DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

IJSGS FUGUSAU VOL. 12 (2) WEBSITE: https://fugus-ijsgs.com.ng

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY
(A PUBLICATION OF FACULTY OF SCIENCE, FEDERAL UNIVERSITY GUSAU, NIGERIA)

A Secure AI-Enabled Data Governance Framework for Digital Economy Platforms

[1]Anazia Eluemunor Kizito, [1]Orove Osu Joshua, [2]Onovughe Anthonia Okeme, [3]Jeroh Esemena and [4]Nwokolo Geofrey Augustine

[1]Department of Information Systems and Technology, Southern Delta University, Ozoro
[2]Department of Software Engineering, Southern Delta University, Ozoro
[3]Department of Library and Information Science, Southern Delta University, Ozoro
[4]Department of Data Science, Southern Delta University, Ozoro

Corresponding Author's Emails & Phone No.: kaymax07@yahoo.com and anaziake@sdu.edu.ng, 08034302473

Received on: April 2026 **Revised and Accepted on:** June, 2026 **Published on:** July, 2026

ABSTRACT

The rapid expansion of digital economy platforms has created an increasing demand for secure, scalable and intelligent data governance systems capable of managing large volumes of digital transactions and sensitive information. Despite the growing adoption of digital technologies, many conventional data governance frameworks still experience major challenges such as; cybersecurity threats, poor scalability, inadequate privacy protection, inefficient governance processes and limited real-time decision-making capabilities. To address these challenges, this study presented a Secure AI-enabled data governance framework for digital economy platforms by integrating artificial intelligence, blockchain technology, cloud computing and intelligent automation mechanisms. A design-oriented and experimental system development methodology was adopted for the development and evaluation of the framework. The system was evaluated using key performance metrics including response time efficiency, precision, recall, Scalability, throughput, system availability, privacy preservation effectiveness, security performance, user satisfaction and governance efficiency. The evaluation results revealed that the framework significantly outperformed the conventional framework across all metrics. Specifically, the framework achieved an overall average performance rate of 96.68%, compared to 60.8% recorded by the conventional system. The findings indicate substantial improvements in operational efficiency, scalability, cybersecurity resilience, privacy preservation, governance effectiveness and system reliability. The study demonstrates that integrating AI-driven governance mechanisms with blockchain-supported security architectures can significantly improve transparency, trust, compliance monitoring and intelligent decision-making within digital economy platforms. Therefore, the framework provides a robust, reliable and sustainable solution for secure digital governance across sectors such as finance, healthcare, e-commerce, education and smart government systems.

Keywords: Artificial Intelligence (AI), Data Governance, Digital Economy Platforms, Blockchain Technology, Cybersecurity

1.0 INTRODUCTION

The rapid advancement of digital technologies has significantly transformed modern economies, business operations, governance systems and social interactions across the globe. Digital economy platforms such as e-commerce systems, fintech applications, cloud computing services, smart governance platforms and artificial intelligence (AI)-driven environments increasingly rely on data for decision-making, automation, innovation and efficient service delivery. As digital data continues to expand in volume and complexity, organizations are becoming more dependent on intelligent systems capable of processing, managing and securing information effectively (Dwivedi *et al.*, 2021; Acev & Back, 2025). While this digital transformation has created enormous opportunities for economic growth and innovation, it has also intensified concerns relating to cybersecurity, privacy protection, regulatory compliance and effective data governance.

Artificial Intelligence has emerged as a transformative technology for enhancing intelligent governance and improving operational efficiency within digital ecosystems. AI technologies including machine learning, predictive analytics, intelligent automation and anomaly detection systems have strengthened organizational capabilities in areas such as data analysis, fraud detection, cybersecurity management and real-time decision-making (Schmitt, 2023; Ahmad *et al.*, 2024). Through automated monitoring and intelligent data processing, AI-enabled systems can support proactive threat detection, improve service delivery and enhance the overall resilience of digital platforms.

DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

IJSGS FUGUSAU VOL. 12 (2) WEBSITE: https://fugus-ijsgs.com.ng

According to Reutter (2024), despite these technological advancements, digital economy platforms continue to experience significant challenges associated with weak governance structures, cyberattacks, data breaches, unauthorized access, algorithmic bias and inadequate compliance mechanisms. Many conventional governance frameworks were designed for centralized systems and are therefore unable to effectively manage the complexity, scalability and dynamic nature of modern digital environments (Wirtz *et al*., 2021). Furthermore, the growing integration of AI technologies into critical digital infrastructures has raised important concerns regarding transparency, accountability, ethical AI usage, privacy risks and digital trust (Hacker *et al.*, 2025).

The increasing sophistication of cyber threats further complicates digital governance practices. Cybercriminals now exploit vulnerabilities within cloud infrastructures, AI systems and interconnected digital platforms, resulting in financial losses, operational disruptions and reputational damage for organizations (Nott, 2025). Consequently, there is an urgent need for secure and intelligent governance frameworks capable of integrating cybersecurity mechanisms, AI-driven analytics, compliance management and privacy protection strategies to ensure secure, reliable and sustainable digital operations.

A Secure AI-Enabled Data Governance Framework provides a structured and integrated approach for managing digital data assets while ensuring security, transparency, accountability and intelligent governance. Such a framework combines artificial intelligence technologies, governance policies, cybersecurity controls and intelligent monitoring systems to improve data protection, operational efficiency and digital trust across digital economy platforms (Ilager *et al.*, 2020; Anazia, 2026). The integration of AI within governance systems can also support adaptive security management, automated policy enforcement and real-time compliance monitoring.

This study therefore presents a secure AI-enabled data governance framework for digital economy platforms to address the growing challenges associated with data governance, cybersecurity and intelligent digital management. The study seeks to develop a framework capable of enhancing secure data management, strengthening digital trust, improving regulatory compliance and supporting sustainable digital transformation within modern digital ecosystems. In addition, the study contributes to existing research in artificial intelligence, cybersecurity and digital governance by providing a practical and integrated framework for intelligent governance in digital economy platforms.

1.1 Literature Review

Digital economy platforms are technology-driven systems that support digital transactions, communication and service delivery through interconnected digital infrastructures. These platforms integrate technologies such as cloud computing, artificial intelligence, big data analytics, blockchain and Internet of Things (IoT) systems to improve innovation, automation and operational efficiency across sectors such as e-commerce, fintech, healthcare, education and governance (Bukht & Heeks, 2021). Modern digital platforms operate within distributed environments where data flows continuously across users, organizations and cloud systems. This complexity has increased the need for effective governance frameworks capable of ensuring data security, transparency, accountability, interoperability and regulatory compliance within digital ecosystems (Wirtz *et al*., 2021).

Artificial Intelligence (AI) plays a significant role in improving digital platform operations through technologies such as machine learning, predictive analytics, deep learning and intelligent automation (Dwivedi *et al.*, 2021). AI systems support data analysis, fraud detection, cybersecurity monitoring, personalized services and automated decision-making within digital environments. These technologies enhance operational efficiency, reduce human error and improve real-time decision-making processes (Schmitt, 2023; Maduabuchukwu *et al*., 2026).

In cybersecurity management, AI-driven security models integrate intelligent technologies into security systems to improve threat detection, adaptive security management and risk mitigation. These systems utilize machine learning algorithms, predictive analytics and automated monitoring tools to identify and respond to cyber threats in real time. Compared to traditional rule-based systems, AI-driven security models provide improved capabilities for detecting sophisticated cyber threats and automating security responses (Schmitt, 2023).

Despite these advantages, the integration of AI into digital platforms and cybersecurity systems has introduced several ethical and governance concerns. Issues such as algorithmic bias, lack of transparency, privacy risks, adversarial attacks and accountability limitations continue to affect trust in AI-driven systems (Wang *et al.*, 2020). Therefore, effective governance frameworks are essential for ensuring responsible, secure

DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

and trustworthy AI deployment within modern digital ecosystems.

Data governance frameworks provide policies, standards and procedures for managing organizational data while ensuring security, integrity, accountability and regulatory compliance (Abraham *et al.,* 2020; Qiu *et al.,* 2026). These frameworks improve transparency, operational efficiency and informed decision-making through effective data management practices.

In modern digital environments, organizations require governance frameworks that support intelligent monitoring, adaptive security management, privacy protection and automated compliance processes. Secure data governance frameworks are therefore essential for responsible AI adoption, cybersecurity protection and sustainable digital transformation (Panian, 2021; Papagiannidis *et al*., 2024).

Cybersecurity and data protection mechanisms are essential for protecting digital infrastructures, networks and organizational data from cyber threats and unauthorized access (Kshetri, 2021). Common security measures include encryption technologies, firewalls, authentication systems, intrusion detection systems and access control mechanisms. The growth of cloud computing and distributed digital systems has increased cybersecurity risks such as ransomware attacks, phishing attacks, malware infections and data breaches (Nott, 2025). Consequently, organizations increasingly adopt intelligent cybersecurity solutions capable of supporting real-time monitoring, anomaly detection and automated incident response.

In spite of these advancements in artificial intelligence (AI) and cybersecurity technologies, digital economy platforms continue to face critical governance and security challenges. Weak governance structures, poor compliance mechanisms, fragmented policies and increasing cyber threats such as data breaches and ransomware attacks continue to undermine digital trust and operational efficiency (Sun *et al.*,2023). In addition, the growing adoption of AI technologies has introduced concerns relating to algorithmic bias, privacy risks, transparency and accountability within digital systems (Rahman *et al.,* 2024).

Several studies have highlighted the importance of integrating AI, cybersecurity and governance mechanisms to support secure digital operations. Torres et al. (2025) emphasized the role of AI in improving intelligent decision-making and organizational performance, while Ahmed *et al.* (2024) stressed the need for transparency and ethical governance in AI-driven systems. Similarly, AI-enabled security systems significantly improve threat detection and cybersecurity resilience, while trustworthy AI systems and secure data governance support sustainable digital transformation (Javaid *et al.,* 2022).

Generally, existing studies largely examine AI, cybersecurity and governance independently, with limited attention given to integrated governance frameworks for digital economy platforms. Most existing systems lack intelligent monitoring capabilities, adaptive cybersecurity controls, automated compliance management and AI-driven analytics required for managing modern distributed digital ecosystems effectively. Therefore, the secure AI-enabled data governance framework for digital economy platforms is presented to improve secure digital governance, operational efficiency and digital trust within modern digital environments.

2.0 METHODS

2.1 Research Design

This study adopted a design-oriented and experimental methodology to develop and evaluate a Secure AI-enabled data governance framework for digital economy platforms. The framework integrated artificial intelligence, cloud computing, blockchain technology, cybersecurity mechanisms and privacy-preserving techniques to improve secure data management, intelligent decision-making, compliance monitoring and operational efficiency. Data collected from digital platforms, cloud systems, IoT devices and cybersecurity datasets were processed using cleaning, normalization and feature extraction techniques, while machine learning, predictive analytics, anomaly detection and natural language processing were utilized for intelligent governance and cybersecurity monitoring.

2.2 System Requirements Analysis

System requirements analysis was conducted to identify the operational, governance, security and intelligent processing needs of the framework. The analysis considered platform security requirements, governance policies, privacy protection, user expectations and regulatory compliance standards, which were categorized into functional and non-functional requirements. The framework supports secure user authentication, role-based access control, AI-driven monitoring and threat detection, governance policy enforcement, compliance management, secure data storage, audit logging, predictive analytics, automated alerts, secure API integration and backup and recovery mechanisms to enhance cybersecurity and governance efficiency. The

DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

system was also designed to achieve scalability, reliability, interoperability, privacy preservation, high performance, usability and maintainability while supporting secure integration with cloud platforms, APIs and enterprise systems for continuous and efficient operations**.**

2.3 Architecture of the Framework

The architecture of framework consists of interconnected layers designed to support intelligent governance and secure digital operations. The architecture includes the user layer, application layer, AI and analytic layer, data governance layer, security and privacy layer, data storage layer, infrastructure layer, cross-cutting services, external data sources.

2.3.1 User Layer

This layer represents the interaction point between users and the digital platform. It includes administrators, customers, employees, regulators and other stakeholders who access the system through web applications, mobile devices, dashboards, or APIs. This layer enables secure user authentication, authorization and communication while ensuring accessibility and accountability within the digital environment.

2.3.2 Application Layer

The Application Layer contains the software applications, operational services and business logic that support digital platform activities. It manages transactions, workflow automation, communication services and application integration across sectors such as e-commerce, fintech, healthcare and governance systems. This layer serves as the operational interface between users and the intelligent backend systems.

2.3.3 AI and Analytic Layer: This layer is responsible for intelligent data processing, machine learning operations, predictive analytics and automated decision-making. It analyzes large volumes of data in real time to support fraud detection, anomaly identification, cybersecurity monitoring and strategic decision support. This layer enhances operational efficiency and enables intelligent governance through AI-driven technologies.

2.3.4 Data Governance Layer

The Data Governance Layer manages organizational policies, standards, procedures and compliance requirements related to data management. It ensures data integrity, accountability, quality control and regulatory compliance while defining data ownership, access rights and lifecycle management processes. This layer supports responsible and ethical data usage across the digital ecosystem.

2.3.5 Security and Privacy Layer

In this layer, the digital infrastructures, systems and data assets from cyber threats, unauthorized access and privacy violations are being protected. It implements encryption technologies, authentication mechanisms, access control systems, intrusion detection tools and privacy-preserving techniques to ensure secure communication and data protection within the framework.

2.3.6 Data Storage Layer

The Data Storage Layer is responsible for storing, organizing, managing and retrieving structured and unstructured data generated within the platform. It supports cloud databases, distributed storage systems, backup mechanisms and recovery processes to ensure data availability, reliability, scalability and efficient storage management.

2.3.7 Infrastructure Layer

This Layer forms the foundational component of the framework and consists of hardware systems, servers, cloud computing resources, networking technologies and virtualization platforms. It provides the computational power, connectivity and technical support required for the operation, scalability and continuity of the entire digital ecosystem.

2.3.8 Cross-Cutting Services

The Cross-Cutting Services component provides shared services and system-wide support across all layers of the framework. It facilitates interoperability, monitoring, auditing, logging, compliance management and policy enforcement while ensuring coordination and integration between different framework components.

2.3.9 External Data Sources

This layer represents the framework's third-party systems, cloud services, IoT devices, external databases, partner platforms and online data streams integrated into the framework. These external sources provide real-time and diverse datasets that support intelligent analytics, interoperability, collaborative services and enhanced decision-making within the digital environment. The diagram showing the Architecture of the Framework is shown in figure 1 below.

DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

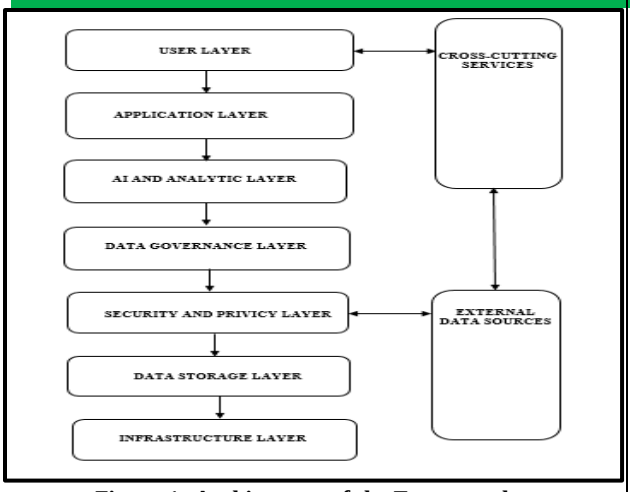

Figure 1: Architecture of the Framework

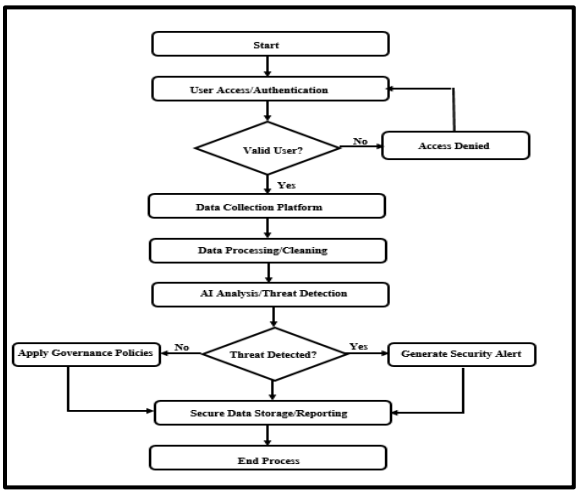

Figure 2: The framework's flowchart

3.4. The System's Algorithm

i. Start

ii. Initialize system and load AI models, governance policies, and security configurations.

iii. Authenticate user access.
If access is invalid:
Deny access and generate alert.
Else:
Grant access.

iiv. Collect data from digital platforms, cloud systems, IoT devices and system logs.

v. Preprocess data using cleaning, normalization, and feature extraction techniques.

vi. Apply AI techniques for threat detection, predictive analysis and anomaly monitoring.

vii. Enforce governance policies, compliance rules, and privacy protection mechanisms.

viii. Encrypt and securely store processed data.

ix. Generate alerts, reports and audit logs.

x. Continuously monitor system activities and update AI models.

xi. End

3.5 AI-Enabled Governance Model

The AI-enabled governance model was designed to support intelligent monitoring, automated governance enforcement and predictive security analysis. The model operates through data collection, preprocessing, AI analysis, governance enforcement and continuous monitoring processes. Machine learning algorithms were applied to analyze user behavior, detect anomalies, identify cyber threats and automate governance decisions. The model improves transparency, risk management, operational efficiency and intelligent decision-making within digital economy platforms. The AI-enabled model is shown in figure 3 below.

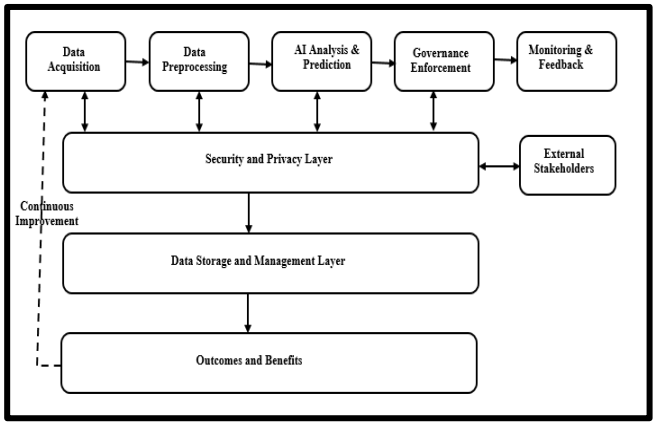

Figure 3: The AI-Enabled Model of the Framework

3.6 Security and Privacy Mechanisms

The framework integrated multiple security and privacy mechanisms to protect digital assets and sensitive information. Advanced encryption techniques, multi-factor authentication, role-based access control, blockchain verification, intrusion detection systems and privacy-preserving methods such as data anonymization were implemented to strengthen security and regulatory compliance. Secure API management, automated backup systems and disaster recovery mechanisms were also integrated to improve system resilience and data

DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

IJSGS FUGUSAU VOL. 12 (2) WEBSITE: https://fugus-ijsgs.com.ng

availability. The security and privacy mechanisms of the framework is shown in figure 4 below.

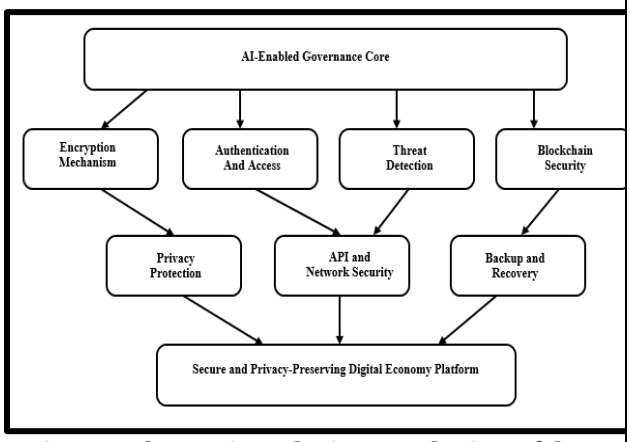

Figure 4: The security and privacy mechanisms of the framework

3.7. Development Tools and Implementation Procedure

The framework was developed using Python, JavaScript, React.js, Node.js, Django, MySQL and MongoDB to support secure and scalable frontend, backend and data management operations. TensorFlow and Scikit-learn were utilized for AI-driven analytics and threat detection, while AWS, Microsoft Azure, OpenSSL, OAuth 2.0, Ethereum and Hyperledger enhanced cloud infrastructure, encryption, authentication and blockchain-based governance operations. The implementation process involved requirement analysis, system design, AI model development, security integration, database and API configuration, testing, deployment and continuous monitoring. Security, integration and performance testing were conducted to ensure reliability, scalability, governance efficiency and cybersecurity effectiveness within the cloud-based distributed environment.

4.0 RESULTS AND DISCUSSIONS

4.1. Evaluation Metrics

The framework was evaluated using metrics such as response time efficiency, precision, recall, scalability, throughput, system availability, compliance rate, privacy preservation effectiveness, security performance user satisfaction, security performance and governance efficiency. These evaluation metrics were used to assess the framework's intelligent analytics capability and operational reliability within digital economy platforms. The table 1 and figure 5 & 6 shows the evaluation metrics of the framework.

Table 1: The evaluation metrics of the framework.

S/N	Evaluation Metric	Conventional Framework (%)	AI-Enabled Data Governance Framework (%)
1	Response Time Efficiency	47%	96%
2	Precision	72%	95%
3	Recall	68%	94%
4	Scalability	35%	98%
5	Throughput	40%	97%
6	System Availability	92%	99.8%
7	Privacy Preservation Effectiveness	58%	96%
8	User Satisfaction	68%	96%
9	Security Performance	63%	98%
10	Governance Efficiency	65%	97%

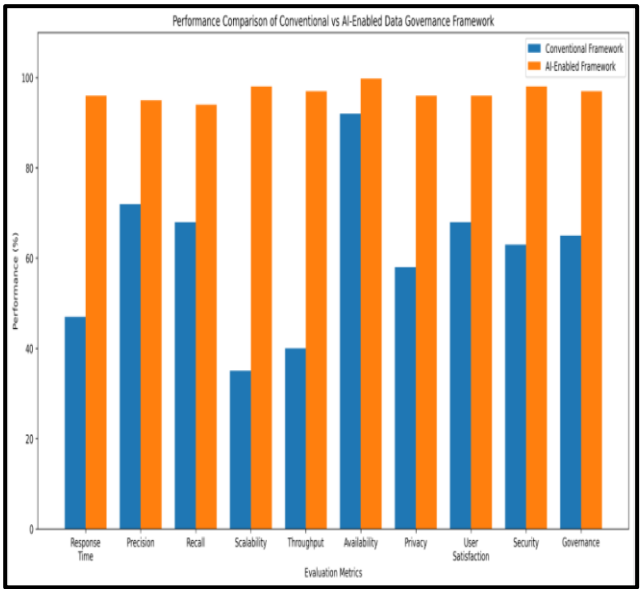

Figure 5: A bar chart showing the evaluation metrics of the framework.

DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

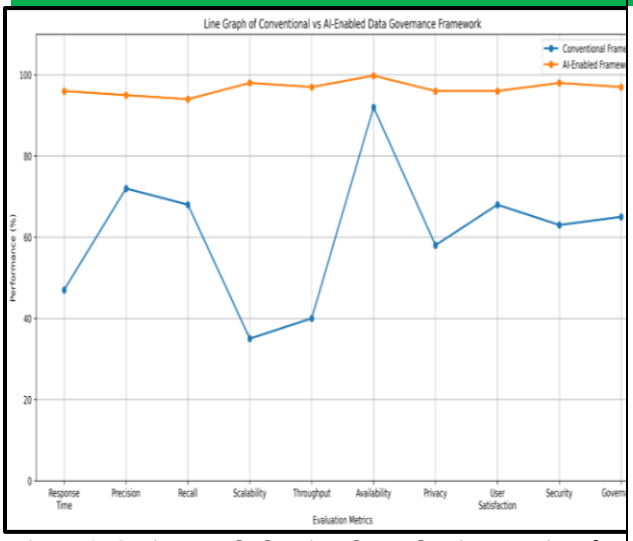

Figure 6: A Line graph showing the evaluation metrics of the framework.

4.2. Discussion

The evaluation results presented in table and graphs above demonstrate that the AI-enabled data governance framework significantly outperformed the conventional framework across all evaluation metrics. The framework achieved a response time efficiency of 96% compared to 47% in the conventional framework, indicating faster, more reliable and more efficient real-time processing capabilities for digital economy operations.

Similarly, the AI-enabled framework recorded higher precision and recall values of 95% and 94%, respectively, whereas the conventional framework achieved 72% precision and 68% recall. These results demonstrate the ability of the system to provide more accurate intelligent analysis, enhanced detection capability and reduced classification errors through the integration of AI-driven analytics and automated governance mechanisms. The new framework also achieved superior scalability and throughput performances of 98% and 97%, respectively, compared to 35% and 40% recorded by the conventional framework. These findings indicate that the AI-enabled architecture effectively supports large-scale data processing, increasing digital transactions and multiple concurrent users without significant degradation in system performance.

In terms of reliability and security, the AI-enabled framework achieved a system availability of 99.8%, exceeding the 92% recorded by the conventional system. privacy preservation effectiveness also improved substantially from 58% in the conventional framework to 96% in the new framework, demonstrating the effectiveness of the integrated encryption, access control and privacy-preserving mechanisms in protecting sensitive data and ensuring confidentiality.

Furthermore, the AI-enabled framework recorded a security performance of 98% compared to 63% in the conventional framework, indicating stronger cybersecurity resilience, intelligent threat detection and improved protection against security vulnerabilities. User Satisfaction increased significantly from 68% to 96%, while governance efficiency improved from 65% to 97%, showing that the AI-enabled framework enhanced system usability, operational transparency, compliance monitoring and governance processes.

Overall, the findings confirm that the AI-enabled data governance framework significantly outperformed the conventional framework in operational efficiency, scalability, security, privacy preservation, system reliability and governance effectiveness. The new framework achieved a higher average performance rate of 96.68% compared to 60.8%, thereby validating its effectiveness, robustness and suitability for secure and intelligent digital economy platforms.

DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

IJSGS FUGUSAU VOL. 12 (2) WEBSITE: https://fugus-ijsgs.com.ng

4.3. Some Screenshot of Interfaces within the Platform

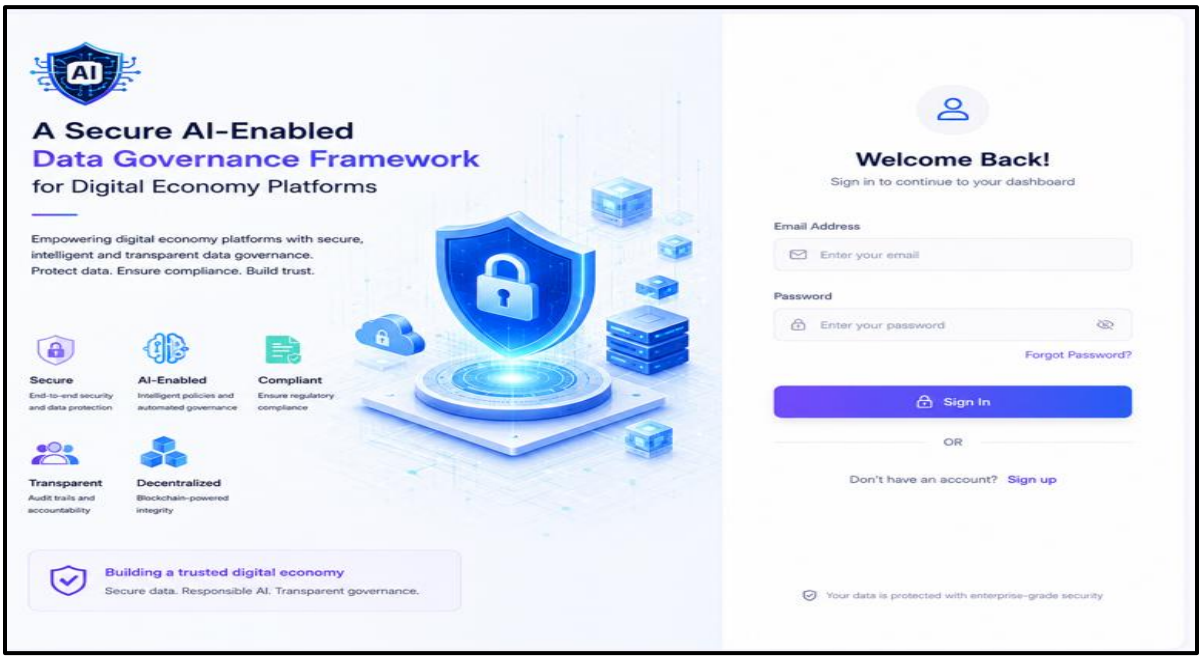

Figure 7: The welcome/login page of the framework.

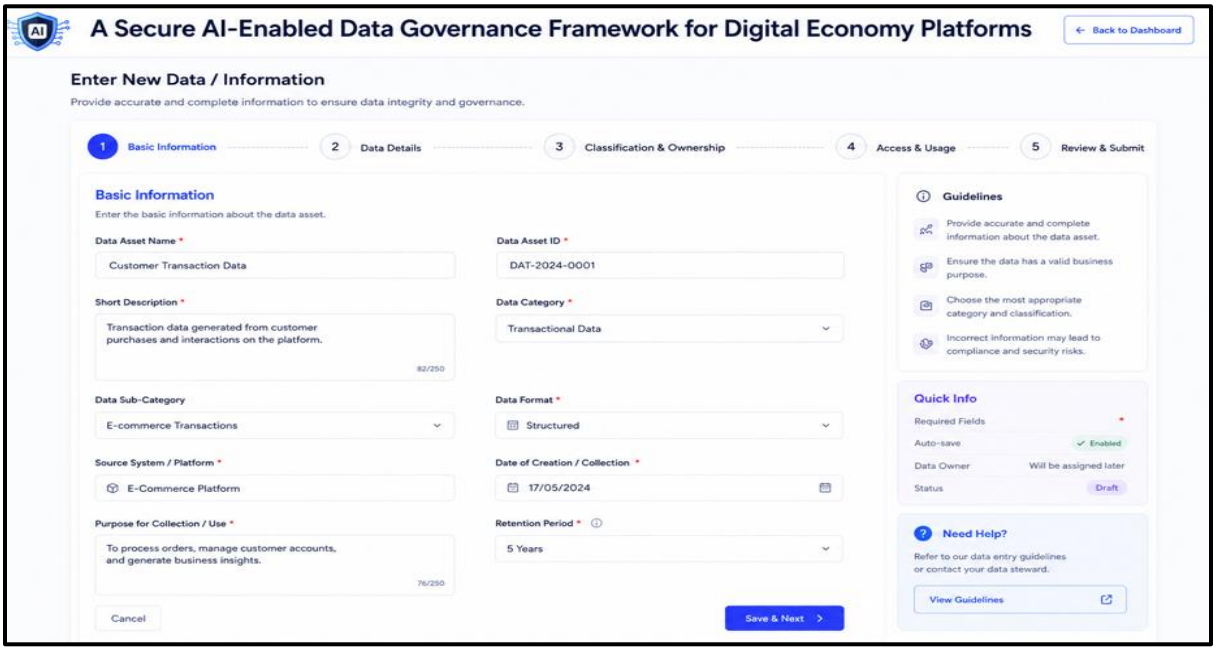

Figure 8: The data/information page of the framework.

DOI: https://doi.org/10.57233/ijsgs.v12i2.1086 ISSNp: 2488-9229; ISSNe: 3027-1118

IJSGS FUGUSAU VOL. 12 (2) WEBSITE: https://fugus-ijsgs.com.ng

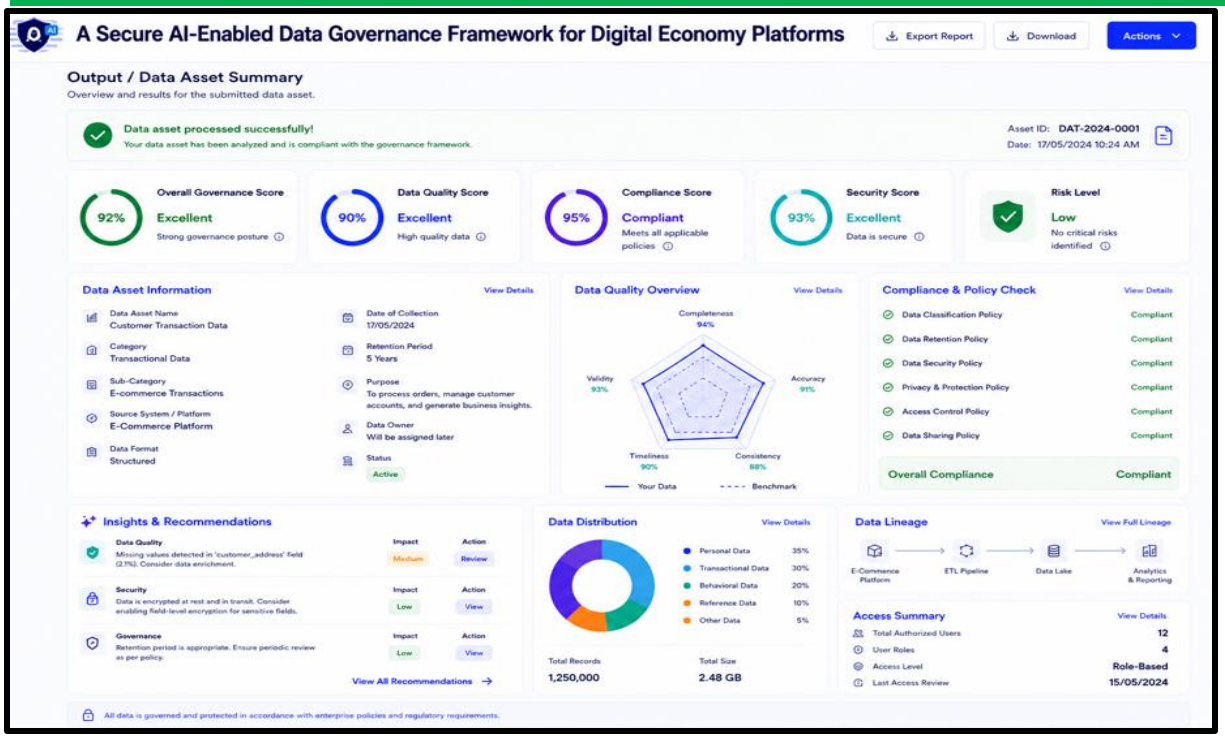

Figure 9: The Output/result page of the framework.

5.0 CONCLUSION

This study presented a secure AI-enabled data governance framework for digital economy platforms aimed at improving security, scalability, privacy preservation, operational efficiency and governance effectiveness. The AI-enabled framework integrated artificial intelligence, blockchain technology, cloud computing and intelligent governance mechanisms to address the limitations of conventional data governance systems. The evaluation results showed that the new framework significantly outperformed the conventional framework across all performance metrics, achieving a higher average performance rate of 96.68% compared to 60.8%. The framework demonstrated improvements in response time, scalability, security performance, privacy preservation, system availability, user satisfaction and governance efficiency.

Overall, the findings confirm that the AI-enabled data governance framework is effective, reliable and suitable for secure and intelligent digital economy platforms. Future research may focus on enhancing the framework using explainable AI, federated learning and advanced cybersecurity technologies.

REFERENCES

Abraham, R., Schneider, J., & vom Brocke, J. (2020). Data governance: A conceptual framework, structured review and research agenda. International Journal of Information Management, 49, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Acev, D., & Back, A. (2025). Systematic analysis of data governance frameworks and their applications in organizations. Business & Information Systems Engineering. Advance online publication. https://doi.org/10.1007/s11301-025-00545-1

Ahmad, S., Bello, M., & Ibrahim, A. (2024). Artificial intelligence-driven knowledge management systems for organizational innovation. International Journal of Information Management Data Insights, 4(1), Article 100215. https://doi.org/10.1016/j.jjimei.2024.100215

Ahmed, S., Khan, M. A., & Rahman, T. (2024). AI-enabled digital research ecosystems for collaborative scientific innovation. Journal of Information Science. Advance online publication. https://doi.org/10.1177/01655515241234567

Anazia, K. E. (2026). Smart governance in Nigerian higher education: Integrating artificial intelligence for integrity and effective university leadership. International Journal of Innovative Science and Research Technology, 11(2), 66–74. https://doi.org/10.38124/IJISRT/26FEB106

Bukht, R., & Heeks, R. (2021). Defining, conceptualising and measuring the digital economy. Development Informatics Working Paper, 68, 1–24. https://doi.org/10.2139/ssrn.3431732

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., & Williams, M. D. (2021). Artificial intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities and agenda for research, practice and policy. International Journal of Information Management, 57, Article 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Hacker, P., Kasirzadeh, A., & Edwards, L. (2025). AI, digital platforms, and the new systemic risk. arXiv. https://doi.org/10.48550/arXiv.2509.17878

Ilager, S., Sharma, R., & Kaur, P. (2020). Artificial intelligence-enabled governance systems for secure digital platforms. International Journal of Advanced Computer Science and Applications, 11(9), 120–128. https://doi.org/10.14569/IJACSA.2020.0110915

Kshetri, N. (2021). Cybersecurity management in the digital economy. Computer, 54(2), 84–88. https://doi.org/10.1109/MC.2020.3042985

Maduabuchukwu, C., Anazia, E. K., & Nwokolo, G. A. (2026). An intelligent role-based access control model enhanced with risk-based multi-factor authentication. International Journal of Research and Innovation in Applied Science (IJRIAS), 11(4), 898–907. https://doi.org/10.51584/IJRIAS.2026.110400057

Nott, C. (2025). Organizational adaptation to generative AI in cybersecurity: A systematic review. arXiv. https://doi.org/10.48550/arXiv.2506.12060

Panian, Ž. (2021). Some practical experiences in data governance. World Journal of Science, Technology and Sustainable Development, 18(4), 255–271. https://doi.org/10.1108/WJSTSD-11-2020-0091

Papagiannidis, E., Gupta, S., & Stamati, T. (2025). Responsible artificial intelligence governance: A review and research framework. The Journal of Strategic Information Systems, 34(1), Article 101885. https://doi.org/10.1016/j.jsis.2024.101885

Qiu, Y., Zhang, H., & Li, X. (2026). Construction of a theoretical framework for scientific data governance in AI-driven research ecosystems. Data and Information Management, 10(1), Article 100045. https://doi.org/10.1016/j.dim.2025.100045

Rahman, M. S., Islam, M. N., & Karim, A. (2024). Artificial intelligence-driven knowledge management systems for organizational innovation and decision-making. Knowledge and Process Management, 31(1), 44–58. https://doi.org/10.1002/kpm.1789

Reutter, L. (2024). Constructing the data economy: Tracing expectations of value through policy discourse. Journal of Cultural Economy, 17(2), 145–160. https://doi.org/10.1080/17530350.2023.2300436

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with artificial intelligence (AI)-enabled malware and intrusion detection. arXiv. https://doi.org/10.48550/arXiv.2401.01342

Sun, Z., Strang, K., & Firmin, S. (2023). Artificial intelligence and knowledge management: A systematic literature review. Journal of Knowledge Management, 27(9), 2211–2234. https://doi.org/10.1108/JKM-10-2022-0823

Torres, R., Almeida, F., & Costa, P. (2025). Artificial intelligence-supported collaborative frameworks for multi-institutional research environments. Computers in Human Behavior Reports, 17, Article 100512. https://doi.org/10.1016/j.chbr.2025.100512

Wang, X., Han, Y., Wang, C., Zhao, Q., Chen, X., & Chen, M. (2020). In-edge AI: Intelligentizing mobile edge computing, caching and communication by federated learning. IEEE Network, 33(5), 156–165.

Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2021). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. International Journal of Public Administration, 44(10), 818–829. https://doi.org/10.1080/01900692.2020.1749851