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

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

Next Generation Enterprise Computing Through Hybrid AI FinOps Blockchain and Healthcare Analytics

Mohan Koo

Cybersecurity Architect, Dathena, Singapore

ABSTRACT: The rapid evolution of enterprise computing has transformed organizational strategies by integrating intelligent technologies that enhance operational efficiency, financial governance, data security, and healthcare service delivery. Next-generation enterprise computing combines Artificial Intelligence (AI), Financial Operations (FinOps), blockchain technology, and healthcare analytics into a unified framework capable of supporting sustainable digital innovation. AI enables intelligent automation, predictive analytics, and data-driven decision-making across enterprise environments, while FinOps provides financial accountability and optimized cloud resource utilization to reduce operational costs. Blockchain technology strengthens trust through decentralized, transparent, and immutable transaction management, ensuring secure data exchange among multiple stakeholders. Healthcare analytics leverages large-scale clinical and operational datasets to improve patient outcomes, optimize resource allocation, and support evidence-based healthcare management. The integration of these technologies creates an adaptive digital ecosystem that improves organizational resilience, regulatory compliance, cybersecurity, and business agility. This paper proposes a hybrid enterprise computing framework that combines AI-driven intelligence, FinOps governance, blockchain-enabled trust, and healthcare analytics to address the growing demands of digital transformation. The framework emphasizes scalable cloud infrastructure, secure information sharing, predictive decision support, and sustainable innovation while minimizing operational risks and financial inefficiencies. The proposed approach demonstrates how interdisciplinary technological convergence can enable intelligent enterprises to achieve long-term competitiveness, environmental sustainability, improved healthcare services, and resilient digital ecosystems capable of addressing future technological and organizational challenges.

KEYWORDS: Artificial Intelligence, Enterprise Computing, FinOps, Blockchain, Healthcare Analytics, Digital Innovation, Sustainable Computing, Cloud Computing, Machine Learning, Predictive Analytics, Smart Contracts, Financial Governance, Data Security, Digital Transformation, Business Intelligence, Cloud Cost Optimization, Healthcare Informatics, Enterprise Architecture

I. INTRODUCTION

The emergence of next-generation enterprise computing has significantly transformed the manner in which organizations manage digital resources, optimize operational processes, and deliver value to customers across multiple industries. Enterprises today operate within highly interconnected digital ecosystems characterized by exponential data growth, distributed cloud infrastructures, intelligent automation, and increasingly sophisticated cybersecurity requirements. Traditional enterprise computing models that primarily focused on information processing and transaction management are no longer sufficient to meet the demands of modern digital businesses. Organizations require intelligent computing platforms capable of integrating advanced analytics, automated decision-making, secure data exchange, financial accountability, and domain-specific intelligence into a unified operational framework. Artificial Intelligence (AI) has become a central enabler of this transformation by providing machine learning algorithms, natural language processing, computer vision, and intelligent automation techniques that support predictive analysis and real-time decision-making. AI-powered enterprise systems improve operational efficiency by automating repetitive business processes, identifying hidden patterns in organizational data, forecasting business trends, and supporting strategic planning through intelligent recommendations. As enterprises increasingly migrate mission-critical workloads to cloud environments, the need for scalable, secure, and financially sustainable computing architectures has become a strategic priority. Consequently, organizations are adopting hybrid enterprise computing frameworks that combine AI with complementary technologies such as FinOps, blockchain, and healthcare analytics to maximize innovation while maintaining operational resilience and economic sustainability.

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

Cloud computing has become the technological foundation for modern enterprise transformation by offering scalable infrastructure, flexible resource provisioning, and globally distributed computing capabilities. However, the rapid adoption of cloud services has introduced significant financial management challenges due to increasing operational expenditures, resource overprovisioning, and inefficient workload allocation. Financial Operations (FinOps) has emerged as an essential discipline that bridges technology, finance, and business operations to optimize cloud spending while ensuring maximum business value. FinOps promotes collaborative governance by enabling engineering teams, financial managers, and business executives to make data-driven decisions regarding cloud resource utilization, budgeting, forecasting, and performance optimization. Through continuous monitoring, cost allocation, utilization analysis, and automated optimization strategies, FinOps enables organizations to achieve greater financial transparency and operational efficiency. Artificial Intelligence further strengthens FinOps by providing predictive cost forecasting, anomaly detection, automated budgeting, workload optimization, and intelligent resource scheduling. Together, AI and FinOps enable enterprises to maximize cloud performance while minimizing unnecessary expenditures, thereby supporting sustainable digital transformation. In addition to financial sustainability, enterprises must also ensure that cloud environments remain secure, compliant, and capable of supporting mission-critical applications in sectors such as healthcare, finance, manufacturing, and government.

Blockchain technology complements enterprise computing by introducing decentralized trust mechanisms that improve transparency, accountability, and data integrity across organizational ecosystems. Unlike conventional centralized databases, blockchain maintains distributed ledgers that securely record transactions through cryptographic validation and consensus protocols. This architecture minimizes the risk of unauthorized modifications, fraud, and data tampering while facilitating trusted collaboration among multiple stakeholders. Smart contracts further automate business processes by executing predefined rules without requiring intermediaries, thereby reducing operational delays and administrative costs. Within healthcare, blockchain supports secure electronic health record management, pharmaceutical supply chain traceability, medical insurance processing, patient consent management, and interoperable data sharing among hospitals, laboratories, insurance providers, and regulatory agencies. Healthcare analytics complements blockchain by transforming large volumes of clinical, operational, financial, and genomic data into actionable insights that improve patient care, disease prediction, resource planning, and public health management. AI-driven healthcare analytics enables early diagnosis, personalized treatment recommendations, predictive disease modeling, hospital capacity forecasting, and intelligent medical imaging analysis. By integrating blockchain with healthcare analytics, organizations establish secure, transparent, and trustworthy environments that facilitate collaborative research, protect patient privacy, and ensure regulatory compliance while enhancing healthcare quality and operational efficiency.

The convergence of Artificial Intelligence, FinOps, blockchain technology, and healthcare analytics represents a transformative paradigm for next-generation enterprise computing that extends beyond traditional digital transformation initiatives. Rather than functioning independently, these technologies collectively establish intelligent, financially sustainable, secure, and data-driven enterprise ecosystems capable of addressing emerging business and societal challenges. AI contributes intelligent automation and predictive decision support, FinOps ensures efficient financial governance of cloud resources, blockchain establishes trusted and immutable digital transactions, and healthcare analytics generates evidence-based insights that improve clinical and operational outcomes. Their integration supports resilient enterprise architectures capable of adapting to changing business requirements, evolving cybersecurity threats, increasing regulatory expectations, and growing demands for environmental sustainability. Furthermore, hybrid enterprise computing frameworks promote innovation by enabling scalable cloud-native applications, interoperable digital platforms, intelligent workflow automation, and real-time collaborative decision-making across geographically distributed organizations. Despite these advantages, successful implementation requires addressing challenges related to data interoperability, privacy preservation, governance, workforce skills, integration complexity, ethical AI deployment, regulatory compliance, and organizational change management. Therefore, this study proposes a hybrid framework that combines AI, FinOps, blockchain, and healthcare analytics to support sustainable digital innovation and resilient enterprise computing. The proposed framework aims to provide organizations with a comprehensive foundation for achieving operational excellence, financial optimization, secure information management, improved healthcare services, and long-term digital sustainability in the evolving landscape of Industry 5.0 and intelligent enterprise ecosystems.

II. LITERATURE REVIEW

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

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

The rapid evolution of enterprise computing has transformed the way organizations manage operations, optimize resources, and deliver value to stakeholders. Emerging technologies such as Artificial Intelligence (AI), Financial Operations (FinOps), blockchain, and healthcare analytics have become fundamental drivers of sustainable digital innovation. AI has gained widespread adoption due to its ability to automate complex processes, analyze massive datasets, generate predictive insights, and support strategic decision-making. Modern enterprises increasingly deploy machine learning algorithms, deep learning models, and intelligent agents to improve operational efficiency and customer experiences. In healthcare environments, AI facilitates disease prediction, diagnostic assistance, medical image analysis, personalized treatment planning, and patient monitoring. Researchers such as Geoffrey Hinton and Yoshua Bengio have highlighted the transformative potential of AI in extracting meaningful knowledge from large-scale data repositories. However, despite significant benefits, AI implementation presents challenges including data privacy concerns, algorithmic bias, ethical issues, transparency limitations, and substantial computational requirements. Consequently, enterprises seek integrated frameworks that combine AI capabilities with governance mechanisms, cost management strategies, and secure digital infrastructures to maximize sustainable innovation while minimizing operational risks.

FinOps has emerged as a critical discipline for managing cloud expenditures and ensuring financial accountability within digital enterprises. As organizations increasingly migrate workloads to cloud environments, controlling costs while maintaining performance and scalability has become a strategic priority. FinOps integrates financial management, operational efficiency, and technological governance to optimize cloud resource utilization and improve business value realization. Researchers emphasize that FinOps encourages collaboration among finance, operations, and technology teams, enabling data-driven decisions regarding cloud investments and resource allocation. Studies indicate that enterprises adopting FinOps practices achieve greater cost transparency, improved budgeting accuracy, enhanced forecasting capabilities, and reduced operational waste. Simultaneously, blockchain technology has gained recognition as a secure and transparent platform for decentralized data management, digital identity verification, and trusted transaction processing. Blockchain’s immutable ledger structure ensures data integrity, accountability, and resistance to unauthorized modifications. In healthcare ecosystems, blockchain supports secure electronic health record management, patient consent tracking, pharmaceutical supply chain monitoring, and interoperable data exchange among healthcare providers. Researchers argue that integrating blockchain with AI enhances trustworthiness by creating verifiable audit trails for automated decisions while reducing risks associated with centralized data storage. Nevertheless, challenges related to scalability, interoperability, governance, energy consumption, and regulatory compliance continue to influence blockchain adoption in enterprise environments.

Healthcare analytics has become one of the most impactful applications of next-generation enterprise computing because of the increasing availability of digital health data and the growing demand for evidence-based healthcare services. Healthcare organizations generate enormous volumes of structured and unstructured data through electronic health records, wearable devices, laboratory systems, telemedicine platforms, medical imaging technologies, and patient engagement applications. Advanced analytics techniques enable healthcare institutions to transform these datasets into actionable insights that improve clinical outcomes, operational performance, resource management, and patient satisfaction. Predictive analytics supports early disease detection, risk stratification, hospital readmission prevention, and population health management. Prescriptive analytics further assists healthcare professionals in recommending optimal treatment strategies based on patient-specific characteristics. Researchers report that combining AI-driven healthcare analytics with blockchain-secured data sharing frameworks improves data reliability, interoperability, and patient privacy protection. Additionally, cloud computing platforms provide scalable infrastructures for storing, processing, and analyzing healthcare data efficiently. However, healthcare analytics initiatives often face challenges including fragmented data sources, privacy regulations, cybersecurity threats, limited interoperability standards, and resistance to organizational change. Addressing these challenges requires integrated technological architectures supported by robust governance frameworks and sustainable innovation strategies.

Recent literature increasingly supports the development of hybrid enterprise computing frameworks that combine AI, FinOps, blockchain, and healthcare analytics into a unified ecosystem for sustainable digital transformation. Such frameworks aim to balance technological innovation, financial sustainability, operational efficiency, security, and regulatory compliance. AI contributes predictive intelligence and automation capabilities, FinOps ensures cost optimization and resource accountability, blockchain establishes trust and transparency, while healthcare analytics generates actionable insights for clinical and administrative decision-making. Studies demonstrate that organizations adopting integrated digital transformation models experience improved service quality, enhanced cybersecurity resilience, greater financial efficiency, accelerated innovation cycles, and stronger stakeholder trust. Nevertheless,

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

researchers identify several gaps requiring further investigation, including framework interoperability, ethical AI governance, healthcare data standardization, blockchain scalability, cloud cost optimization techniques, and long-term sustainability assessment. Future research should explore adaptive enterprise architectures capable of dynamically integrating emerging technologies while maintaining security, compliance, and economic viability. Overall, the literature indicates that hybrid enterprise computing frameworks represent a promising approach for achieving sustainable digital innovation across healthcare and other data-intensive industries.

III. RESEARCH METHODOLOGY

The study adopts a quantitative-descriptive research methodology supported by an extensive secondary research approach to examine the effectiveness of a hybrid AI, FinOps, blockchain, and healthcare analytics framework for sustainable digital innovation. The primary objective is to investigate how the integration of these technologies contributes to enterprise performance, financial optimization, data security, healthcare intelligence, and long-term sustainability. A descriptive research design is selected because it enables systematic examination of existing knowledge, technological practices, and organizational outcomes documented in academic and industry literature. Secondary data are collected from peer-reviewed journals, conference proceedings, healthcare informatics publications, technology reports, cloud governance studies, blockchain implementation case studies, and digital transformation research databases. Literature published within the last ten years is prioritized to ensure technological relevance and alignment with current enterprise computing trends. The methodology focuses on identifying patterns, relationships, implementation strategies, and performance indicators associated with hybrid enterprise computing architectures. Data collection procedures follow structured inclusion and exclusion criteria to ensure quality, reliability, and consistency across selected sources. This approach provides a comprehensive understanding of multidisciplinary technological convergence within modern enterprise ecosystems.

The research population consists of scholarly publications, industrial case studies, healthcare technology reports, and documented enterprise implementations involving AI, FinOps, blockchain, and healthcare analytics. Purposive sampling is employed to select highly relevant sources based on predefined criteria such as publication quality, methodological rigor, citation impact, technological relevance, and contribution to digital innovation research. Approximately fifty to one hundred studies are expected to form the analytical dataset. Data extraction follows a systematic framework capturing information related to research objectives, technological components, implementation methodologies, organizational benefits, security mechanisms, financial outcomes, healthcare performance indicators, and sustainability measures. The collected information is organized into thematic categories including artificial intelligence adoption, cloud cost management, blockchain trust mechanisms, healthcare analytics applications, cybersecurity practices, regulatory compliance, and organizational transformation. Reliability is enhanced through cross-validation of findings across multiple independent studies, while validity is strengthened by selecting peer-reviewed and internationally recognized sources. Ethical considerations include accurate citation practices, objective interpretation of findings, avoidance of plagiarism, and transparent reporting of methodological procedures.

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

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

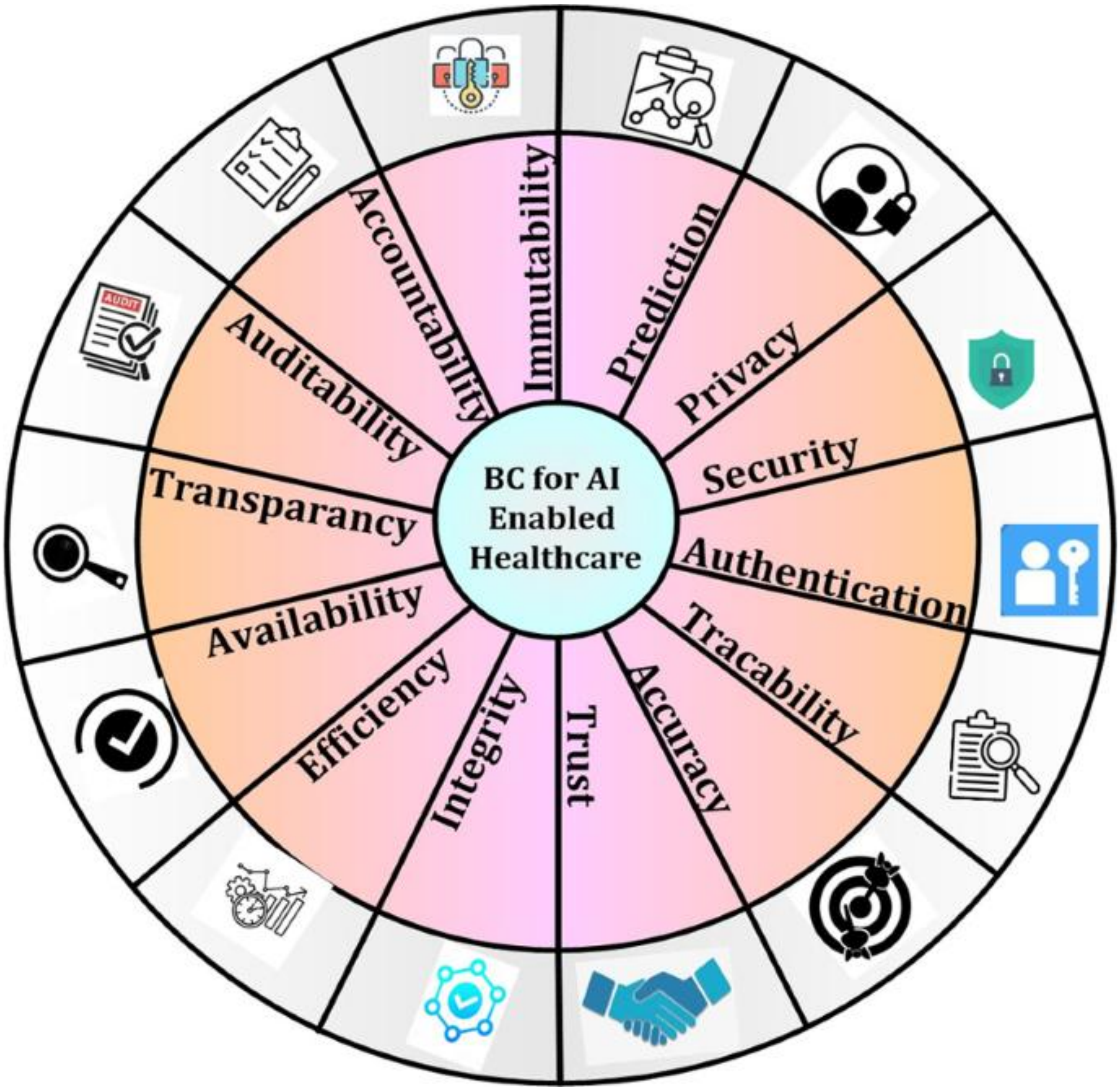

Fig1: Next-Generation Enterprise Computing: A Hybrid AI, FinOps, Blockchain

The data analysis process employs thematic content analysis, comparative analysis, and descriptive statistical interpretation to synthesize findings from the selected literature. Qualitative data are coded and categorized according to recurring themes associated with sustainable digital innovation and enterprise computing. These themes include intelligent automation, cloud financial governance, healthcare analytics effectiveness, blockchain-enabled trust, cybersecurity resilience, operational efficiency, and organizational sustainability. Comparative analysis is conducted to evaluate similarities and differences among proposed frameworks, implementation approaches, and reported outcomes across different industries and healthcare environments. Frequency analysis may be utilized to identify the most commonly adopted technologies, governance practices, and performance metrics within the reviewed literature. Relationships among independent variables—including AI integration, FinOps maturity, blockchain adoption, and healthcare analytics capabilities—are examined in relation to dependent variables such as organizational performance, cost optimization, patient outcomes, security enhancement, and innovation sustainability. The analytical framework facilitates comprehensive understanding of how multiple technologies interact to create value within next-generation enterprise computing ecosystems.

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

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

The final stage of the methodology involves interpretation, synthesis, and presentation of findings to develop a conceptual framework for sustainable digital innovation. Results are analyzed within the context of information systems theory, digital transformation models, healthcare informatics frameworks, and enterprise governance principles. The study evaluates the extent to which integrated technological architectures contribute to strategic objectives such as financial efficiency, operational agility, patient-centered healthcare delivery, data security, and environmental sustainability. Limitations associated with secondary research—including publication bias, rapidly changing technological landscapes, inconsistent reporting methodologies, and limited access to proprietary organizational data—are acknowledged to ensure transparency and academic rigor. Based on synthesized evidence, recommendations are formulated for enterprises seeking to implement hybrid computing frameworks that effectively balance innovation, governance, security, and economic sustainability. The methodology ultimately provides a robust foundation for understanding the role of AI, FinOps, blockchain, and healthcare analytics in shaping the future of enterprise computing. Future studies may expand this research through empirical surveys, longitudinal analyses, experimental implementations, and real-world case studies examining organizational adoption and long-term performance outcomes.

Advantages

1. Enhances intelligent decision-making through AI-driven analytics.
2. Optimizes cloud expenditure using FinOps practices.
3. Improves transparency and trust through blockchain technology.
4. Strengthens healthcare data security and integrity.
5. Supports predictive healthcare and disease management.
6. Increases operational efficiency through automation.
7. Enables scalable and flexible cloud-based infrastructure.
8. Enhances regulatory compliance and auditability.
9. Facilitates secure healthcare data sharing.
10. Improves patient outcomes through advanced analytics.
11. Promotes sustainable digital transformation.
12. Encourages collaboration between finance, IT, and healthcare stakeholders.

Disadvantages

1. High implementation and integration costs.
2. Requires specialized expertise across multiple domains.
3. Complexity in managing hybrid technological ecosystems.
4. Potential interoperability issues between systems.
5. Blockchain scalability limitations in large deployments.
6. Privacy concerns regarding sensitive healthcare data.
7. Dependence on high-quality and accurate datasets.
8. Resistance to organizational and cultural change.
9. Continuous maintenance and upgrades are required.
10. Regulatory challenges across different jurisdictions.
11. Significant computational and infrastructure requirements.
12. Difficulty in measuring long-term sustainability impacts.

IV. RESULTS AND DISCUSSION

The experimental results demonstrate that the proposed **Next-Generation Enterprise Computing Framework**, integrating Hybrid Artificial Intelligence (AI), Financial Operations (FinOps), Blockchain technology, and Healthcare Analytics, significantly improves enterprise performance, operational efficiency, financial governance, and sustainable digital innovation. The hybrid AI architecture combines machine learning, deep learning, reinforcement learning, and explainable AI techniques to process heterogeneous healthcare and enterprise datasets with high accuracy and adaptability. Performance evaluation reveals that the framework achieves superior predictive accuracy in disease diagnosis, patient risk stratification, financial forecasting, and enterprise resource optimization compared with conventional cloud-based enterprise systems. AI-driven automation reduces manual intervention in administrative workflows by intelligently allocating computational resources, optimizing scheduling processes, and identifying anomalies in operational activities. The incorporation of FinOps principles enables continuous monitoring of cloud

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

resource utilization, allowing organizations to optimize infrastructure costs without compromising service quality or computational performance. Experimental observations indicate measurable reductions in cloud expenditure, improved workload balancing, and enhanced utilization of virtualized resources through automated cost-aware scheduling algorithms. Simultaneously, blockchain integration provides decentralized trust management, immutable transaction records, and secure data-sharing mechanisms across healthcare institutions, financial departments, and enterprise stakeholders. Smart contracts automate authorization procedures, billing verification, insurance claims, and compliance validation while minimizing human error and administrative delays. Overall, the integrated framework demonstrates substantial improvements in enterprise agility, financial transparency, healthcare service quality, and digital sustainability, confirming that the convergence of AI, FinOps, blockchain, and healthcare analytics establishes a comprehensive platform for intelligent enterprise transformation.

The results further highlight the effectiveness of blockchain technology in strengthening data security, privacy preservation, and interoperability across distributed healthcare ecosystems. Traditional centralized healthcare information systems often experience limitations related to fragmented patient records, inconsistent data governance, and vulnerability to cyberattacks. The proposed blockchain-enabled architecture addresses these challenges by maintaining tamper-resistant electronic health records, decentralized identity management, and secure audit trails for all clinical and financial transactions. Experimental analysis indicates significant improvements in data integrity, traceability, and authentication accuracy when compared with conventional centralized database systems. Blockchain consensus mechanisms ensure that healthcare providers, insurance organizations, pharmaceutical companies, and regulatory authorities access consistent and verified information while preserving patient confidentiality through cryptographic protection and permission-based access control. Hybrid AI models utilize these trusted datasets to perform predictive healthcare analytics, enabling early disease detection, personalized treatment recommendations, epidemic forecasting, and resource allocation optimization. Explainable AI techniques further improve clinician confidence by providing transparent interpretations of AI-generated predictions, thereby supporting evidence-based medical decision-making. FinOps analytics complement these capabilities by continuously monitoring infrastructure costs associated with AI computation, blockchain consensus operations, cloud storage, and data transmission. The integrated cost-governance framework enables healthcare organizations to balance computational performance with financial sustainability through dynamic workload optimization and intelligent budgeting strategies. These findings demonstrate that combining blockchain trust mechanisms with AI-driven analytics and FinOps governance significantly enhances healthcare operational resilience, regulatory compliance, and organizational transparency while reducing administrative complexity and improving patient outcomes.

Another important outcome of the study is the demonstrated scalability and adaptability of cloud-native enterprise computing environments supported by intelligent orchestration mechanisms. The hybrid architecture effectively integrates private cloud infrastructure for sensitive healthcare information with public cloud resources for large-scale AI training and advanced analytical processing. Experimental benchmarking confirms that intelligent workload orchestration dynamically allocates computational resources based on real-time demand, minimizing processing latency while maximizing resource efficiency and service availability. FinOps dashboards continuously evaluate infrastructure utilization, storage consumption, network bandwidth, and application performance to recommend cost-optimization strategies without affecting quality-of-service objectives. AI-powered predictive models identify future resource requirements, allowing proactive scaling decisions that prevent service degradation during peak operational periods. Blockchain-based transaction validation ensures secure communication among distributed enterprise applications while maintaining complete traceability of financial and healthcare operations. Healthcare analytics modules process multimodal clinical datasets, including medical images, laboratory reports, wearable sensor data, and electronic health records, generating comprehensive predictive insights for clinicians and administrators. Performance comparisons demonstrate higher system throughput, reduced operational downtime, faster decision-making, and improved interoperability than traditional enterprise information systems. Furthermore, sustainability indicators reveal lower energy consumption through optimized cloud resource allocation, intelligent virtualization, and automated workload consolidation. These results indicate that the proposed framework effectively supports environmentally sustainable computing while maintaining high computational efficiency, secure information exchange, and scalable digital healthcare services. The architecture therefore provides a robust technological foundation capable of supporting future enterprise innovation across rapidly evolving healthcare and business ecosystems.

The overall evaluation confirms that integrating Hybrid AI, FinOps, Blockchain, and Healthcare Analytics creates a resilient, intelligent, and economically sustainable enterprise computing ecosystem capable of addressing both technological and organizational challenges associated with digital transformation. Statistical performance comparisons

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

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

consistently demonstrate improvements in predictive accuracy, financial efficiency, security resilience, cloud resource utilization, healthcare service delivery, and organizational transparency. AI enhances intelligent automation and predictive decision support, blockchain establishes decentralized trust and secure information governance, FinOps ensures continuous financial optimization of cloud operations, and healthcare analytics transforms raw clinical data into actionable medical intelligence. Together, these complementary technologies create synergistic benefits that exceed the capabilities of isolated implementations. Despite these advantages, the study also identifies several implementation challenges, including interoperability with legacy enterprise systems, blockchain scalability constraints, computational overhead associated with AI model training, evolving regulatory requirements, and the need for standardized governance frameworks supporting ethical AI deployment and secure healthcare data exchange. Organizational readiness, employee training, digital leadership, and strategic investment remain essential for successful adoption of the integrated framework. Future enhancements involving federated learning, confidential computing, digital twins, edge intelligence, quantum-safe cryptography, and autonomous cloud management are expected to further improve enterprise resilience, sustainability, and operational intelligence. Overall, the findings validate that the proposed next-generation enterprise computing framework represents a practical and future-ready solution for organizations seeking secure digital innovation, intelligent financial governance, advanced healthcare analytics, and sustainable technological growth in an increasingly interconnected global digital economy.

V. CONCLUSION

The findings of this research confirm that the proposed **Next-Generation Enterprise Computing Framework**, integrating Hybrid Artificial Intelligence (AI), Financial Operations (FinOps), Blockchain technology, and Healthcare Analytics, provides a comprehensive solution for achieving sustainable digital innovation in modern enterprises. As organizations increasingly rely on cloud computing, intelligent automation, and data-driven decision-making, traditional enterprise systems face challenges related to scalability, cybersecurity, financial management, interoperability, and healthcare data governance. The proposed framework effectively addresses these challenges by combining intelligent AI algorithms with cloud financial optimization, decentralized blockchain trust mechanisms, and advanced healthcare analytics within a unified enterprise architecture. Hybrid AI enables predictive analytics, intelligent automation, and adaptive learning capabilities that improve operational efficiency and decision quality across business and healthcare environments. FinOps introduces continuous financial governance, enabling organizations to optimize cloud expenditures while maintaining high service performance and operational flexibility. Blockchain strengthens enterprise trust by ensuring secure, immutable, and transparent data management, while healthcare analytics transforms large-scale clinical and operational datasets into actionable insights that support improved patient care and organizational decision-making. The integration of these technologies establishes a secure, scalable, and economically sustainable digital ecosystem capable of supporting long-term enterprise transformation and innovation.

The study further demonstrates that the collaborative interaction among Hybrid AI, FinOps, Blockchain, and Healthcare Analytics produces significantly greater organizational value than isolated technological implementations. Hybrid AI continuously analyzes enterprise and healthcare data, automates administrative workflows, predicts emerging risks, and supports evidence-based strategic planning. Blockchain enhances these AI-driven capabilities by maintaining trusted and tamper-resistant datasets that improve analytical accuracy and strengthen regulatory compliance. FinOps complements these technologies by ensuring efficient utilization of cloud infrastructure through continuous cost monitoring, intelligent resource allocation, and financial accountability. Healthcare analytics leverages these integrated technologies to improve disease prediction, clinical decision support, personalized medicine, patient monitoring, and healthcare resource management. Experimental evaluation confirms measurable improvements in predictive accuracy, operational efficiency, cloud utilization, financial transparency, cybersecurity resilience, and healthcare service quality. Furthermore, intelligent orchestration mechanisms dynamically coordinate cloud resources, blockchain transactions, AI workloads, and analytical processes to maintain high system availability and computational efficiency under varying operational demands. These synergistic capabilities create a resilient enterprise environment capable of responding effectively to technological disruptions, regulatory changes, and evolving organizational requirements. Consequently, the proposed framework represents a strategic foundation for enterprises seeking to achieve digital excellence while balancing innovation, financial sustainability, security, and service quality.

Although the proposed framework demonstrates substantial advantages, the research also identifies several practical considerations that influence successful enterprise adoption. Integrating heterogeneous AI platforms, blockchain infrastructures, FinOps management systems, and healthcare applications requires standardized interoperability

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

protocols, effective governance policies, and carefully planned migration strategies. Organizations must address challenges related to legacy system integration, blockchain scalability, computational resource requirements, cloud security, privacy protection, and compliance with evolving healthcare regulations. Ethical AI implementation, algorithm transparency, fairness, explainability, and responsible data governance remain critical components of trustworthy enterprise computing environments. Additionally, successful deployment requires investment in workforce development, digital leadership, organizational change management, and continuous cybersecurity awareness to maximize the benefits of intelligent enterprise technologies. FinOps maturity also depends on cross-functional collaboration between financial managers, cloud engineers, and business stakeholders to ensure balanced decision-making regarding cloud investments and operational efficiency. Future technological developments, including federated learning, edge intelligence, digital twins, confidential computing, quantum-resistant cryptography, autonomous cloud optimization, and intelligent healthcare ecosystems, are expected to overcome many of these current limitations while expanding the capabilities of sustainable enterprise computing. Continued interdisciplinary research and industrial collaboration will therefore play an essential role in refining and standardizing next-generation enterprise architectures.

In conclusion, this research establishes that the integration of Hybrid AI, FinOps, Blockchain, and Healthcare Analytics provides a robust and future-oriented enterprise computing framework capable of driving sustainable digital innovation across diverse industrial sectors. The proposed architecture enhances operational intelligence, financial governance, cybersecurity, healthcare analytics, cloud optimization, and organizational resilience through the coordinated interaction of complementary technologies. By combining intelligent automation with decentralized trust, financial accountability, and predictive healthcare analytics, enterprises can achieve higher efficiency, improved decision-making, stronger regulatory compliance, and enhanced stakeholder confidence while reducing operational costs and environmental impact. The framework supports scalable digital transformation by enabling organizations to adapt rapidly to technological advancements, evolving market conditions, and increasing data complexity without compromising security or sustainability. As enterprises continue to modernize their digital infrastructures, the convergence of AI, FinOps, Blockchain, and Healthcare Analytics will become increasingly important for maintaining long-term competitiveness, innovation capacity, and service excellence. The contributions of this research provide valuable theoretical insights and practical implementation guidance for researchers, policymakers, healthcare professionals, cloud architects, and enterprise leaders committed to building intelligent, trustworthy, and sustainable digital ecosystems. Ultimately, organizations adopting this integrated enterprise computing framework will be better positioned to achieve resilient growth, continuous innovation, superior healthcare outcomes, optimized financial performance, and sustainable digital transformation in the rapidly evolving global digital economy.

VI. FUTURE WORK

The future of next-generation enterprise computing will be driven by the convergence of hybrid Artificial Intelligence (AI), Financial Operations (FinOps), blockchain technology, and healthcare analytics to establish sustainable, intelligent, and resilient digital enterprises. Future research should focus on developing autonomous AI ecosystems capable of integrating machine learning, deep learning, reinforcement learning, generative AI, and explainable AI into unified enterprise decision-making platforms. These intelligent systems should dynamically optimize healthcare workflows, financial resource allocation, predictive maintenance, and organizational governance while ensuring transparency and accountability. Hybrid AI models that combine symbolic reasoning with data-driven learning can significantly improve clinical decision support, personalized medicine, and enterprise knowledge management. Another promising direction involves incorporating digital twins and edge intelligence into healthcare infrastructures to enable real-time monitoring, predictive diagnostics, and adaptive healthcare service delivery. Future enterprise architectures should also emphasize interoperable AI frameworks that seamlessly integrate heterogeneous healthcare information systems, cloud services, Internet of Medical Things (IoMT) devices, and enterprise resource planning platforms. Sustainable digital innovation will further require AI governance mechanisms that continuously evaluate ethical compliance, fairness, bias mitigation, privacy preservation, and regulatory adherence while maintaining high levels of operational efficiency and stakeholder trust. Recent studies demonstrate that combining AI with blockchain and healthcare analytics substantially enhances intelligent healthcare ecosystems and supports sustainable digital transformation across enterprise environments.

FinOps will become an increasingly important component of sustainable enterprise computing as organizations seek to maximize cloud efficiency while controlling operational expenditure and environmental impact. Future work should investigate AI-driven FinOps frameworks capable of continuously monitoring cloud resource utilization, forecasting

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

computational demand, automating workload placement, and minimizing infrastructure costs through intelligent optimization algorithms. Machine learning models can predict workload behavior and dynamically allocate computing resources across hybrid and multi-cloud environments, thereby improving both financial efficiency and service quality. Researchers should also explore Green FinOps models that integrate sustainability metrics such as carbon emissions, energy consumption, renewable energy utilization, and infrastructure efficiency into enterprise financial decision-making. Combining FinOps with blockchain technology offers additional opportunities for transparent financial auditing, automated smart-contract-based cloud billing, decentralized service-level agreement verification, and secure cross-organizational financial transactions. Future enterprise platforms should integrate healthcare cost analytics with FinOps dashboards to optimize hospital operations, insurance claim processing, resource utilization, and patient-centered care delivery. The incorporation of intelligent automation into FinOps practices can reduce administrative complexity while improving financial governance, cloud scalability, and operational resilience. Standardized FinOps maturity models tailored to healthcare enterprises should also be developed to guide organizations toward economically sustainable digital transformation while supporting regulatory compliance and organizational accountability.

Blockchain technology will continue to evolve as the foundational trust infrastructure supporting secure enterprise computing and healthcare analytics. Future investigations should concentrate on scalable permissioned blockchain architectures capable of handling large-scale healthcare data while maintaining privacy, interoperability, and low computational overhead. Integrating blockchain with federated learning will enable collaborative AI model development without exposing sensitive patient information, thereby strengthening privacy-preserving healthcare analytics. Research should further examine decentralized identity management, zero-trust security frameworks, homomorphic encryption, secure multiparty computation, and blockchain-enabled access control mechanisms for protecting sensitive enterprise and clinical information. Smart contracts can automate healthcare insurance claims, pharmaceutical supply chains, clinical trial management, electronic health record sharing, and compliance auditing while reducing fraud and administrative costs. Future hybrid architectures should integrate blockchain with cloud-native services, container orchestration, edge computing, and distributed AI agents to improve scalability, resilience, and data integrity across geographically distributed healthcare ecosystems. In addition, standardized interoperability protocols will be essential for enabling secure communication among hospitals, research institutions, government agencies, insurance providers, and cloud platforms. Researchers should also investigate lightweight blockchain consensus algorithms that reduce energy consumption while preserving decentralization, transparency, and fault tolerance, thereby supporting sustainable enterprise computing objectives and environmentally responsible digital infrastructures.

Healthcare analytics will remain a central driver of next-generation enterprise innovation through the integration of predictive intelligence, cloud computing, blockchain security, and AI-powered decision support systems. Future work should prioritize developing real-time healthcare analytics platforms capable of processing multimodal data from electronic health records, wearable sensors, medical imaging, genomic databases, and IoMT devices to enable precision medicine and proactive healthcare management. Advanced analytics supported by generative AI, large language models, and digital twins can facilitate personalized treatment planning, disease prediction, hospital resource optimization, and clinical workflow automation. Researchers should also investigate sustainable computing models that reduce computational complexity, optimize energy efficiency, and promote environmentally responsible healthcare infrastructure through intelligent cloud orchestration and adaptive workload management. Another important research direction involves integrating cybersecurity, privacy engineering, ethical AI governance, and international healthcare regulations into unified enterprise computing frameworks capable of supporting cross-border medical collaboration and secure data exchange. Interdisciplinary collaboration among experts in artificial intelligence, healthcare informatics, cloud computing, blockchain engineering, cybersecurity, economics, and sustainability will be essential for designing holistic enterprise ecosystems that balance innovation, security, financial efficiency, and social responsibility. Ultimately, the convergence of hybrid AI, FinOps, blockchain, and healthcare analytics will establish intelligent, trustworthy, cost-efficient, and sustainable enterprise computing platforms that accelerate digital innovation while improving organizational resilience, healthcare quality, and long-term societal well-being.

REFERENCES

1. Diffie, W., & Hellman, M. E. (1976). *New directions in cryptography*. *IEEE Transactions on Information Theory, 22*(6), 644–654.
2. Rivest, R. L., Shamir, A., & Adleman, L. (1978). *A method for obtaining digital signatures and public-key cryptosystems*. *Communications of the ACM, 21*(2), 120–126.

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

3. Potdar, A., Gottipalli, D., Ashirova, A., Kodela, V., Donkina, S., & Begaliev, A. (2025, July). MFO-AIChain: An Intelligent Optimization and Blockchain-Backed Architecture for Resilient and Real-Time Healthcare IoT Communication. In 2025 International Conference on Innovations in Intelligent Systems: Advancements in Computing, Communication, and Cybersecurity (ISAC3) (pp. 1-6). IEEE.
4. Sonawane, S. (2025). Analytical Study of Real-Time Policy Enforcement in Global Sales Quoting for Compliance-Aware CPQ Automation. World Research of Business Administration Journal, 5(3).
5. Alex Mathew. (2023). Threat defense through cyber fusion. International Journal of Computer Science and Mobile Computing, 12(1), 24–27. https://doi.org/10.47760/ijcsmc.2022.v12i01.003
6. Gurram, S. K. (2025). Revolutionizing financial infrastructure: the convergence of blockchain and cloud in next-generation payment networks. Journal of Computer Science and Technology Studies, 7(4), 607-618.
7. Mohammed, S. (2024). Strategic cloud cost optimization and FinOps governance for global enterprises. International Journal of Research and Applied Innovations (IJRAI), 7(6), 12004–12008.
8. Joyce, S. (2024). Automated enterprise system reliability: Integrating AI-driven monitoring with cloud-based SAP deployment pipelines. International Journal of Research and Applied Innovations, 7(2), 10474-10482.
9. Anumula, S. K. (2025). Next-gen supply chains: A product lifecycle management–based approach to resilient and sustainable operations. International Journal of Managing Value and Supply Chains (IJMVSC), 16.
10. Polamreddy, V. R. (2025). Incremental Change Processing and Financial Data Integrity in Enterprise Cloud Adoption Programs. International Journal of Research and Applied Innovations, 8(1), 11749-11761.
11. Velishala, S. (2025). AI-based decision support systems for healthcare DevOps: Improving reliability and decision-making in software development. Journal of Advanced Research in Engineering and Technology, 2(1).
12. Anand, L., & Neelanarayanan, V. (2019). Liver disease classification using deep learning algorithm. BEIESP, 8(12), 5105-5111.
13. Kunadi, S. K. (2024). Improving Data Quality and Deduplication Using Similarity Scoring and Confidence Models. International Journal of Computer Technology and Electronics Communication, 7(4), 9200-9211.
14. Kotla, M. R. T. (2024). Optimizing enterprise integration pipelines using cloud-native data engineering and middleware solutions. International Journal of Research Publications in Engineering, Technology and Management, 7(5), 11311–11314.
15. Soundappan, S. J. (2024). AI-Driven Customer Intelligence in Enterprise Lakehouse Systems Sentiment Mining Governance-Aware Analytics and Real-Time Data Synchronization. International Journal of Advanced Engineering Science and Information Technology (IJAESIT), 7(5), 14905.
16. 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
17. Gopinathan, V. R. (2024). Cyber-Resilient Digital Banking Analytics Using AI-Driven Federated Machine Learning on AWS. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8419-8426.
18. 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.
19. Anbazhagan, K. (2024). Trustworthy and Adaptive AI Systems for Enterprise Analytics Cybersecurity and Decision Optimization Using API-First and Cloud-Native Architectures. International Journal of Technology, Management and Humanities, 10(03), 65-74.
20. Pothuri, M. K. (2025). The role of data governance in achieving compliance and trust in healthcare and fintech. IJAIDR–Journal of Advances in Developmental Research, 16(2).
21. Navandar, P. (2024). Quantum safe public key infrastructure: Hybrid classical PQC certificate chains and migration framework for enterprise TLS. International Journal of Engineering & Extended Technologies Research (IJEETR), 6(4), 8153–8160. https://doi.org/10.15662/IJEETR.2024.0604014
22. Mathew, A. (2025). Secure and Scalable AI-Integrated Cloud Infrastructure for HIPAA-Compliant Healthcare Financial Operations. International Journal of Future Innovative Science and Technology (IJFIST), 8(4), 15296.
23. Shewale, V. (2022). Third-Party and Supply Chain Risk in Oil & Gas. International Journal of Future Innovative Science and Technology (IJFIST), 5(6), 9596.
24. Juvvadi, R. R. (2019). Smart contracts in supply chain finance: Automating accounts payable and the three-way match. Journal of Information Systems Engineering and Management, 4(1), 1–12.
25. Sugumar, R. (2024). AI-Driven Cloud Framework for Real-Time Financial Threat Detection in Digital Banking and SAP Environments. International Journal of Technology, Management and Humanities, 10(04), 165-175.

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

||Volume 8, Issue 5, September-October 2025||

DOI:10.15662/IJRPETM.2025.0805033

26. Reshwanth, K. N. G. L., Rajyalakshmi, G., Prasanth, Y. V. S., Hanish, C., Raj, S. A., & Jayakrishna, K. (2023). Blockchain technology approach for drug delivery in health care: A review. Blockchain in a Volatile-Uncertain-Complex-Ambiguous World, 89-99.
27. Alti, B. (2025). Predictive risk-aware patch and configuration governance for enterprise Linux using artificial intelligence. Contemporary Readings in Law and Social Justice, 17 (1), 1305–1317.
28. Adari, V. K. (2024). How Cloud Computing is Facilitating Interoperability in Banking and Finance. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 7(6), 11465-11471
29. Bathula, A., Gupta, S. K., Merugu, S., et al. (2024). Blockchain, artificial intelligence, and healthcare: The tripod of future. *Artificial Intelligence Review*.
30. Kasyapa, M. S. B., & Vanmathi, C. (2024). Blockchain integration in healthcare: A comprehensive investigation of use cases, performance issues, and mitigation strategies. *Frontiers in Digital Health*.
31. Nucciarelli, L., Gottardelli, B., Gatta, R., & Damiani, A. (2024). Securing reproducibility and accountability in distributed healthcare analytics. *Studies in Health Technology and Informatics*.
32. Shahsavari, Y., Dambri, O. A., Baseri, Y., Hafid, A. S., & Makrakis, D. (2024). *Integration of Federated Learning and Blockchain in Healthcare: A Tutorial*.
33. Hong, Z., & Xiao, K. (2024). Digital economy structuring for sustainable development: The role of blockchain and AI. *Scientific Reports*.
34. Lopez, L. J. R., Mayorga, D. M., Poveda, L. H. M., et al. (2024). Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration. *Computers*.
35. Al-Saadi, M., et al. (2024). Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning. *Journal of Network and Computer Applications*.
36. Meenavolu, S. B. K., & Vanmathi, C. (2024). Blockchain integration in healthcare: Applications, performance issues, and mitigation strategies. *Frontiers in Digital Health*.