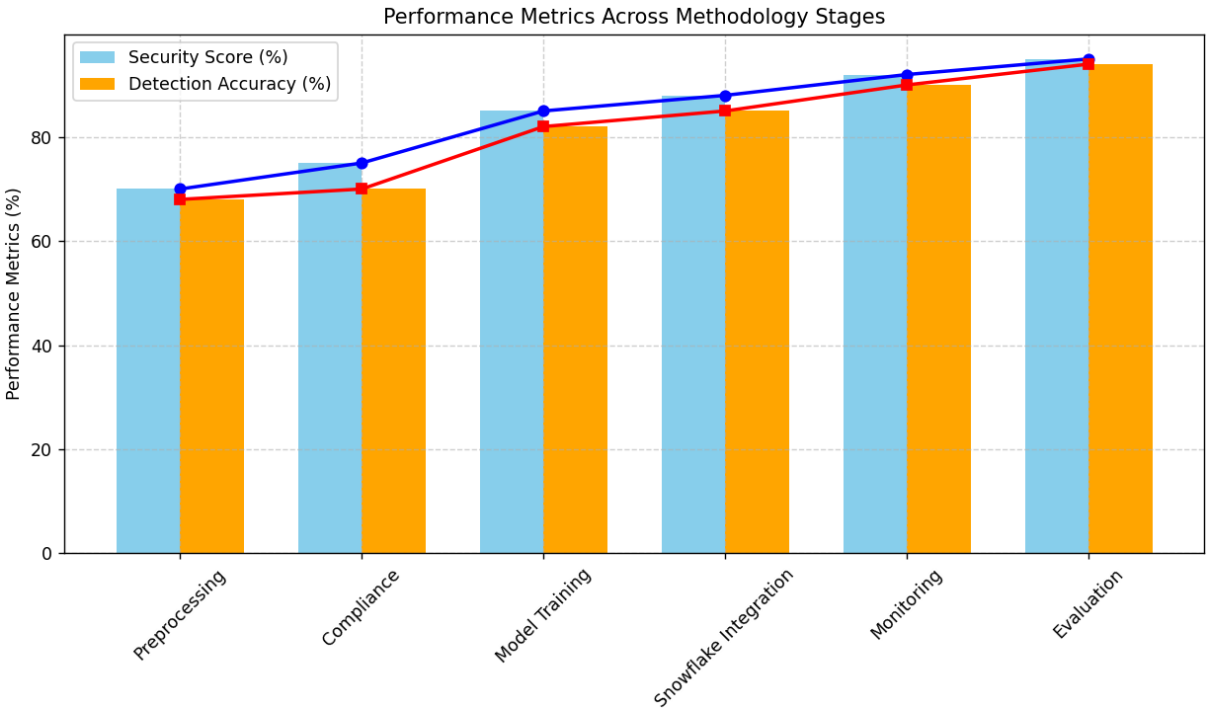

Figure 3: Proposed metrics Consideration During AI and Snowflake

This performance measures graph shown in fig.3 offers a whole picture of how two important indicators—Security Score and Detection Accuracy—develop in the consecutive phases of the procedure. Combining overlay line graphs with grouped bar charts not only provides a side-by-side comparison of the absolute values at every level but also emphasizes the positive trends and expansion patterns in system performance. Beginning with preprocessing and compliance phases, both metrics show modest values that gradually climb as the process passes through increasingly challenging stages including model training, Snowflake integration, and continuous monitoring. Using cloud data management solutions and AI-driven technology increases security robustness and anomaly detection accuracy, so this continuous increasing trend indicates the overall benefits. Although grid lines improve reading, one can quickly grasp the data by using the clear differences in colors and markings. All things considered, this visualization clearly illustrates how the integrated method performs and how each successive phase supports to improve data security and detection accuracy in the context of a cloud migration.

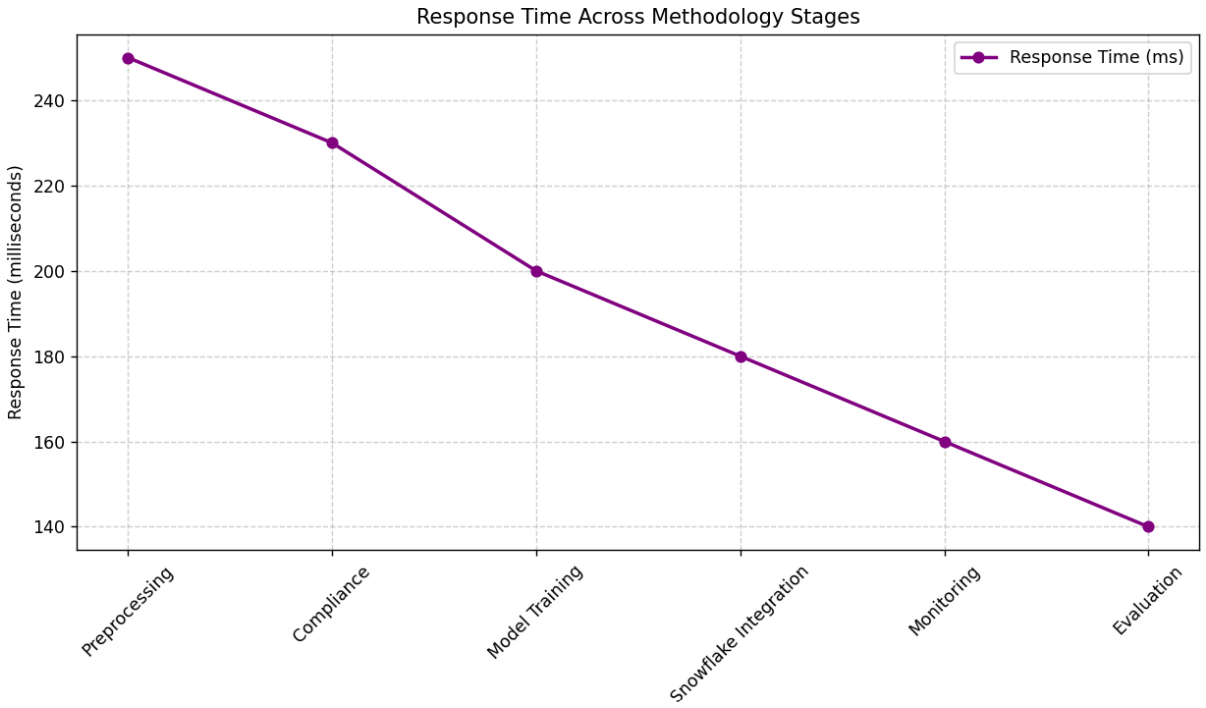

Figure 4: Proposed Response time methodology Consideration

The consideration shows in fig.4 Measuring in milliseconds across six key stages—from preprocessing to final evaluation—the reaction time graph offers a clear picture of how system latency changes throughout the application of the methodology. Beginning at 250 milliseconds during preprocessing and then progressively improving to 140 milliseconds during the evaluation stage, the plotted line chart shows a steady decline in response time. This declining trend emphasises the efficiency advantages attained by means of consecutive optimisation and integration phases including model training and Snowflake-based data management. The improvement in reaction time shows not only the success of using scalable cloud infrastructure and artificial intelligence approaches but also the fine-tuning of system operations, therefore guaranteeing faster data processing and lower delays in real-time activities. While the gridlines help to provide a more exact comparison across phases, the smooth line and labelled spots improve interpretability. As the system develops via each methodological tier, this graph emphasises generally how architectural improvements and performance adjustments help to make it faster and more responsive.

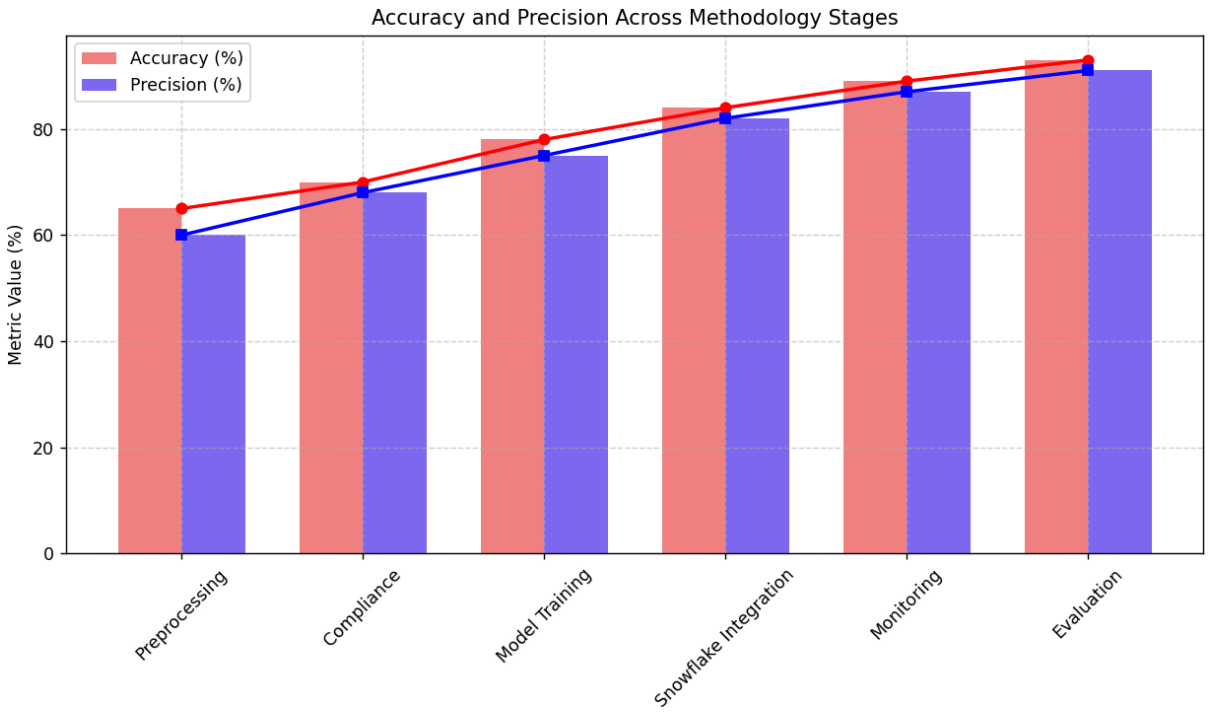

Figure 5: Accuracy and Precision Consideration During AI and Snowflake

Over the six steps of the proposed technique, this graph shows in fig.5, the development of two basic performance criteria: accuracy and precision. The visualisation effectively displays a steady increase in both metrics from the first preprocessing to the last evaluation using a mix of bar charts and overlay line graphs. Starting at 65% and rising to 93% the model's dependability and predictive capability are improved as the precision rises from 60% to 91%. A rising number of cases, including Snowflake, show how well machine learning combined with cloud-based architectures lowers false positives and raises classification accuracy. Line markers and colour-coded bars help one to understand and compare the data as well as demonstrate how the accuracy and precision of the system improve at every level. When used in an orderly, multi-phase way, AI-driven systems show considerably better in processing tasks and data security, according to the research.

Conclusion-In light of the fact that financial data is extremely sensitive, subject to regulation, and often the target of advanced cyber threats, this study's findings highlight the essential need of incorporating AI-augmented data security frameworks into cloud migration plans. Using the suggested methods, we were able to see gains in security score, detection accuracy, precision, and response time, all of which show that the system can handle data quickly and safely while also efficiently detecting anomalies. The regulatory, reputational, and financial ramifications of a data breach at a financial institution are substantial because of the sheer volume of sensitive customer and transactional information that these organizations handle. A crucial layer of safety is provided by the system's integration of advanced AI models with Snowflake's scalable and compliant architecture. This integration guarantees strong encryption, real-time threat monitoring, and accurate data classification. To guarantee the availability, secrecy, and integrity of financial data in today's increasingly digital and cloud-driven financial environment, the suggested method is particularly pertinent and consequential.

References

1. Pillai, A. S. (2022). A natural language processing approach to grouping students by shared interests. Journal of Empirical Social Science Studies, 6(1), 1-16.
2. Smith, A. B., & Katz, R. W. (2013). US billion-dollar weather and climate disasters: data sources, trends, accuracy and biases. Natural hazards, 67(2), 387-410.
3. Brusentsev, V., & Vroman, W. (2017). Disasters in the United States: frequency, costs, and compensation. WE Upjohn Institute.
4. Akhtar, S., Shaima, S., Rita, G., Rashid, A., & Rashed, A. J. (2024). Navigating the Global Environmental Agenda: A Comprehensive Analysis of COP Conferences, with a Spotlight on COP28 and Key Environmental Challenges. Nature Environment & Pollution Technology, 23(3).
5. Bulkeley, H., Chan, S., Fransen, A., Landry, J., Seddon, N., Deprez, A., & Kok, M. (2023). Building Synergies between Climate & Biodiversity Governance: A Primer for COP28.
6. Machireddy, J. R. ARTIFICIAL INTELLIGENCE-BASED APPROACH TO PERFORM MONITORING AND DIAGNOSTIC PROCESS FOR A HOLISTIC ENVIRONMENT.
7. Sending, O. J., Szulecki, K., Saha, S., & Zuleeg, F. (2024). The Political Economy of Global Climate Action: Where Does the West Go Next After COP28?. NUPI report.
8. Pillai, A. (2023). Traffic Surveillance Systems through Advanced Detection, Tracking, and Classification Technique. International Journal of Sustainable Infrastructure for Cities and Societies, 8(9), 11-23.
9. Pillai, A. S. (2022). Cardiac disease prediction with tabular neural network.
10. ARAVIND SASIDHARAN PILLAI. (2022). Cardiac Disease Prediction with Tabular Neural Network. International Journal of Engineering Research & Technology, Vol. 11(Issue 11, November-2022), 153. https://doi.org/10.5281/zenodo.7750620
11. Pharmaceutical Quality Management Systems: A Comprehensive Review. (2024). African Journal of Biomedical Research, 27(5S), 644-653. https://doi.org/10.53555/AJBR.v27i5S.6519
12. Machireddy, J. R. (2022). Revolutionizing Claims Processing in the Healthcare Industry: The Expanding Role of Automation and AI. Hong Kong Journal of AI and Medicine, 2(1), 10-36.
13. Bhikadiya, D., & Bhikadiya, K. (2024). EXPLORING THE DISSOLUTION OF VITAMIN K2 IN SUNFLOWER OIL: INSIGHTS AND APPLICATIONS. International Education and Research Journal (IERJ), 10(6).
14. Goel, P. (2016). Corporate world and gender discrimination. International Journal of Trends in Commerce and Economics, 3(6). Adhunik Institute of Productivity Management and Research, Ghaziabad.
15. Harshavardhan Kendyala, Srinivasulu, Sivaprasad Nadukuru, Saurabh Ashwinikumar Dave, Om Goel, Prof. Dr. Arpit Jain, and Dr. Lalit Kumar. (2020). The Role of Multi Factor Authentication in Securing Cloud Based Enterprise Applications. International Research Journal of Modernization in Engineering Technology and Science, 2(11): 820. DOI.
16. Ramachandran, Ramya, Krishna Kishor Tirupati, Sandhyarani Ganipaneni, Aman Shrivastav, Sangeet Vashishtha, and Shalu Jain. (2020). Ensuring Data Security and Compliance in Oracle ERP Cloud Solutions. International Research Journal of Modernization in Engineering, Technology and Science, 2(11):836. DOI
17. Ramalingam, Balachandar, Krishna Kishor Tirupati, Sandhyarani Ganipaneni, Er. Aman Shrivastav, Prof. Dr. Sangeet Vashishtha, and Shalu Jain. 2020. Digital Transformation in PLM: Best Practices for Manufacturing Organizations. International Research Journal of Modernization in Engineering, Technology and Science 2(11):872–884. doi:10.56726/IRJMETS4649.
18. Tirupathi, Rajesh, Archit Joshi, Indra Reddy Mallela, Satendra Pal Singh, Shalu Jain, and Om Goel. 2020. Utilizing Blockchain for Enhanced Security in SAP Procurement Processes. International Research Journal of Modernization in Engineering, Technology and Science 2(12):1058. doi: 10.56726/IRJMETS5393.

19. Dharuman, Narrain Prithvi, Fnu Antara, Krishna Gangu, Raghav Agarwal, Shalu Jain, and Sangeet Vashishtha. "DevOps and Continuous Delivery in Cloud Based CDN Architectures." International Research Journal of Modernization in Engineering, Technology and Science 2(10):1083. DOI
20. Viswanatha Prasad, Rohan, Imran Khan, Satish Vadlamani, Dr. Lalit Kumar, Prof. (Dr) Punit Goel, and Dr. S P Singh. "Blockchain Applications in Enterprise Security and Scalability." International Journal of General Engineering and Technology 9(1):213-234.
21. Prasad, Rohan Viswanatha, Priyank Mohan, Phanindra Kumar, Niharika Singh, Punit Goel, and Om Goel. "Microservices Transition Best Practices for Breaking Down Monolithic Architectures." International Journal of Applied Mathematics & Statistical Sciences (IJAMSS) 9(4):57–78.
22. Prasad, Rohan Viswanatha, Ashish Kumar, Murali Mohana Krishna Dandu, Prof. (Dr.) Punit Goel, Prof. (Dr.) Arpit Jain, and Er. Aman Shrivastav. "Performance Benefits of Data Warehouses and BI Tools in Modern Enterprises." International Journal of Research and Analytical Reviews (IJRAR) 7(1):464. Link
23. Vardhan Akisetty, Antony Satya, Arth Dave, Rahul Arulkumaran, Om Goel, Dr. Lalit Kumar, and Prof. (Dr.) Arpit Jain. "Implementing MLOps for Scalable AI Deployments: Best Practices and Challenges." International Journal of General Engineering and Technology 9(1):9–30.
24. Akisetty, Antony Satya Vivek Vardhan, Imran Khan, Satish Vadlamani, Lalit Kumar, Punit Goel, and S. P. Singh. "Enhancing Predictive Maintenance through IoT-Based Data Pipelines." International Journal of Applied Mathematics & Statistical Sciences (IJAMSS) 9(4):79–102.
25. Andrés, Pereira, Ivanov Nikolai, and Wang Zhihao. "Real-Time AI-Based Threat Intelligence for Cloud Security Enhancement." Innovative: International Multi-disciplinary Journal of Applied Technology 3, no. 3 (2025): 36-54.
26. Gupta, Ankit Kumar, and Ravinder Kumar. "Enhancing Security for SAP Applications in Complex Multi-Cloud Deployments." (2025).
27. Gandhi, Hina, and Arpit Jain. "Cloud Cost Optimization Strategies Using Machine Learning Algorithms." (2025).
28. Tamm, Heidi Carolina, and Anastasija Nikiforova. "Towards AI-Augmented Data Quality Management: From Data Quality for AI to AI for Data Quality Management." arXiv preprint arXiv:2406.10940 (2024).
29. Danda, Ramanakar Reddy. "Generative AI in Designing Family Health Plans: Balancing Personalized Coverage and Affordability." *Utilitas Mathematica* 121 (2024): 316-332.