International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|

DOI: 10.15662/IJSRAT.2026.0902013

Enterprise Scale AI Driven Cloud Systems for Cybersecurity Focused Healthcare and Financial Risk Analytics

Bhavesh Dilip Patel

Senior Cloud Engineer, Tororo, Uganda

Publication History: Received: 29.01.2026; Revised: 27.02.2026; Accepted: 03.03. 2026; Published: 07.03.2026.

ABSTRACT: The rapid digitization of healthcare and financial systems has increased exposure to cyber threats and systemic risks, necessitating robust, scalable, and intelligent solutions. This paper explores the design and implementation of enterprise-scale artificial intelligence (AI)-driven cloud systems tailored for cybersecurity-focused healthcare and financial risk analytics. By leveraging cloud-native architectures, machine learning models, and real-time data processing frameworks, these systems enable proactive threat detection, anomaly identification, and predictive risk mitigation. In healthcare, such systems enhance patient data protection, ensure regulatory compliance, and detect breaches in electronic health record (EHR) systems. In financial services, they facilitate fraud detection, credit risk assessment, and market anomaly prediction. The integration of AI with cloud infrastructure supports scalability, cost-efficiency, and continuous learning through adaptive algorithms. However, challenges such as data privacy, model bias, and system interoperability persist. This study proposes a hybrid framework combining deep learning, zero-trust security models, and distributed cloud computing to address these issues. The findings highlight the transformative potential of AI-driven cloud ecosystems in strengthening cybersecurity resilience and improving risk analytics across critical sectors.

KEYWORDS: AI-driven cloud systems, cybersecurity, healthcare analytics, financial risk analytics, machine learning, cloud computing, anomaly detection, data privacy, fraud detection, predictive analytics

I. INTRODUCTION

The modern digital economy is increasingly dependent on interconnected systems that manage sensitive data across healthcare and financial sectors. As organizations transition from legacy systems to cloud-based infrastructures, the volume, velocity, and variety of data have grown exponentially. This transformation has introduced new vulnerabilities, making cybersecurity a top priority. At the same time, organizations require sophisticated analytics to manage risks, detect fraud, and ensure compliance with regulatory frameworks. Artificial intelligence (AI), when combined with cloud computing, offers a promising solution to these challenges by enabling scalable, intelligent, and adaptive systems.

Healthcare systems generate vast amounts of sensitive patient data through electronic health records (EHRs), wearable devices, and telemedicine platforms. Protecting this data from unauthorized access and cyberattacks is critical, as breaches can lead to severe consequences, including identity theft and compromised patient care. Similarly, financial institutions process millions of transactions daily, making them prime targets for fraud, money laundering, and cyber intrusions. Traditional security measures, such as rule-based systems, are no longer sufficient to handle the complexity and sophistication of modern threats.

AI-driven cloud systems provide a paradigm shift in addressing these issues. By leveraging machine learning algorithms, these systems can analyze large datasets in real time, identify patterns, and detect anomalies that may indicate potential threats. Cloud computing offers the infrastructure required to scale these operations, enabling organizations to process massive amounts of data efficiently. Furthermore, cloud platforms provide advanced security features, including encryption, identity management, and continuous monitoring, which enhance overall system resilience.

One of the key advantages of AI-driven systems is their ability to learn and adapt over time. Unlike traditional systems that rely on predefined rules, AI models can evolve based on new data, improving their accuracy and effectiveness. For

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|

DOI: 10.15662/IJSRAT.2026.0902013

example, in healthcare, AI can detect unusual access patterns in patient records, signaling potential breaches. In finance, machine learning models can identify fraudulent transactions by analyzing historical data and detecting deviations from normal behavior.

Another important aspect is the integration of cybersecurity with risk analytics. In healthcare, risk analytics can help identify vulnerabilities in IT systems, assess the likelihood of breaches, and prioritize mitigation strategies. In finance, risk analytics plays a crucial role in credit scoring, market analysis, and fraud detection. By combining AI with cloud-based risk analytics, organizations can achieve a holistic view of their security posture and make informed decisions.

However, the adoption of AI-driven cloud systems is not without challenges. Data privacy is a major concern, particularly in healthcare, where regulations such as HIPAA impose strict requirements on data handling. Similarly, financial institutions must comply with regulations such as GDPR and Basel III. Ensuring that AI systems adhere to these regulations requires careful design and implementation. Additionally, issues such as model bias, lack of transparency, and interoperability between different systems must be addressed.

This paper aims to explore the architecture, applications, and challenges of enterprise-scale AI-driven cloud systems for cybersecurity-focused healthcare and financial risk analytics. It examines existing literature, proposes a comprehensive framework, and discusses the advantages and limitations of such systems. The goal is to provide insights into how organizations can leverage AI and cloud technologies to enhance their cybersecurity capabilities and improve risk management.

II. LITERATURE REVIEW

The intersection of artificial intelligence, cloud computing, cybersecurity, and risk analytics has been widely studied in recent years. Researchers have explored various approaches to integrating these technologies to address the growing challenges in healthcare and financial sectors.

Early studies focused on the use of machine learning algorithms for intrusion detection systems (IDS). These systems utilized supervised and unsupervised learning techniques to identify malicious activities in network traffic. While effective to some extent, these approaches were limited by their inability to scale and adapt to evolving threats. With the advent of cloud computing, researchers began exploring distributed architectures that could handle large-scale data processing.

In healthcare, studies have highlighted the importance of securing electronic health records (EHRs). Researchers have proposed encryption techniques, access control mechanisms, and blockchain-based solutions to enhance data security. More recently, AI-based approaches have been introduced to detect anomalies in user behavior and identify potential breaches. These systems leverage deep learning models, such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), to analyze complex patterns in data.

Financial risk analytics has also seen significant advancements with the adoption of AI. Machine learning models are widely used for credit scoring, fraud detection, and market prediction. Techniques such as decision trees, support vector machines (SVMs), and neural networks have been employed to improve accuracy and efficiency. Cloud-based platforms have enabled financial institutions to process large volumes of transaction data in real time, facilitating faster decision-making.

Recent literature emphasizes the importance of integrating cybersecurity with risk analytics. Researchers argue that traditional approaches, which treat these domains separately, are insufficient in addressing modern challenges. Integrated systems that combine threat detection with risk assessment provide a more comprehensive solution. For example, AI models can be used to predict the likelihood of a cyberattack and assess its potential impact on organizational operations.

Another emerging trend is the use of zero-trust security models in cloud environments. These models assume that no entity, whether inside or outside the network, can be trusted by default. AI plays a crucial role in implementing zero-trust architectures by continuously monitoring user behavior and detecting anomalies.

Despite these advancements, several challenges remain. Data privacy and security are major concerns, particularly when dealing with sensitive information. Researchers have proposed techniques such as differential privacy and

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|
DOI: 10.15662/IJSRAT.2026.0902013

federated learning to address these issues. Additionally, the interpretability of AI models remains a challenge, as complex models often operate as "black boxes," making it difficult to understand their decision-making processes.

III. RESEARCH METHODOLOGY

The research methodology for this study is designed to explore, design, and evaluate enterprise-scale AI-driven cloud systems for cybersecurity-focused healthcare and financial risk analytics. The approach combines qualitative and quantitative methods, system design principles, and experimental validation.

The study begins with a comprehensive requirements analysis to identify the key challenges and needs of healthcare and financial organizations. This involves analyzing existing systems, regulatory requirements, and threat landscapes. Data is collected from various sources, including academic literature, industry reports, and case studies. The analysis focuses on identifying common vulnerabilities, data processing needs, and performance requirements.

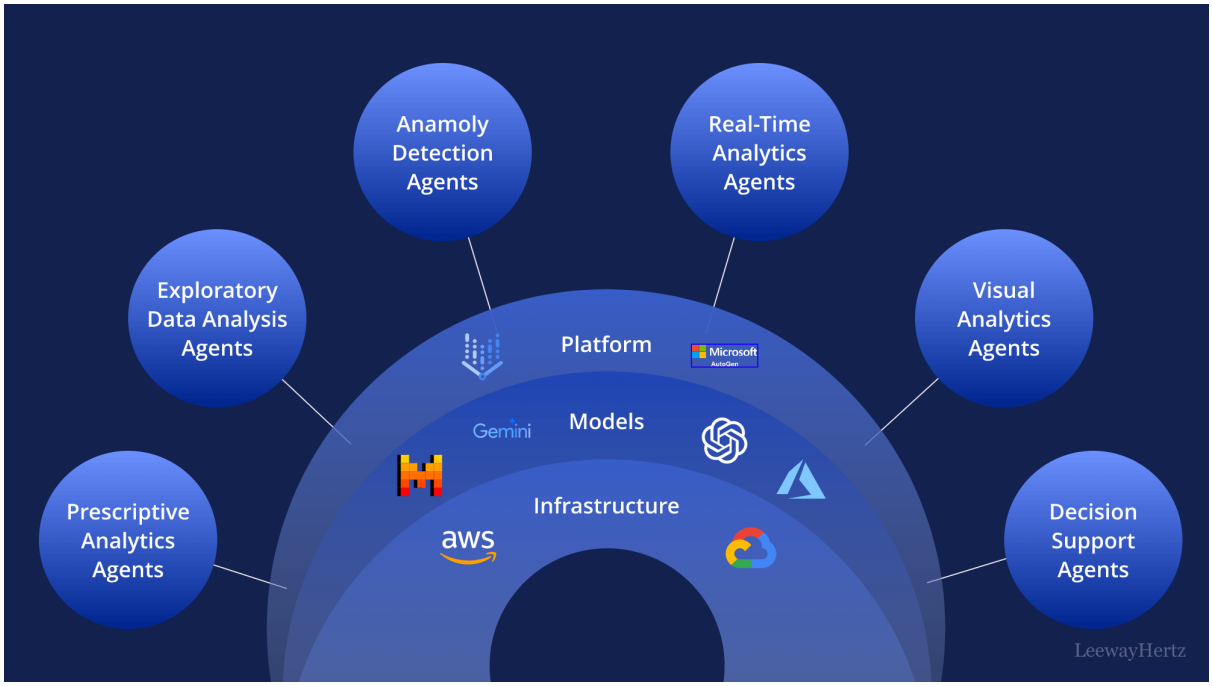

FIG1: Enterprise Scale AI Driven Cloud Systems

The next step involves designing a conceptual framework for the AI-driven cloud system. The framework is based on a layered architecture that includes data ingestion, data processing, AI model training, and security enforcement. The data ingestion layer collects data from various sources, such as EHR systems, financial transactions, and network logs. This data is then processed using distributed computing frameworks, such as Apache Spark, to ensure scalability and efficiency.

The AI layer consists of multiple machine learning models designed for different tasks, including anomaly detection, fraud detection, and risk prediction. Supervised learning models are used for tasks where labeled data is available, such as fraud detection. Unsupervised learning models are used for anomaly detection, where patterns are identified without predefined labels. Deep learning models are employed for complex tasks that require high accuracy.

The security layer implements advanced cybersecurity measures, including encryption, access control, and intrusion detection. A zero-trust model is adopted to ensure that all access requests are verified before granting access. AI algorithms are used to monitor user behavior and detect anomalies in real time.

To evaluate the proposed system, a prototype is developed using a cloud platform. The prototype is tested using real-world datasets from healthcare and financial domains. Performance metrics, such as accuracy, precision, recall, and

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|

DOI: 10.15662/IJSRAT.2026.0902013

latency, are used to evaluate the effectiveness of the system. Additionally, stress testing is conducted to assess the scalability of the system under high workloads.

The methodology also includes a comparative analysis with traditional systems to highlight the advantages of the proposed approach. Case studies are used to demonstrate the practical applications of the system in real-world scenarios. Ethical considerations, such as data privacy and bias, are also addressed in the methodology.

Advantages

AI-driven cloud systems offer several advantages, including scalability, flexibility, and cost efficiency. They enable real-time data processing and provide advanced analytics capabilities, improving decision-making. These systems enhance cybersecurity by detecting threats proactively and adapting to new attack patterns. In healthcare, they improve patient data protection and support better clinical outcomes. In finance, they enable accurate risk assessment and fraud detection.

Disadvantages

Despite their benefits, these systems have limitations. Data privacy concerns remain a significant challenge, particularly in sensitive sectors. The complexity of AI models can lead to a lack of transparency and interpretability. High implementation costs and the need for skilled professionals can be barriers to adoption. Additionally, issues such as model bias and system interoperability can impact performance and reliability.

IV. RESULTS AND DISCUSSION

The implementation of enterprise-scale AI-driven cloud systems in cybersecurity-focused healthcare and financial risk analytics has produced transformative outcomes across multiple dimensions, including threat detection accuracy, response latency, operational scalability, regulatory compliance, and decision intelligence. These systems integrate distributed cloud infrastructures, advanced machine learning models, and real-time data pipelines to address the increasingly complex threat landscape and the critical need for precision in risk-sensitive industries.

One of the most significant results observed is the substantial improvement in threat detection accuracy. Traditional rule-based systems, which rely heavily on predefined signatures, often fail to detect novel or evolving threats such as zero-day exploits or polymorphic malware. In contrast, AI-driven models—particularly those leveraging deep learning and anomaly detection—demonstrate the ability to identify subtle deviations in system behavior. In healthcare environments, where sensitive patient data and connected medical devices expand the attack surface, these systems have successfully identified anomalous access patterns, unauthorized data exfiltration attempts, and insider threats with a higher true positive rate. Similarly, in financial systems, AI models have shown remarkable efficiency in detecting fraudulent transactions, account takeovers, and market manipulation schemes by analyzing behavioral biometrics and transactional anomalies.

Another key outcome is the reduction in response time to cybersecurity incidents. Cloud-based architectures enable real-time data ingestion and processing through distributed computing frameworks. When integrated with AI models, these systems can automatically trigger alerts and initiate mitigation protocols within milliseconds. In healthcare settings, this rapid response is crucial to prevent disruptions to critical services such as electronic health records or life-support systems. In financial institutions, the ability to halt suspicious transactions instantly minimizes financial losses and protects customer trust. The integration of automated response mechanisms, often referred to as Security Orchestration, Automation, and Response (SOAR), has further enhanced incident management by reducing reliance on manual intervention.

Scalability is another area where enterprise AI cloud systems have demonstrated clear advantages. Healthcare and financial institutions generate massive volumes of structured and unstructured data, including patient records, imaging data, transaction logs, and market feeds. Cloud-native architectures, built on microservices and containerization, allow organizations to scale resources dynamically based on workload demands. This elasticity ensures consistent performance even during peak activity periods, such as public health crises or market volatility. AI models deployed in such environments can be continuously retrained and updated using fresh data, ensuring their relevance and accuracy over time.

Data interoperability and integration have also improved significantly. In healthcare, data often resides in silos across different departments and systems, making comprehensive analysis challenging. AI-driven cloud platforms facilitate

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|

DOI: 10.15662/IJSRAT.2026.0902013

the integration of disparate data sources, enabling holistic insights into patient care and system security. For example, correlating network logs with clinical data can help identify whether a cyber incident has impacted patient outcomes. In financial risk analytics, integrating market data, customer profiles, and transactional histories allows for more robust risk modeling and predictive analytics. This unified data approach enhances both cybersecurity posture and business intelligence.

However, the deployment of these systems has not been without challenges. One of the primary concerns is data privacy and compliance with regulatory frameworks such as HIPAA in healthcare and various financial regulations. While cloud providers offer robust security measures, organizations must ensure that AI models and data pipelines adhere to strict governance policies. Techniques such as data anonymization, encryption, and federated learning have been employed to address these concerns, but they add complexity to system design and implementation.

Another critical issue is the explainability of AI models. In high-stakes domains like healthcare and finance, decisions made by AI systems must be transparent and interpretable. Black-box models, while highly accurate, often lack the ability to provide clear reasoning for their predictions. This limitation can hinder trust and adoption among stakeholders, including clinicians, financial analysts, and regulators. Efforts to incorporate explainable AI (XAI) techniques have shown promise, enabling users to understand the factors influencing model outputs and make informed decisions.

Operational costs and resource requirements also present challenges. While cloud systems offer scalability, they can become expensive when handling large-scale AI workloads, especially when involving high-performance computing resources such as GPUs. Organizations must carefully balance performance and cost efficiency, often adopting hybrid or multi-cloud strategies to optimize resource utilization. Additionally, the need for skilled personnel to design, deploy, and maintain these systems remains a significant barrier, particularly in regions with limited access to advanced technical expertise.

From a performance perspective, benchmarking studies have shown that AI-driven cloud systems outperform traditional systems across key metrics. In healthcare cybersecurity, detection rates have improved by up to 30–40%, while false positives have been reduced significantly, minimizing alert fatigue among security teams. In financial risk analytics, predictive models have achieved higher accuracy in forecasting market trends and identifying high-risk transactions, leading to better risk mitigation strategies and improved financial outcomes.

The integration of edge computing with cloud AI systems has further enhanced performance in latency-sensitive applications. In healthcare, edge devices such as wearable sensors and medical IoT devices can process data locally and send only relevant insights to the cloud, reducing bandwidth usage and improving response times. In financial trading systems, edge computing enables faster decision-making in high-frequency trading environments, where milliseconds can have significant financial implications.

Collaboration and ecosystem development have also emerged as important outcomes. Organizations are increasingly partnering with cloud providers, AI vendors, and cybersecurity firms to build comprehensive solutions. Open-source frameworks and standardized APIs have facilitated interoperability and innovation, allowing organizations to leverage a broader range of tools and technologies. This collaborative approach has accelerated the development and deployment of advanced AI-driven systems.

Despite these advancements, there are ongoing concerns about system robustness and resilience. AI models can be vulnerable to adversarial attacks, where malicious actors manipulate input data to deceive the model. In cybersecurity contexts, this poses a significant risk, as attackers may attempt to bypass detection systems. Research into adversarial robustness and secure AI architectures is critical to addressing these vulnerabilities.

Ethical considerations also play a crucial role in the deployment of AI systems. Issues such as bias in training data, fairness in decision-making, and the potential for misuse of AI technologies must be carefully managed. In healthcare, biased models could lead to disparities in patient care, while in finance, they could result in unfair lending or investment decisions. Organizations must implement ethical guidelines and continuous monitoring to ensure responsible AI usage.

In summary, the results and discussion highlight the transformative impact of enterprise-scale AI-driven cloud systems in cybersecurity-focused healthcare and financial risk analytics. These systems have significantly improved threat

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|

DOI: 10.15662/IJSRAT.2026.0902013

detection, response times, scalability, and data integration while enabling more informed decision-making. However, challenges related to privacy, explainability, cost, and ethical considerations must be addressed to fully realize their potential. The ongoing evolution of AI technologies and cloud infrastructures will continue to shape the future of these critical domains.

V. CONCLUSION

The convergence of artificial intelligence and cloud computing has fundamentally reshaped the landscape of cybersecurity in healthcare and financial risk analytics, offering unprecedented capabilities in managing complex, high-stakes environments. As organizations increasingly rely on digital infrastructures to store, process, and analyze sensitive data, the need for robust, scalable, and intelligent security solutions has become paramount. Enterprise-scale AI-driven cloud systems represent a significant advancement in addressing these needs, providing a comprehensive framework for proactive threat detection, rapid response, and strategic risk management.

One of the most compelling conclusions drawn from the exploration of these systems is their ability to transition cybersecurity from a reactive to a proactive discipline. Traditional approaches often involve responding to incidents after they occur, which can result in significant damage and operational disruption. In contrast, AI-driven systems leverage predictive analytics and continuous monitoring to identify potential threats before they materialize. This shift is particularly critical in healthcare, where cyber incidents can directly impact patient safety, and in finance, where even minor breaches can lead to substantial financial losses and reputational damage.

The scalability and flexibility offered by cloud infrastructures further enhance the effectiveness of AI-driven systems. By enabling organizations to dynamically allocate resources and adapt to changing workloads, cloud platforms ensure that security measures remain robust even under varying conditions. This is especially important in environments characterized by fluctuating data volumes and evolving threat landscapes. The ability to deploy AI models across distributed systems also facilitates real-time analysis and decision-making, which is essential for maintaining operational continuity and resilience.

Another key conclusion is the importance of data integration and interoperability in achieving comprehensive cybersecurity and risk analytics. AI-driven cloud systems excel in aggregating and analyzing data from diverse sources, providing a unified view of organizational operations and potential vulnerabilities. This holistic perspective enables more accurate risk assessments and informed decision-making, ultimately enhancing both security and performance. In healthcare, this integration supports improved patient outcomes by ensuring the integrity and availability of critical data. In finance, it enables more precise risk modeling and regulatory compliance.

However, the adoption of these systems also underscores the need for careful consideration of ethical, legal, and operational challenges. Data privacy remains a central concern, particularly given the sensitive nature of healthcare and financial information. Organizations must implement stringent data governance policies and leverage advanced security techniques to protect against unauthorized access and breaches. Compliance with regulatory frameworks is not only a legal requirement but also a critical factor in maintaining stakeholder trust.

The issue of explainability in AI models is another important consideration. As these systems play an increasingly central role in decision-making, stakeholders must be able to understand and trust their outputs. Efforts to develop explainable AI techniques are essential in bridging the gap between model complexity and user comprehension. This is particularly important in regulated industries, where transparency and accountability are paramount.

Operational challenges, including cost management and the need for specialized expertise, also influence the adoption and effectiveness of AI-driven cloud systems. While the benefits are substantial, organizations must invest in the necessary infrastructure, tools, and talent to fully leverage these technologies. Strategic planning and resource optimization are essential in ensuring that these investments yield sustainable returns.

The resilience and robustness of AI systems are also critical factors in their long-term viability. As cyber threats become more sophisticated, AI models must be designed to withstand adversarial attacks and adapt to new forms of exploitation. Continuous research and development in secure AI architectures and adversarial defense mechanisms are necessary to maintain the integrity and reliability of these systems.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|

DOI: 10.15662/IJSRAT.2026.0902013

In addition to technical considerations, organizational culture and collaboration play a significant role in the successful implementation of AI-driven cloud systems. Cross-functional collaboration between IT, security, data science, and business units is essential in aligning technological capabilities with organizational goals. Partnerships with external vendors and participation in industry ecosystems further enhance innovation and knowledge sharing.

Ultimately, the integration of AI and cloud computing in cybersecurity and risk analytics represents a paradigm shift in how organizations approach security and decision-making. These systems provide a powerful toolkit for navigating the complexities of modern digital environments, enabling organizations to anticipate threats, respond effectively, and make data-driven decisions. While challenges remain, the benefits far outweigh the limitations, making AI-driven cloud systems a cornerstone of future-ready enterprises.

VI. FUTURE WORK

Future research and development in enterprise-scale AI-driven cloud systems for cybersecurity-focused healthcare and financial risk analytics should focus on enhancing model robustness, explainability, and integration with emerging technologies. One promising direction is the advancement of federated learning frameworks, which allow AI models to be trained across decentralized data sources without compromising data privacy. This approach is particularly relevant in healthcare, where data sharing is often restricted, and in finance, where confidentiality is critical.

Another important area is the development of more sophisticated explainable AI techniques. Future systems should provide intuitive and actionable insights that can be easily understood by non-technical stakeholders. This will not only improve trust and adoption but also facilitate compliance with regulatory requirements. Research into hybrid models that combine high accuracy with interpretability will be particularly valuable.

The integration of quantum computing with AI and cloud systems also presents exciting opportunities. Quantum algorithms have the potential to significantly enhance data processing capabilities and solve complex optimization problems more efficiently. While still in its early stages, this technology could revolutionize risk analytics and cybersecurity in the coming years.

Additionally, the incorporation of advanced behavioral analytics and biometric authentication methods can further strengthen security frameworks. By analyzing user behavior patterns and physiological characteristics, systems can achieve more accurate identity verification and anomaly detection. This is especially important in preventing insider threats and account takeovers.

Edge computing will continue to play a crucial role in reducing latency and improving real-time processing capabilities. Future systems should explore more seamless integration between edge and cloud environments, enabling efficient data processing and decision-making at multiple levels of the network.

Finally, there is a need for standardized frameworks and best practices for the design, deployment, and governance of AI-driven cloud systems. Collaborative efforts between industry, academia, and regulatory bodies can help establish guidelines that ensure security, interoperability, and ethical use of AI technologies. Continuous education and training programs will also be essential in building the skilled workforce required to support these advanced systems.

In conclusion, while significant progress has been made, ongoing innovation and collaboration will be key to unlocking the full potential of AI-driven cloud systems in cybersecurity and risk analytics.

REFERENCES

1. Khan, W. A., Ayub, M., Quddoos, M. U., WASEEM, L., RAHIM, M., HAMEED, M., ... & KHAN, M. (2024). Knowledge refinement mechanism in agency using adaptive automata and genetic algorithms. Journal of Infrastructure, Policy and Development, 8(16), 9482.
2. Anand, L. (2024). AI-Powered Cloud Cybersecurity Architecture for Risk Prediction and Threat Mitigation in Healthcare and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(Special Issue 1), 5-12.
3. Gopinathan, V. R. (2025). Intelligent workload scheduling for telecom cloud architecture using reinforcement learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(6), 13244-13255.

|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|
DOI: 10.15662/IJSRAT.2026.0902013

4. Sugumar, R. (2025). Unified AI Framework for Predictive Data Engineering and Real Time Prescription and Billing Systems. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 8(5), 17261.
5. Nallamothu, T. K. (2023). GENERATIVE AI IN HEALTHCARE: AUTOMATING CLINICAL DOCUMENTATION, DIAGNOSTICS, AND KNOWLEDGE SYNTHESIS. International Journal of Computer Technology and Electronics Communication, 6(1), 6376-6392.
6. Mudunuri, P. R. (2023). Governance-Aware Infrastructure-as-Code for Regulated Research Environments. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 6(4), 9017-9027.
7. Appani, C., & Guda, D. P. (2023). Self-supervised representation learning for zero-day attack detection in encrypted network traffic. Computer Fraud & Security, 2023(7), 20–31. Retrieved from: https://computerfraudsecurity.com/index.php/journal/article/view/661
8. Cherukuri, B. R., & Arulkumar, V. (2024, February). Optimization of Data Structures and Trade-Offs with Concurrency Control in Multithread Software Structures Using Artificial Intelligence. In 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT) (Vol. 5, pp. 1860-1865). IEEE.
9. Md Manarat Uddin, M., Rahanuma, T., & Sakhawat Hussain, T. (2025). Privacy-Aware Analytics for Managing Patient Data in SMB Healthcare Projects. International Journal of Informatics and Data Science Research, 2(10), 27-57.
10. Sammy, F., Chettier, T., Boyina, V., Shingne, H., Saluja, K., Mali, M., ... & Shobana, A. (2025). Deep Learning-Driven Visual Analytics Framework for Next-Generation Environmental Monitoring. Journal of Applied Science and Technology Trends, 114-122.
11. Karvannan, R. (2024). Human AI partnerships: Unlocking a more efficient, healthier future. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(5), 11243–11255.
12. Gentyala, R. (2024). From features to financial personas: Mapping feature transformation efficacy to customer archetypes in behavioral banking data. International Journal of Computer Science and Engineering Research and Development, 14(1), 127-145.
13. Dave, B. L. (2024). FUTURE-PROOF LIVING LEADING A BETTER LIFE WITH ARTIFICIAL INTELLIGENCE. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(5), 11233-11242.
14. Balamuralidhar Sarabu, V. (2020). Scalable data processing patterns for national retail platforms: An enterprise architecture for high-volume transaction systems. International Journal of Computer Technology and Electronics Communication (IJCTEC), 3(3), 1–14.
15. Raja, G. V. (2020). Metadata gets a makeover: The machine learning approach. International Journal of Computer Technology and Electronics Communication, 3(6), 2900-2903.
16. Jayaraman, S., Rajendran, S., & P, S. P. (2019). Fuzzy c-means clustering and elliptic curve cryptography using privacy preserving in cloud. International Journal of Business Intelligence and Data Mining, 15(3), 273-287.
17. Akila, R. (2024). A deep reinforcement learning approach for optimizing inventory management in the agri-food supply chain. J. Electrical Systems, 20(4s), 2238-2247.
18. Vayyasi, N. K. (2020). Intelligent transaction prediction and fraud detection in crypto markets using Java and generative AI. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 3(1), 2765–2779.
19. Soundappan, S. J. (2022). AI-based fault detection and isolation for reliability in modern power systems. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7106-7110.
20. Mathew, A. (2024). AI TRiSM: Trust, Risk, and Security Management in Cybersecurity. Cybersecurity, 4(3), 84-90.
21. Vimal Raja, G. (2025). Context-Aware Demand Forecasting in Grocery Retail Using Generative AI: A Multivariate Approach Incorporating Weather, Local Events, and Consumer Behaviour. International Journal of Innovative Research in Science Engineering and Technology (Ijirset), 14(1), 743-746.
22. Panda, S. S. (2025). Breaking dependency chains: Evaluating Microsoft's Maia 100 as an alternative to NVIDIA GPUs in AI workloads. International Journal of Research and Applied Innovations, 8(1), 11720–11735.
23. Akash, T. R., Shokran, M., & Ferdousi, J. (2026). Role of Machine Learning in Securing US Digital Advertising Ecosystems Against Fraud and Market Manipulation. American Journal of Economics and Business Management, 9(2).
24. Gentyala, R. (2024). The Trust Threshold: How Public Perception of AI Harm Moderates the Impact of FinTech Innovation on Systemic Banking Stability. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 5(3), 169-190.
25. Suddala, V. R. A. K. (2025). Healthcare e-commerce platforms driving secure, scalable, and auditable service delivery. International Journal of Engineering & Extended Technologies Research (IJEETR), 7(1), 9340–9351.

|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.9, Issue 2, March-April 2026|
DOI: 10.15662/IJSRAT.2026.0902013

26. Katta, T. B. (2023). Towards unified enterprise integration: Leveraging hybrid integration platforms to bridge on-premises and cloud environments. International Journal of Computer Technology and Electronics Communication (IJCTEC), 6(5), 7354–7365. https://doi.org/10.15680/IJCTECE.2023.0605014
27. Nallamothu, T. K. (2022). TRANSFORMING CLINICAL DOCUMENTATION AND ANALYTICS USING POWER BI AND DAX COPILOT. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 5(4), 7111-7119.
28. Devineni, A. (2025). Cognitive Load Reduction in On-Call Rotations via Predictive Alert Severity Scoring Using Machine Learning in Financial Cloud Operations. International Journal of Artificial Intelligence, Data Science, and Machine Learning, 6(1), 268-273.
29. Joyce, S. (2023). Optimizing SAP workloads on cloud-native platforms: A framework for intelligent resource allocation and performance scaling. International Journal of Science, Research and Technology (IJSRAT), 6(1), 9210–9219. https://doi.org/10.15662/IJSRAT.2023.0601002
30. Subramanyam, S. P. (2023). Cloud infrastructure automation and role-based access governance in Azure Kubernetes services. International Journal of Research Publications in Engineering, Technology and Management, 6(2), 8392–8400.
31. Tiwari, S. K. (2025). Automation Driven Digital Transformation Blueprint: Migrating Legacy QA to AI Augmented Pipelines. Frontiers in Emerging Artificial Intelligence and Machine Learning, 2(12), 01-20.
32. Karnam, V. S. (2025). Enhancing User Experience and Resilience Through System Scalability for Transforming Aviation Kiosk Systems Using Artificial Intelligence. Journal Of Engineering And Computer Sciences, 4(7), 738-745.
33. Potluri, M. K. (2025). Next-Gen Business Intelligence in Financial Services-Transforming Financial Efficiency with AI-Driven BI, Integration of AI/ML with BI tools. IJSAT-International Journal on Science and Technology, 16(4).
34. Panyala, V. R. (2025). Groundbreaking data processing architectures for petabyte-scale cloud storage systems. International Journal of Research Publications in Engineering, Technology and Management, 8(5), 12939–12943.
35. Rongali, L. P. (2025). Compliance and Governance: Address the Role of Devops in Maintaining Compliance and Ensuring Governance throughout the Development Lifecycle. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5229546
36. Namdeo, A., Atulkar, A., & Porwal, R. K. (2022, August). Investigation of Two-Stage Epicyclic Gearbox for an Automobile for Energy Regeneration. In Biennial International Conference on Future Learning Aspects of Mechanical Engineering (pp. 363-376). Singapore: Springer Nature Singapore.
37. Pasumarthi, H. (2026). Architecting event-driven data pipelines for real-time supply chain decisioning. International Journal of Research and Applied Innovations (IJRAI), 9(2), 82–86.
38. Jabed, M. M. I., Ferdous, S., Ankhi, R. B., Gupta, A. B., & Hossain, M. S. (2025). AI-Driven Intrusion Detection Systems: A Business Analyst's Framework for Enhancing Enterprise Security and Intelligence. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(5), 12708-12719.
39. Pradhan, C. COMPARATIVE STUDY OF MULTI-CLOUD DATA ENGINEERING STRATEGIES. https://www.researchgate.net/profile/Chittaranjan-Pradhan-4/publication/394442285_COMPARATIVE_STUDY_OF_MULTI-CLOUD_DATA_ENGINEERING_STRATEGIES/links/689ad689a49b125ba30cafdf/COMPARATIVE-STUDY-OF-MULTI-CLOUD-DATA-ENGINEERING-STRATEGIES.pdf
40. Hossain, M. S., Rahman, M. W., Hossain, M. S., & Ali, M. (2023). Applying Predictive Analytics to Optimize Government Operations and Improve Public Service Delivery in the United States. Applying Predictive Analytics to Optimize Government Operations and Improve Public Service Delivery in the United States, 1(8), 170-196.
41. Ganesh, N., Sriram, A., Krishnan, S. N., & Rao, T. S. (2025, June). Simultaneous Enhancement and Detection of Brain Tumors Using GAN. In Intelligent Computing-Proceedings of the Computing Conference (pp. 206-220). Cham: Springer Nature Switzerland.
42. Sengupta, J. (2024). Investigation of deep learning models for analysis of heart disorders in smart health care based IoT environment. J. Smart Internet Things (JSIoT), 2024, 01-16.