JRIIE Journal of Research Innovation and Implications in Education
Center for Research Implications & Practice

Website: www.jriiejournal.com ISSN 2520-7504 (Online) Vol.9, Iss.4, 2025 (pp. 840 - 850)

Artificial Intelligence (AI)-Driven Data Protection Strategies in Banking Institutions in Uasin Gishu County, Kenya

Hillary Kiprob, Francis Musembi Kwale & Philemon Kittur
Department of Computer Science
School of Science, University of Eldoret, Eldoret, Kenya
Email: kiproph7@gmail.com

Abstract: *In an era where traditional cybersecurity measures are increasingly inadequate against the growing sophistication and volume of digital threats, banks are compelled to adopt innovative technologies such as AI. The study explored the adoption and effectiveness of Artificial Intelligence (AI)-based strategies for data protection among banking institutions in Uasin-Gishu County, Kenya. The present study employed surveys and interviews to investigate the integration of AI tools, particularly machine learning algorithms for fraud detection, predictive analytics, and anomaly detection in selected banking institutions. The study revealed that all surveyed banks (100%) had adopted AI-based security systems, with 68.6% focusing on fraud prevention and 66.7% on anomaly detection. A statistically significant relationship (p < 0.001) was observed between strong data protection policies and firms' integration of AI in security frameworks. The adoption of AI was driven by its capacity to predict threats, enhance fraud detection, and improve operational efficiency. Despite these benefits, the study identified significant challenges, including a shortage of skilled professionals for AI system implementation and persistent concerns regarding data privacy. Additionally, existing regulatory frameworks were deemed insufficient to address emerging risks associated with AI-driven data security. Most respondents acknowledged that the advantages of AI outweighed its challenges, making it a preferred solution for enhancing data protection. The study concludes that AI enhances data security in the banking sector and recommends strengthened regulatory frameworks, increased investment in specialized AI training, and continuous stakeholder engagement to maximize AI's potential in the cybersecurity landscape.*

Keywords: *Artificial Intelligence, Cybersecurity, Data protection, Banking, Uasin Gishu County, Fraud detection, Anomaly detection, Machine learning, Digital transformation, Data Privacy*

How to cite this work (APA):

Kiprob, H., Kwale, F. M. & Kittur, P. (2025). Artificial Intelligence (AI)-Driven Data Protection Strategies in Banking Institutions in Uasin Gishu County, Kenya. *Journal of Research Innovation and Implications in Education, 9*(4), 840 – 850. **https://doi.org/10.59765/prgw85**.

1. Introduction

Cybersecurity has become one of the most critical issues for financial institutions in the digital economy, which is presently experienced in the contemporary global world. The use of digital platforms by banks and other financial service providers is increasingly gaining momentum in providing smooth services, maintaining records of customers, and making financial transactions. Nevertheless, the financial industry has become a highly profitable target of computer criminals, who use advanced attacks, including ransomware attacks, phishing, identity theft, and insider attacks, as highlighted by the Office of the Data Protection Commissioner (ODPC, 2024). The financial sector is considered one of the most attacked industries, according to the global cybersecurity reports, because financial data is sensitive and valuable (Abdulsalam & Tajudeen, 2024). Consequently, bank security has become resistant to cyberattacks, whereby modern technologies like Artificial Intelligence (AI) have been embraced to identify, stop, and address the constantly changing cyber threats.

The financial institutions in the African continent are equally reporting a spike in digital transformation due to mobile banking, fintech innovations, and financial inclusion programs. Nevertheless, the cybersecurity preparedness has not expanded concurrently. There is a lack of proper cyber defense mechanisms, highly trained security experts, and viable regulations in many African countries, and this makes banks more susceptible to attacks, as highlighted by Mithra et al. (2023). Cybercriminals are using such security loopholes to engage in massive fraud, data breaches, and hacking into systems. As a result, African financial institutions are currently proceeding with AI-based data protection solutions to enhance threat detection, prevent fraud, and secure sensitive financial information.

The financial sector in Kenya is one of the most advanced sectors in Africa and has been majorly attributed to innovations like mobile banking platforms like M-Pesa and the growing use of digital and online banking solutions. Digital finance has been growing at a fast rate, where the data of many customers is stored and sent electronically. To protect such data, the government introduced the Data Protection Act (DPA) of 2019, which is implemented by the Office of the Data Protection Commissioner. This legislation is forcing financial institutions to make serious data privacy and data security policies. Regardless of this legislation, cyber-attacks in Kenya have been on the rise in frequency and severity, with banks being susceptible to fraud, data breaches, and operational interruptions (ODPC, 2024). Perimeter-based security strategies that were traditionally used are not enough to combat these emerging threats anymore, which has increased attention to AI-based security mechanisms.

The Uasin Gishu County in the Rift Valley region in Kenya has experienced a substantial increase in the use of digital financial services as banks keep increasing their operations to satisfy the customers. The digital transformation has led to growth in the consumption and production of sensitive financial data, which has raised the issue of privacy and cybersecurity. Otieno (2019) conducted a study on competitive strategies employed by commercial banks within the county, but did not discuss the implementation of an up-to-date AI-driven cybersecurity. This shows that there is a gap in critical knowledge regarding the integration of Artificial Intelligence by banks in Uasin Gishu to increase data protection.

This research aims to fill this gap by analyzing the application of AI-related approaches to protect data in banking institutions in Uasin Gishu County. In particular, the paper examines AI as a way of improving data security, analyzes its efficacy in improving cybersecurity resilience in organizations, and determines the advantages and issues of adopting AI. The results of this research will give useful advice to banks, technology providers, and policymakers on how to focus on the enhancement of cybersecurity systems, the reduction of operational risks, and the advancement of safe digital banking in Kenya.

Research Objectives

The main objective of this research is to analyze the application and efficacy of AI-related approaches to protect data in banking institutions in Uasin Gishu County, Kenya.

The study's specific objectives are:

1. To examine the adoption and integration level of AI-driven data protection strategies in banking institutions in Uasin Gishu County.
2. To analyze the effectiveness of AI in improving data security and cybersecurity resilience within these banking institutions.
3. To determine the advantages and issues associated with adopting AI-driven data protection strategies in the banking sector.

2. Literature Review

Banking systems worldwide are undergoing rapid digital transformation, driven by high-volume transactions, mobile banking, and real-time payment infrastructures. As cyber-risks evolve, traditional perimeter security models are no longer sufficient. The CIA triad and Zero-Trust security frameworks guide modern institutions toward continuous monitoring and dynamic threat response. In this context, AI, especially machine-learning-based fraud detection and anomaly detection models, has become central to financial data protection. However, the pace of AI adoption varies globally, with emerging markets such as Kenya facing capability gaps and regulatory constraints. This review examines the current state of AI-driven data protection in banking, with emphasis on Africa’s evolving financial-technology landscape and the policy environment shaping cybersecurity practices.

2.1 Digital Transformation in Banking

The banking sector is experiencing a fundamental digital transformation due to technological innovations and changing customer needs in the market (Sun & Zhang, 2025). Digital transformation requires implementing digital technologies across all banking operations to produce fundamental changes in operational and customer value. According to Saba et al. (2025), mobile connectivity acts as a catalyst for financial inclusion, representing, is a vital aspect of this transformation. Research by Tian (2024) reveals how AI helps organizations achieve these transformative objectives through better operations management and improved client interactions and risk mitigation strategies. Digital banking operations need modernized protection strategies for data because the industry now relies heavily on technological information.

2.2 Cybersecurity Challenges in the Digital Age

Digital platforms have exposed banking institutions to multiple cybersecurity threats due to their growing dependency on these systems. Major financial setbacks and damaged reputations emerge from data breaches, fraud, and cyberattacks targeting banking institutions. According to Mishra (2023), the financial industry needs sophisticated security solutions to safeguard sensitive data, as AI-based cybersecurity provides protection. The growth of digital technologies has increased the weaknesses of conventional security systems, so businesses need to adopt modern data protection methods based on AI technology. A recent study by Zziwa et al. (2024) identifies AI and data analytics as crucial tools for reducing cybersecurity threats in financial establishments.

2.3 The Role of Artificial Intelligence (AI) in Banking

Artificial Intelligence is fundamentally transforming the banking industry by providing solutions to a multitude of challenges, with data protection being a primary application (Tian, 2024). This transformation is driven by the enhancement of key security measures through AI technologies, including predictive analytics, machine learning, and anomaly detection software. The implementation of these systems, however, presents the financial sector with a dual landscape of significant opportunities and inherent risks, as AI continues to power the new digital economy (Tian, 2024). Beyond security, AI and machine learning are recognized for effectively optimizing core banking operations. This broad utility is evident in emerging economies, where the applications of AI in customer service journeys and other service areas have been extensively analyzed (Abdulsalam & Tajudeen, 2024).

2.4 Challenges and Ethical Considerations of AI Adoption

Banks' implementation of AI systems includes multiple advantages but requires addressing several business and ethical issues. The banking sector faces challenges related to personal information protection, biased algorithms, and workforce replacements. Borah and Borah (2024) evaluated the advantages and safety concerns linked to AI-driven financial stability while advocating for deliberate evaluation of its implications and how AI affects banking operations through its applicability and corresponding difficulties. Onyenje et al. (2024) explored privacy attitudes alongside human behaviors during post-privacy times, since they affect AI-driven data collection operations.

2.5 AI-Driven Data Protection Strategies

When protecting their sensitive data, AI algorithms have become a critical need for banking institutions. The banking sector uses anomaly detection systems, machine learning algorithms, and predictive analytics to prevent fraud. Nwafor et al. (2024) explored how banking institutions can achieve security through AI risk assessment techniques without sacrificing innovation. Research by Asongu and Odhiambo (2022) provided a systematic AI-related fraud detection review examining data science solutions for improved cybersecurity. Onyenje et al. (2024) examined data privacy and cybersecurity issues within AI-enhanced financial services sectors via their extensive review of the research field. Engvell (2024) examined the institutional elements that shape AI adoption in European Union banking cybersecurity operations, providing evaluation data from various institutions.

3. Methodology

3.1 Research Design

The study employed a descriptive survey, which is suitable for describing the population's characteristics and current events with the guidance of research done by Borah and Borah (2024). This design made it possible to study the adoption and effects of AI strategies with questionnaires and the advantages and problems related to the topic by interviewing people familiar with the area. This approach provided a broad picture of the situation, and further insight could be gained into important matters.

3.2 Study Area and Target Population

The banking institutions in Uasin Gishu County formed the study area for this study. Due to the large share of banking and increasing digital changes, Uasin Gishu County was chosen as the right setting for reviewing present-day data protection issues and AI.

The participants in this study were personnel working in data protection and IT security in banking institutions in Uasin-Gishu County. The target participants were IT managers, cybersecurity experts, data privacy officers, and other professionals responsible for managing and overseeing data protection methods. The target population was the 37 financial institutions based in Uasin Gishu County, according to the Kenya National Bureau of Statistics (KNBS) (2021). In the first stage of the study, the number of banks and the size of the target group were established to ensure the results accurately represent the area.

3.3 Sampling Size and Sampling Procedures

The study employed various methods to select the 102 participants who participated in the survey. Purposive sampling was performed to get responses from participants with expertise and knowledge in AI and data protection. The quantitative part employed stratified random sampling to ensure that various banking institutions are represented. KNBS (2021) indicated that the target population was the 37 financial institutions based in Uasin Gishu County. The study analyzed 34 banking customers in relation to customer trust, alongside five instances of banking institutions that had effectively adopted AI-driven data protection approaches. To represent the whole population of banking institutions in Uasin-Gishu County and make findings accurate, the sample size was calculated according to Kothari's (2004) formula, as shown below.

$n=(Z^2 \cdot P \cdot (1-P))/e^2$
Where:

- n - sample size
- P - population proportion (0.5)
- Z - standard variance at 95% confidence level (1.96)
- e - desired precision level (0.05)

3.4 Data Collection Tools and Procedure

Open-ended and closed-ended questions were used in a structured questionnaire given to a larger group. The questionnaires were designed to gather information on the number of firms adopting AI security systems, the methods they use, the results of data security, and opinions on both the positive and negative aspects, according to Osabutey and Jackson (2024). Semi-structured interviews were conducted with a group of selected participants. The interviews helped to discuss multiple issues, specific problems, and detailed groups or cases related to AI protecting data.

The questionnaires captured adoption levels of AI, specific tools in use, perceived effectiveness of protection practices, and challenges experienced. Interviews were then used to clarify and deepen these responses by probing issues such as regulatory pressure, skill gaps, and institutional readiness. Questionnaires were distributed in person and via secure internal email channels were permitted by the institutions. Interviews were scheduled at times chosen by the respondents and recorded in detailed notes for analysis.

3.5 Validity and Reliability

The study results are reliable and trustworthy, as both validity and reliability were closely examined. The content was checked by review panels of academic supervisors and experts in cybersecurity and banking to ensure that the instruments were appropriate. Because of this, the instruments were properly suited to test the key aspects and aimed at variables in the research. Cronbach's Alpha coefficient, widely used, was employed to measure the reliability of the questionnaires. A pilot study was conducted before data collection to identify any potential issues and clarify any uncertainties or discrepancies in the instruments, thereby enhancing their reliability.

3.6 Data Analysis

The quantitative responses obtained from the questionnaires were coded, uploaded into SPSS, and analyzed. Data on adoption rates, practices, and perceptions were summarized using frequencies, percentages, means, and standard deviations. I relied on statistical approaches, such as correlation and regression analysis, to examine how AI impacts data protection. The information accessed from interviews was transcribed, identified with codes, and then analyzed with thematic analysis. Important patterns in the transcripts were noted, grouped, and blended with the data from the questionnaires to enhance the understanding of the findings.

3.7 Ethical Considerations

Approval for the study was obtained from the National Commission for Science, Technology, and Innovation (NACOSTI) and the banking organizations concerned. The subjects in the interviews chose the days and times that were most convenient for them, and they understood and agreed to the procedures beforehand. Every effort was made to ensure that the participants' identities remained secret while gathering data.

4. Results and Discussions

4.1 Adoption of AI-Based Security Systems in Surveyed Financial Institutions (N =102)

Findings indicate that all surveyed financial institutions in Uasin Gishu County have implemented at least one AI-based security system. Every respondent (N = 102, 100%) confirmed that their institution currently employs AI in data-protection operations (Table 1). This universal adoption demonstrates a high degree of technological advancement and institutional recognition of AI's critical role in safeguarding sensitive banking data.

Table 1: AI use in financial institutions in Uasin Gishu County

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	102	100.0	100.0	100.0

The results confirm full adoption of AI-based security solutions across all banks in the County. This consensus highlights broad recognition of AI's strategic importance in mitigating digital risks. Consistent with Fares et al. (2022), AI is predominantly deployed for early fraud detection and proactive threat prevention. Local banks now regard AI not as a competitive differentiator but as a foundational element of digital resilience. The technology's predictive capabilities further strengthen institutional preparedness for evolving cyber threats (ODPC, 2024).

4.2 Most Common AI Tools

Fraud detection through machine learning (68.6%), anomaly detection (66.7%), and biometric authentication (57.8%) emerged as the most frequently implemented AI technologies (Table 2). These tools enable institutions to identify suspicious activity, verify user identities securely, and anticipate potential cyber threats. The findings align with global trends in which fraud detection remains the leading driver of AI adoption in finance (Alaba et al., 2025). Soyombo (2024) similarly observes that AI's ability to detect complex, subtle patterns indicative of fraudulent behavior underscores its superiority in processing large, dynamic datasets. Less common applications, such as predictive analytics and natural language processing, are limited, likely due to higher technical and resource requirements.

Table 2: Common AI Tools in Financial Institutions in Uasin Gishu County

AI Technology	*% Selected*
Anomaly Detection	66.7%
Fraud Detection (Machine Learning)	68.6%
Predictive Analytics	34.3%
Natural Language Processing (Logs)	23.5%
Biometric Authentication	57.8%

4.3 Level of AI Integration in Financial Institutions in Uasin Gishu County

On average, institutions rated their level of AI integration as 3.61 out of 5 (Table 3), indicating that most banks are currently utilizing AI periodically but still have opportunities to expand their use in daily operations. The boxplot in Figure 2 illustrates the distribution of AI integration levels among financial institutions. The median integration score was 4, indicating that at least half of the banks reported moderate to high levels of AI integration.

Most institutions fall within the 3 to 5 range, showing a strong overall presence of AI in operational systems. A few outliers, however, reported integration scores as low as 1, suggesting that some institutions are still in early stages of AI implementation.

Table 3: Level of AI integration in financial institutions in Uasin Gishu County

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Integration Level	102	1	5	3.61	1.136
Valid N (listwise)	102				

The presence of outliers with very low integration suggests disparities in institutional capacity, possibly linked to differences in financial resources, staff expertise, or infrastructure. This finding is consistent with those of Olowu et al. (2024), which showed that even in regions with widespread AI awareness, uneven adoption is common due to cost and technical barriers. According to Chlouverakis and Rawal (2024), the absence of AI guidelines, lack of human touch, and lack of audibility and transparency of AI systems are some of the critical barriers to the deployment of AI banking practices in India, and the same could be the reason in Kenya, which is also a developing country. However, the high median score of 4 suggests that at least half of the institutions are on track toward embedding AI as a core part of their operational frameworks.

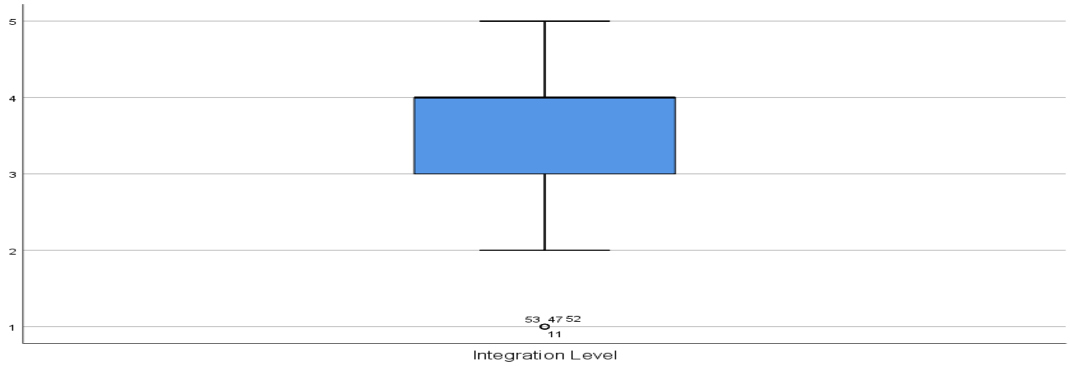

Figure 1: Level of AI integration in financial Institutions in Uasin Gishu County

4.4 Effectiveness of Data Protection Practices

Participants rated the effectiveness of their existing data protection measures on a scale from 1 (poor) to 5 (excellent). The best-rated protections were regular security audits (4.25), firewall systems (4.24), and data encryption (4.22) (Table 3). These tools help protect the system from cyber-attacks and unauthorized access. However, cybersecurity training for staff scored the lowest (3.62), indicating that many banks may lack the trained personnel needed to fully support AI systems.

Similar findings have been reported by Boukherouaa et al. (2022), who showed that the human factor remains the weakest link in cybersecurity despite advanced technical measures. Therefore, without adequate staff awareness and skills, the effectiveness of AI systems may be undermined. This highlights the need for financial institutions to strike a balance between technical investment and human capacity building through targeted training, workshops, and certification programs.

Table 4: Descriptive Statistics on the Effectiveness of Data Protection Practices

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Firewall and intrusion detection	102	2	5	4.24	.811
Regular security audits	102	2	5	4.25	.727
Data encryption	102	2	5	4.22	.816
Data Access and Control	102	2	5	4.07	.735
Employee cybersecurity training	102	2	5	3.62	.890
Incident Response Plans	102	2	5	4.00	.901
Data loss and prevention systems	102	2	5	3.96	.757
Valid N (listwise)	102				

4.5 Data Protection Scores within Financial Institutions with higher AI integration levels

Pearson correlation analysis revealed strong, statistically significant positive relationships between AI integration levels and all seven data protection practices ($p < 0.001$). Banks with greater AI adoption exhibited more effective implementation of security mechanisms, including firewalls, encryption, audits, and incident response plans. The strongest correlation occurred between AI integration and data loss prevention systems ($r = 0.696$), followed by encryption ($r = 0.562$), and incident response mechanisms ($r = 0.532$) (Table 5).

Table 4: AI Integration Scores

		Firewall	Audits	Encryption	Access Control	Training	Incident Response	DLP	Integration Level
Firewall	Pearson Correlation	1	.502**	.581**	.388**	.483**	.664**	.612**	.521**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000
Audits	Pearson Correlation	.502**	1	.307**	.375**	.534**	.514**	.432**	.422**
	Sig. (2-tailed)	.000		.002	.000	.000	.000	.000	.000
Encryption	Pearson Correlation	.581**	.307**	1	.289**	.455**	.525**	.655**	.562**
	Sig. (2-tailed)	.000	.002		.003	.000	.000	.000	.000
Access Control	Pearson Correlation	.388**	.375**	.289**	1	.479**	.434**	.486**	.472**
	Sig. (2-tailed)	.000	.000	.003		.000	.000	.000	.000
Training	Pearson Correlation	.483**	.534**	.455**	.479**	1	.580**	.506**	.467**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000
Incident Response	Pearson Correlation	.664**	.514**	.525**	.434**	.580**	1	.668**	.532**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000
DLP	Pearson Correlation	.612**	.432**	.655**	.486**	.506**	.668**	1	.696**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000
Integration Level	Pearson Correlation	.521**	.422**	.562**	.472**	.467**	.532**	.696**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	

**. Correlation is significant at the 0.01 level (2-tailed).

This correlation suggests that AI-driven systems play a critical role in safeguarding against data breaches by reinforcing key technical measures. Moderate but still significant associations were found with employee training (r = 0.467) and access control (r = 0.472), showing that institutions that invest in AI also make parallel efforts to strengthen human and procedural aspects of data security.

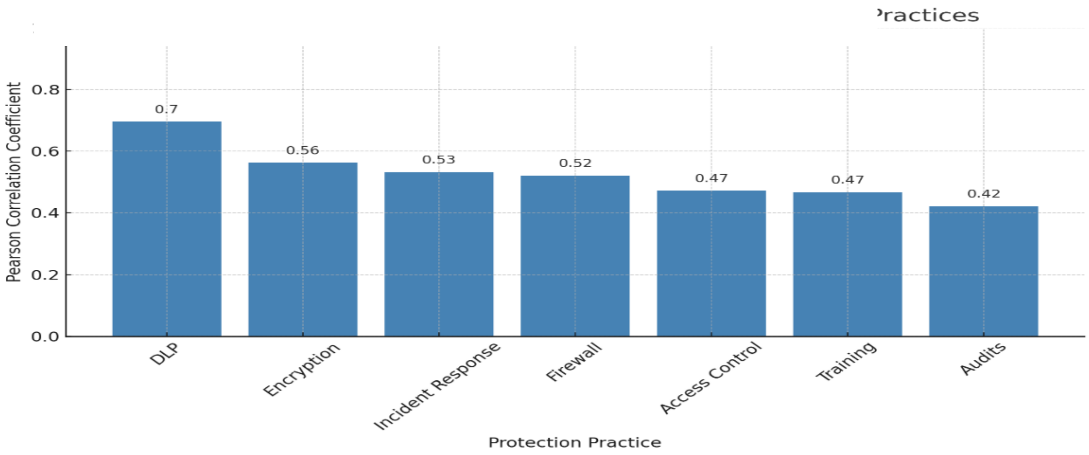

Figure 2: Correlation between AI Integration Levels in Financial Institutions and Protection Practices

These findings demonstrate that AI integration is not only linked to the adoption of advanced technologies but also enhances the overall security culture within financial institutions. The results are consistent with global studies, as indicated by Ikudabo and Kumar (2024), which highlight that AI strengthens both technological and organizational resilience against cyber risks. However, the relatively weaker correlations with training and access control underline the persistent gap in human capacity and governance frameworks, which may limit the full potential of AI adoption. Generally, the correlation results confirm that AI integration is a strong predictor of improved data protection effectiveness, particularly for advanced security mechanisms such as encryption, incident response, and data loss prevention, as highlighted by Sadok et al. (2022).

5. Conclusions and Recommendations

5.1 Conclusion

The findings show that AI adoption in banking institutions across Uasin Gishu County is already universal, with all surveyed institutions reporting the use of AI-based security systems. Fraud detection and anomaly detection emerged as the most common applications, reflecting a strong focus on preventing financial crime and safeguarding customer data. On average, banks demonstrated a moderately high level of AI integration (mean score of 3.61 out of 5), suggesting that while AI tools are actively in use, there is still room for growth in embedding AI across broader security functions. The study also established a strong and statistically significant association between higher AI adoption and more effective data protection practices, particularly in areas such as data loss prevention, encryption, and incident response systems. However, capacity gaps remain, especially in staff training and the clarity of regulatory guidelines, indicating that banks still face human-resource and governance challenges even as their technical capabilities advance.

5.2 Recommendations

The present study revealed that AI has been widely adopted by financial institutions in Uasin Gishu County, with fraud detection and anomaly detection being the most commonly used applications. The average integration level is moderately high, indicating a growing reliance on AI for security functions. The correlation analysis confirms that institutions with deeper AI integration are more likely to report stronger security practices, supporting the conclusion that AI not only enhances operational capacity but also reinforces institutional commitment to data protection. It is therefore recommended that:

1. Financial institutions should prioritize continuous staff training and training and technical upskilling in AI and cybersecurity to address existing human-resource gaps.
2. Policymakers should establish adaptive and transparent regulatory frameworks that balance innovation with accountability, ensuring responsible AI deployment.
3. Strengthening cooperation among banks, regulators, and technology providers is essential to share best practices and coordinate responses to evolving cyber threats.
4. Banks should allocate resources for ongoing AI infrastructure upgrades and ethical-use monitoring to sustain long-term data protection resilience. Collectively, these measures can help the Kenyan banking sector optimize AI's potential while minimizing its associated risks.

References

Abdulsalam, T. A., & Tajudeen, R. B. (2024). Artificial Intelligence (AI) in the banking industry: A review of service areas and customer service journeys in emerging economies. *Business & Management Compass*, *68*(3), 19–43.

Alaba, J. S., Ahmed, S. J., Farida, A. P., & Oluwatosin, O. V. (2025). Adoption of AI-Driven Fraud Detection System in the Nigerian Banking Sector: An Analysis of Cost, Compliance, and Competency. *Economic Review of Nepal*, *8*(1), 16–33.

Asongu, S. A., & Odhiambo, N. M. (2022). The role of economic growth in modulating mobile connectivity dynamics for financial inclusion in developing countries. *World Affairs*, *185*(3), 530–556.

Borah, P., & Borah, A. C. (2024). A Review of use of Artificial Intelligence in Teaching and Learning of Mathematics. *International Journal on Science and Technology*, *15*(4), 1–9.

Boukherouaa, E., AlAjmi, K., Deodoro, J., Farias, A., & Ravikumar, R. (2022). *Powering the digital economy: Opportunities and risks of artificial intelligence in finance.* International Monetary Fund. https://doi.org/10.5089/9781589063952.087

Chlouverakis, K., & Rawal, A. (2024). *How artificial intelligence is reshaping the financial services industry*. EY CESA Financial Services.

Engvall, N. (2024). The influence of institutional factors on AI adoption in EU banking cybersecurity: A narrative literature review [Master's thesis, Södertörn University]. https://www.diva-portal.org/smash/get/diva2:1875709/FULLTEXT01.pdf

Fares, O. H., Butt, I., & Lee, S. H. M. (2022). Utilization of artificial intelligence in the banking sector: A systematic literature review. *Journal of Financial Services Marketing*, *28*, 835–852.

Ikudabo, A. O., & Kumar, P. (2024). AI-driven risk assessment and management in banking: Balancing innovation and security. *International Journal of Research Publication and Reviews*, *5*(10), 3573–3588.

KNBS. (2021). *Uasin Gishu County statistical abstract*. Kenya National Bureau of Statistics. https://www.knbs.or.ke/wp-content/uploads/2023/09/2021-County-Statistical-Abstracts-Uasin-Gishu.pdf

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Age International. https://books.google.co.ke/books?id=hZ9wSHysQDYC

Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, *13*(10), 5875.

Mithra, A. S., Duddukuru, V. C., & Manu, K. (2023). How artificial intelligence is revolutionizing the banking sector: The applications and challenges. *Asian Journal of Management*, *14*(3), 166–170.

Nwafor, K. C., Ikudabo, A. O., Onyeje, C. C., & Ihenacho, D. (2024). Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics. *International Journal of Science and Research Archive*, *13*(01), 2895–2910.

ODPC. (2024). *Personal Data Protection Act handbook*. Office of the Data Protection Commissioner. https://www.odpc.go.ke/wp-content/uploads/2024/02/PERSONAL-DATA-PROTECTION-HANDBOOK.pdf

Olowu, O., Adeleye, A. O., Omokanye, A. O., Ajayi, A. M., Adepoju, A. O., Omole, O. M., & Chianumba, E. C. (2024). AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity. *Advanced Research and Review*, *21*(2), 227–237.

Onyeje, C. C., Oluloni, T. M., & Olanrewaju, J. (2024). Data Privacy and Cybersecurity Challenges in AI-Enhanced Financial Services: A Comprehensive Analysis. *International Journal of Research Publication and Reviews*, *5*(10), 3498–3509.

Osabutey, E. L., & Jackson, T. (2024). Mobile money and financial inclusion in Africa: Emerging themes, challenges and policy implications. *Technological Forecasting and Social Change*, *202*, 123339.

Otieno, K. (2019). Competitive strategies and performance of selected commercial banks in Uasin Gishu County, Kenya [Master's Thesis, Kenyatta University]. https://ir-library.ku.ac.ke/bitstreams/f4704c73-e5e3-43af-80c4-88515febd15e/download

Saba, C. S., Ngepah, N., & Odhiambo, N. M. (2025). The Nexus Between ICT Diffusion, Financial Development, Industrialization and Economic Growth: Evidence from Sub-Saharan African Countries. *Journal of African Business*, *26*(2), 454–478.

Sadok, H., Sakka, F., & El Maknouzi, M. E. H. (2022). Artificial intelligence and bank credit analysis: A review. *Cogent Economics & Finance*, *10*(1), 2023262.

Soyombo, O. T. (2024). Reviewing the role of AI in fraud detection and prevention in financial services. *International Journal of Science and Research Archive*, *11*(1), 2101–2110.

Sun, Y., & Zhang, Q. (2025). Navigating the digital transformation of commercial banks: Embracing innovation in customer emotion analysis. *Journal of the Knowledge Economy*, *16*(1), 3440–3461.

Tian, X. (2024). The Role of Artificial Intelligence in the Digital Transformation of Commercial Banks: Enhancing Efficiency, Customer Experience, and Risk Management. E3S Web of Conferences, *208*, 01029.

Zziwa, I., Ilolo, A., Nwafor, K. C., & Ihenacho, D. O. (2024). Cloud Computing and AI in

Cybersecurity Forensics: Leveraging Data Analytics for Enhanced Threat Detection and Incident Response. *International Journal of Research Publication and Reviews*, *5*(10), 2907–2920.