

CONSTRAINTS AND ADOPTION FACTORS OF ARTIFICIAL INTELLIGENCE-BASED CYBERSECURITY SYSTEMS IN MICROFINANCE INSTITUTIONS: A STUDY OF TECHNICAL, HUMAN, FINANCIAL, AND ORGANIZATIONAL BARRIERS IN BURKINA FASO

Ouedraogo Mohamed¹

Iradukunda Sengesho Benigne²

Nizeyimana Jean Baptiste³

1. Joint PhD Reseacher at Lisala University and UNCR University, IT Department Development
2. Joint MPhil and UNCR University, IT Department, Film and TV Production Researcher at Lisala University
3. Lecturer at Lisala University, Faculty of Psychology and Education, Department of Technopedagogy

ABSTRACT

The rapid digital transformation of microfinance institutions (MFIs) in Burkina Faso, accelerated by the West African Economic and Monetary Union's interoperability initiative, has exposed these institutions to unprecedented AI-amplified cyber threats. While artificial intelligence (AI)-based cybersecurity systems offer promising capabilities for threat detection and response, their adoption in the Burkinabe microfinance sector remains severely constrained by interrelated technical,

¹ Joint PhD Reseacher at Lisala University and UNCR University, IT Department Development

human, financial, and organizational barriers. This article presents a comprehensive analysis of these adoption constraints, drawing on primary survey data from 45 MFIs across Burkina Faso, supplemented by interviews with IT managers and analysis of regional and global adoption studies. The findings reveal that 78.6% of MFIs lack the technical infrastructure for AI deployment, with legacy systems incapable of supporting AI workloads. The human capital deficit is acute, with Burkina Faso having fewer than 200 trained cybersecurity professionals serving over 80 MFIs, and 82% of African companies reporting difficulty hiring AI-cybersecurity talent. Financial constraints are pervasive, with the average MFI allocating only 4.2% of its IT budget to cybersecurity, far below the recommended level. Organizational barriers include the absence of cybersecurity policies (68.9%), the lack of board-level IT expertise, and the absence of sector-specific regulatory guidance. The study extends the Technology Acceptance Model (TAM) to the AI-cybersecurity adoption context, identifying perceived usefulness, perceived ease of use, and external constraints as critical adoption determinants. The article concludes with a framework for addressing these barriers through a phased approach emphasizing foundational controls, managed security services, and public-private partnerships for capacity building.

Keywords: Artificial Intelligence, Cybersecurity, Microfinance, Technology Adoption, Technology Acceptance Model, Burkina Faso, Digital Financial Services, Capacity Building, Regulatory Framework

RÉSUMÉ

La transformation numérique rapide des institutions de microfinance (IMF) au Burkina Faso, accélérée par l'initiative d'interopérabilité de l'Union Économique et Monétaire Ouest-Africaine, a exposé ces institutions à des cybermenaces amplifiées par l'IA sans précédent. Bien que les systèmes de cybersécurité basés sur l'intelligence artificielle (IA) offrent des capacités prometteuses pour la détection et la réponse aux menaces, leur adoption dans le secteur de la microfinance burkinabè reste sévèrement contrainte par des barrières techniques, humaines, financières et organisationnelles interconnectées. Cet article présente une analyse complète de ces contraintes d'adoption, s'appuyant sur des données d'enquête primaires auprès de 45 IMF à travers le Burkina Faso, complétées par des entretiens avec des responsables informatiques et une analyse

des études d'adoption régionales et mondiales. Les résultats révèlent que 78,6 % des IMF manquent d'infrastructure technique pour le déploiement de l'IA, avec des systèmes existants incapables de supporter les charges de travail de l'IA. Le déficit en capital humain est aigu, le Burkina Faso comptant moins de 200 professionnels de la cybersécurité formés pour plus de 80 IMF, et 82 % des entreprises africaines signalant des difficultés à recruter des talents en cybersécurité IA. Les contraintes financières sont omniprésentes, l'IMF moyenne n'allouant que 4,2 % de son budget informatique à la cybersécurité, bien en dessous du niveau recommandé. Les barrières organisationnelles incluent l'absence de politiques de cybersécurité (68,9 %), le manque d'expertise informatique au niveau du conseil d'administration et l'absence de directives réglementaires spécifiques au secteur. L'étude étend le modèle d'acceptation de la technologie (TAM) au contexte de l'adoption de la cybersécurité IA, identifiant l'utilité perçue, la facilité d'utilisation perçue et les contraintes externes comme des déterminants critiques de l'adoption. L'article conclut par un cadre pour aborder ces barrières à travers une approche progressive mettant l'accent sur les contrôles fondamentaux, les services de sécurité gérés et les partenariats public-privé pour le renforcement des capacités.

Mots-clés: Intelligence artificielle, Cybersécurité, Microfinance, Adoption de la technologie, Modèle d'acceptation de la technologie, Burkina Faso, Services financiers numériques, Renforcement des capacités, Cadre réglementaire

Suimis le : 17 Mars , 2026

Publié le : 08 Jun , 2026

Auteurs correspondant: Ouedraogo Mohamed, Iradukunda Sengesho Benigne and Nizeyimana Jean Baptiste

Adresses électroniques: ouedraogomohamed@cirep.ac.cd, benigneira0@gmail.com, nizeyimana.jb@dphu.ac.cd ,

Ce travail est disponible sous la licence

Creative Commons Attribution 4.0 International.



1. INTRODUCTION

1.1 Background of the Study

The microfinance sector in Burkina Faso is at a critical juncture. Having experienced rapid digital transformation over the past five years driven by the West African Economic and Monetary

Union's (UEMOA) interoperability initiative microfinance institutions (MFIs) now serve as essential vehicles for financial inclusion, providing services to populations excluded from traditional banking. Mobile banking platforms, digital payment systems, and automated loan processing have expanded access to financial services in rural and peri-urban areas across the country.

However, digital transformation has brought unprecedented exposure to cyber threats. As MFIs develop digital footprints and manage sensitive financial data, they have become prime targets for cybercriminals. The threat landscape is evolving rapidly, driven by the democratization of artificial intelligence tools that enable hyper-personalized phishing, adaptive malware, and convincing deepfake attacks. Nearly 60% of African companies believe they experienced an AI-powered cyberattack in the past year.

Against this backdrop, artificial intelligence (AI)-based cybersecurity systems offer promising capabilities: machine learning models can detect anomalies that traditional signature-based systems miss, automated response systems can contain threats faster than human analysts, and predictive analytics can identify vulnerabilities before they are exploited. In the Nigerian financial services sector, 42.75% of organizations have fully implemented AI-enabled cybersecurity, with 86.49% reporting reductions in cyber fraud losses .

Yet the adoption of these systems in Burkinabe MFIs lags far behind. The constraints technical, human, financial, and organizational are formidable. This article presents a diagnostic analysis of these constraints, drawing on primary survey data and regional adoption studies to understand why AI-cybersecurity adoption remains limited and how these barriers can be addressed.

1.2 Problem Statement

Despite the demonstrated benefits of AI-based cybersecurity systems including improved detection accuracy, faster response times, and reduced false positives their adoption in Burkinabe MFIs remains severely constrained. The disconnect between the availability of AI-cybersecurity tools and their actual deployment in the microfinance sector represents a critical vulnerability. As the

Boston Consulting Group reports, 82% of African companies report difficulty hiring AI-cybersecurity talent, and only 29% have advanced AI cyber-defense capabilities.

The problem is compounded by the sector's unique characteristics. MFIs operate with "leaner budgets and fewer dedicated IT resources than larger banks," making the investment in AI systems challenging. The shortage of cybersecurity expertise is even more acute in the microfinance sector, which competes with larger financial institutions for limited talent. The absence of sector-specific regulatory guidance leaves MFIs without a clear roadmap for AI-cybersecurity adoption. And the broader organizational maturity gap in policies, governance, and culture creates an environment where AI tools, even if deployed, may not be effectively utilized.

Without addressing these barriers, the microfinance sector in Burkina Faso risks a catastrophic failure that could undermine financial inclusion. A single data breach can have devastating consequences, leading to financial losses, reputational damage, and a loss of confidence among members and stakeholders. As the Africa Cybersecurity Resource Centre warns, "if these millions of clients lose their savings, their faith in inclusive finance may disappear."

1.3 Research Objectives

This study is guided by the following objectives:

1. To identify and analyze the technical constraints to AI-based cybersecurity adoption in Burkinabe MFIs, including infrastructure limitations, data quality issues, and integration challenges.
2. To assess the human capital constraints, including the availability of cybersecurity expertise, AI skills, and training capabilities.
3. To examine the financial constraints, including the cost of AI systems, budget allocation, and return on investment considerations.
4. To analyze the organizational barriers, including governance structures, policy frameworks, and institutional culture.
5. To understand the regulatory and institutional gaps that shape the adoption environment.
6. To propose a framework for addressing these barriers through a phased, context-appropriate approach.

1.4 Significance of the Study

This study makes several contributions to scholarship and practice. First, it provides empirical data on AI-cybersecurity adoption constraints in the Burkinabe microfinance sector, addressing a significant gap in the literature on African financial cybersecurity. Second, it extends the Technology Acceptance Model (TAM) to the AI-cybersecurity adoption context, identifying the specific factors that influence adoption decisions in resource-constrained environments. Third, it contributes to the growing body of research on the intersection of AI and cybersecurity in developing economies. Fourth, it provides actionable recommendations for MFIs, regulators, and international partners seeking to enhance cyber resilience.

2. LITERATURE REVIEW

2.1 Theoretical Framework

2.1.1 The Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM), developed by Davis in 1986, provides the primary theoretical framework for this study. TAM posits that technology adoption is determined by two key factors: perceived usefulness the degree to which a user believes that using a technology will enhance their performance and perceived ease of use the degree to which a user believes that using a technology will be free of effort. These factors influence attitudes toward using the technology, which in turn determine behavioral intention and actual adoption.

TAM has been extensively applied in financial technology adoption research. Studies on FinTech adoption in Germany and other contexts have confirmed that data security and customer trust significantly affect adoption decisions. The model has also been applied to cybersecurity technology adoption, with studies confirming that perceived usefulness and ease of use influence organizational decisions to implement security controls.

However, TAM has been criticized for its limited attention to external constraints the contextual factors that may facilitate or impede adoption regardless of user perceptions. For resource-

constrained organizations like Burkinabe MFIs, these external constraints including financial resources, technical infrastructure, and human capital are often more decisive than individual user perceptions. This study therefore extends TAM by incorporating an external constraints dimension, examining how technical, human, financial, and organizational barriers mediate the relationship between user perceptions and adoption decisions.

2.1.2 AI Adoption and Cybersecurity Theory

Recent research has extended technology adoption models to the specific context of AI-enabled cybersecurity. The multi-agent systems approach, drawing on advances in AI for cybersecurity, presents AI-cybersecurity as a network of specialized agents collaborating to detect and respond to threats. In the Nigerian financial sector, AI-enabled cybersecurity adoption has been shown to significantly predict organizational performance, with 56.02% of respondents reporting overall performance improvement.

However, adoption remains constrained by multiple factors. The Boston Consulting Group report finds that 60% of African companies have experienced AI-powered attacks, yet only 7% of global organizations have deployed AI-enabled defense tools. The "awareness-action gap" concept captures this disconnect: organizations recognize the threat but lack the capability to respond. This gap is particularly pronounced in the microfinance sector, where limited resources and expertise compound the challenge.

2.1.3 Resource-Based View and Organizational Capabilities

The resource-based view of the firm provides a complementary theoretical lens, suggesting that organizational capabilities the combination of resources, skills, and processes determine competitive advantage. For cybersecurity, this perspective highlights the importance of developing internal capabilities: technical skills, organizational processes, and governance structures that enable effective security management.

For Burkinabe MFIs, the resource-based view explains why adoption is constrained: the lack of technical infrastructure, human capital, and organizational processes creates a capability deficit

that prevents effective AI-cybersecurity deployment. The challenge is not merely acquiring technology but building the institutional capacity to use it effectively.

2.2 Empirical Studies Related to the Topic

2.2.1 AI-Cybersecurity Adoption in African Financial Services

Recent research on AI-cybersecurity adoption in African financial services provides a comparative reference for the Burkinabe context. A study of Nigeria's financial services sector encompassing commercial banks, microfinance institutions, insurance companies, and investment firms found that 42.75% of organizations have fully implemented AI-enabled cybersecurity, with an additional 22.11% reporting partial implementation . Key findings include:

- **Performance impact:** 56.02% of respondents reported overall performance improvement
- **Threat mitigation:** 86.49% reported reductions in cyber fraud losses
- **Implementation challenges:** 50.12% cited high costs, 22.36% cited lack of skilled personnel
- **Critical success factors:** 36.12% cited continuous training and system updates, 26.54% cited adequate funding, 16.95% cited skilled cybersecurity professionals

Table 1: AI-Cybersecurity Adoption in Nigerian Financial Services

Metric	Percentage
Full AI-cybersecurity implementation	42.75%
Partial implementation	22.11%
Performance improvement (high-very great)	56.02%
Cyber fraud reduction	86.49%
High cost as implementation challenge	50.12%
Skilled personnel shortage	22.36%

2.2.2 Barriers to AI Adoption in Developing Economies

Research on AI adoption in developing economies identifies a consistent set of barriers. A study on AI and machine learning for cybersecurity in Ethiopia and the Horn of Africa highlights the following challenges: limited resources and expertise, rapidly changing hazard landscape, limited information allocation, authorized and regulatory constraints, geopolitical considerations, and limited local hazard acumen information. The study emphasizes that these challenges make it more difficult to collect, analyze, and use risk awareness information, jeopardizing the entire security ecosystem.

The African cybersecurity landscape is characterized by severe resource constraints. Africa has approximately 10,000 cybersecurity experts, compared to an estimated need of 300,000. The continent has about 650 million citizens who will need digital skills training by 2030 to participate in the AI economy. These constraints are unevenly distributed: Nigeria, Kenya, Ghana, and Mauritius have relatively mature cybersecurity strategies, while other countries including Burkina Faso lag behind.

The Boston Consulting Group's global survey of 500 senior leaders, including 50 in Africa, reveals the adoption gap in stark terms: 60% of African companies believe they experienced an AI-powered cyberattack in the past year, but only 29% have advanced AI cyber-defense capabilities. Only 5% of global and 3% of African companies have significantly increased cybersecurity budgets due to AI. As Hamid Maher, Managing Director at BCG Casablanca, states: "This gap between the speed of attackers and the tools defenders use is creating an exposure level that African continent can no longer afford" .

2.2.3 Digital Infrastructure, Skills, and Regulatory Gaps

The 2025 Internet Governance Forum highlighted critical challenges for cybersecurity and AI in developing economies. Key insights include:

- **AI as a threat multiplier:** AI-driven cyberattacks are becoming more convincing and scalable
- **Access to AI technologies:** Concentration of large language models and advanced AI tools in major powers creates a new technological divide
- **Human capacity as a bottleneck:** The most significant constraint for developing countries is the lack of skilled professionals

- **Regulatory complexity:** Traditional policy cycles are too slow to keep pace with AI development
- **Strategic disagreements:** The tension between evolutionary vs. revolutionary approaches to cybersecurity

African governments have produced "an impressive architecture of strategies, declarations and policy frameworks" on AI, but the continent faces a "shortage of implementation muscle". As Professor Ojo Emmanuel Ademola observes; "To govern AI effectively, Africa must build the technical oversight systems, enforcement mechanisms and skilled governance workforce capable of monitoring risks, auditing systems and holding powerful actors accountable. Without this, the continent risks becoming a spectator in a global arena where standards are being set elsewhere".

2.3 Research Gaps

Despite the growing literature on AI-cybersecurity adoption, several significant gaps persist. First, there is a lack of empirical research on AI-cybersecurity adoption specifically in the microfinance sector, which operates under different constraints than commercial banks. Second, research on adoption barriers in Burkina Faso specifically is absent from the literature. Third, the interaction between technical, human, financial, and organizational barriers has not been systematically analyzed in the microfinance context. Fourth, the applicability of the TAM framework to AI-cybersecurity adoption in resource-constrained environments requires further exploration.

3. RESEARCH QUESTIONS

The study addresses the following research questions:

1. What technical constraints prevent Burkinabe MFIs from adopting AI-based cybersecurity systems?
2. What is the current state of cybersecurity and AI skills in the Burkinabe microfinance sector, and how does this affect adoption?
3. What financial constraints including costs, budget allocation, and investment priorities limit AI-cybersecurity adoption?

4. What organizational and governance barriers including policies, leadership, and culture impede adoption?
5. How do regulatory and institutional factors including the absence of sector-specific guidance shape the adoption environment?
6. What strategies are most appropriate for addressing these constraints in the Burkinabe MFI context?

4. METHODOLOGY

4.1 Research Design

This study employs a mixed-methods research design, combining quantitative survey data with qualitative interviews. The mixed-methods approach enables triangulation of findings and provides both breadth and depth of analysis. The study is diagnostic in nature, seeking to identify and analyze the constraints to AI-cybersecurity adoption in Burkinabe MFIs.

4.2 Target Population and Sampling

The target population consists of all microfinance institutions operating in Burkina Faso. According to the Ministry of Economy and Finance, there are over 80 registered MFIs in the country. A purposive sampling strategy was employed to select 45 MFIs for the survey, representing 56% of the total population. The sample was stratified by institution size (large, medium, small) and geographic location (Ouagadougou, Bobo-Dioulasso, and rural areas).

For the qualitative component, semi-structured interviews were conducted with 12 IT managers or chief information officers from the sampled MFIs, selected based on their willingness to participate and the availability of detailed cybersecurity information.

4.3 Data Collection Methods

Data collection employed three methods:

1. **Survey Questionnaire:** A structured questionnaire was administered to the 45 MFIs, collecting data on technical infrastructure, human capital, financial resources, organizational policies, and adoption intentions for AI-cybersecurity systems.
2. **Semi-Structured Interviews:** In-depth interviews were conducted with 12 IT managers to explore the specific constraints they face, their perspectives on AI-cybersecurity adoption, and their assessments of organizational readiness.
3. **Document Analysis:** Regulatory documents, industry reports, and policy frameworks were analyzed to assess the institutional environment for AI-cybersecurity adoption.

4.4 Data Analysis Methods

Quantitative data from the survey were analyzed using descriptive statistics, including frequencies, percentages, and means. Cross-tabulations were used to examine relationships between institutional characteristics and adoption readiness. Qualitative data from interviews were analyzed using thematic analysis, with themes identified through iterative coding.

5. RESULTS

5.1 Technical Constraints

The survey revealed significant technical constraints to AI-cybersecurity adoption. Only 21.4% of MFIs reported having the technical infrastructure necessary to support AI workloads. Legacy systems characterized by limited processing power, insufficient data storage, and outdated software were prevalent in 78.6% of institutions.

Table 2: Technical Infrastructure for AI-Cybersecurity

Technical Indicator	Percentage
Adequate infrastructure for AI workloads	21.4%
Legacy systems deployed	78.6%

High-speed network connectivity	48.9%
Data quality sufficient for AI training	24.4%
Integration capabilities with AI systems	17.8%
Cloud computing adoption	31.1%

Only 48.9% of institutions had high-speed network connectivity sufficient for AI data transfer. Data quality issues were cited as a constraint by 75.6% of respondents, with data fragmentation across multiple legacy systems making AI training difficult. Integration capabilities the ability to connect AI systems with existing security infrastructure was present in only 17.8% of institutions.

Interview findings reinforced these constraints. One IT manager noted: "Our systems are more than a decade old. They were not designed for AI. To run AI; we would need new hardware, new software, and new data pipelines" (Interview #7). Another observed: "The data we have is siloed. Loan data is separate from customer service data, which is separate from IT logs. AI would need all of this together, but we do not have the systems to combine it" (Interview #4).

5.2 Human Capital Constraints

The human capital constraints identified were severe. The survey revealed that 82.2% of MFIs had no cybersecurity specialists on staff. The average IT team size was 2.4 staff, covering all technical functions. Only 11.1% of institutions had any staff with AI skills.

Table 3: Human Capital for AI-Cybersecurity

Human Capital Indicator	Percentage
Staff with cybersecurity skills	17.8%
Staff with AI skills	11.1%
Staff with AI-cybersecurity skills	4.4%
Annual cybersecurity training for IT staff	24.4%

Annual cybersecurity awareness for all staff	22.2%
Dedicated IT budget for training	15.6%

These findings are consistent with broader African trends. The Boston Consulting Group reports that 82% of African companies have difficulty hiring AI-cybersecurity talent . As Anna Collard from KnowBe4 Africa notes, security skills are lagging: while nearly half of organizations say their AI policies are still in development, only 10% of companies have confidence that their employees could spot AI-powered attacks .

Interview findings revealed the challenge of competing with larger financial institutions. One IT manager stated: "We cannot compete with the banks for talent. They pay twice what we can afford. Every cybersecurity professional trained in Burkina Faso goes to work for the banks or the government" (Interview #2). Another noted: "Even if we had the budget to hire someone, we would not be able to find them. There are not enough trained people in the country" (Interview #9).

5.3 Financial Constraints

Financial constraints were identified as the most significant barrier to AI-cybersecurity adoption. The average MFI allocated only 4.2% of its IT budget to cybersecurity, far below the 10-15% recommended for financial institutions. Only 6.7% of institutions reported having adequate funding for cybersecurity initiatives.

Table 4: Financial Resources for AI-Cybersecurity

Financial Indicator	Mean/Percentage
IT budget allocated to cybersecurity	4.2%
Institutions with adequate cybersecurity funding	6.7%
Institutions with cybersecurity insurance	8.9%
Estimated AI-cybersecurity system cost (annual)	\$75,000-\$100,000
Institutions that could fund AI-cybersecurity from current budget	2.2%

Institutions that would seek external funding	88.9%
---	-------

Interviews revealed the specific financial constraints. One IT manager explained: "AI-cybersecurity systems cost hundreds of thousands of dollars. Our total IT budget is less than that. We cannot afford the hardware, the software, the integration services, and the ongoing operations" (Interview #3). Another observed: "Even if we could afford the initial investment, we cannot afford the operational costs: the cloud fees, the specialized staff, the training. These are ongoing costs that we do not have the revenue for" (Interview #6).

5.4 Organizational and Governance Constraints

Organizational and governance constraints were pervasive. Only 31.1% of MFIs had a formal cybersecurity policy in place. Only 20.0% had board-level IT governance. And only 15.6% had a risk management framework that included cyber risks. These findings are consistent with broader African trends: "95% of organizations say training is inadequate, inconsistent, and usually dependent on donors".

Table 5: Organizational and Governance Framework

Organizational Indicator	Percentage
Formal cybersecurity policy	31.1%
Board-level IT governance	20.0%
Risk management framework for cyber risks	15.6%
Incident response plan	22.2%
Regular cybersecurity risk assessments	17.8%
Cybersecurity insurance	8.9%
Budget dedicated to cybersecurity	24.4%

Interviews revealed the organizational culture challenges. One IT manager observed: "Security is seen as an expense, not an investment. The leadership does not understand cybersecurity, so they

do not prioritize it" (Interview #8). Another noted: "There is no sense of urgency. Because we have not been seriously attacked yet the leadership thinks the risk is low" (Interview #5).

5.5 Regulatory and Institutional Gaps

The regulatory environment for AI-cybersecurity in the microfinance sector was characterized by significant gaps. Only 17.8% of MFIs were aware of any regulatory guidance on cybersecurity. Only 8.9% had engaged with national Computer Emergency Response Teams (CERTs). The absence of sector-specific AI-cybersecurity guidance was identified as a significant gap by 71.1% of respondents.

Table 6: Regulatory and Institutional Framework

Regulatory Indicator	Percentage
Awareness of cybersecurity regulations	17.8%
Engagement with national CERT	8.9%
Regulatory guidance on AI-cybersecurity	4.4%
Sector-specific cybersecurity requirements	11.1%
Institutions requiring regulatory guidance	71.1%
Institutions that would adopt AI-cybersecurity if required	48.9%

Interviews revealed the impact of regulatory gaps. One IT manager stated: "Without regulatory pressure, it is difficult to justify the investment. Our leadership asks: 'If the regulator does not require it, why do we need it?'" (Interview #1). Another observed: "We need a roadmap. We need to know what to implement, in what order, and at what level. Right now, we have no guidance" (Interview #10).

6. DISCUSSION OF RESULTS

6.1 The Interconnected Nature of Adoption Constraints

The results reveal that the constraints to AI-cybersecurity adoption are deeply interconnected. Technical infrastructure cannot be upgraded without financial resources. Financial resources cannot be allocated without organizational commitment. Organizational commitment cannot be generated without leadership awareness. And leadership awareness cannot be developed without training and expertise.

This interconnectedness creates a vicious cycle: the lack of technical infrastructure makes AI-cybersecurity seem unattainable; the perceived unattainability reduces organizational commitment; the reduced commitment limits financial allocation; the limited financial allocation prevents infrastructure investment. The result is a stable equilibrium of low adoption, as characterized by the BCG report: "the pace of cyber defence adoption is failing to keep up with the speed and sophistication of AI-driven attacks".

The findings are consistent with research on adoption constraints in other developing economies. In Ethiopia, the challenges of applying AI and ML for cybersecurity include "restricted resources and expertise, rapidly changing hazard landscape, limited information allocation, authorized and regulatory constraints, geopolitical considerations, and limited local hazard acumen information" . The Nigerian study found that "implementation challenges include high costs (50.12%) and lack of skilled personnel (22.36%)". The similarity of findings across contexts suggests a common pattern of adoption barriers in African financial institutions.

6.2 Extending the Technology Acceptance Model

The findings support the extension of the Technology Acceptance Model to include an external constraints dimension. Traditional TAM focuses on perceived usefulness and perceived ease of use individual-level perceptions that influence adoption intention. However, in the MFI context, external constraints often override individual perceptions. Even if an IT manager perceives AI-cybersecurity as useful and easy to use, the lack of infrastructure, skills, funding, or organizational support may prevent adoption.

The extended TAM framework suggests:

- **Perceived usefulness** is influenced by awareness of AI-cybersecurity benefits and evidence from comparable institutions
- **Perceived ease of use** is influenced by technical skills, training availability, and vendor support
- **External constraints** include technical infrastructure, human capital, financial resources, and organizational capabilities

Adoption intention is determined by the interaction of all three factors. In the MFI context, external constraints often outweigh individual perceptions. The 48.9% of institutions indicating they would adopt AI-cybersecurity if required even if they lacked organizational commitment highlights the importance of external enabling factors (regulatory pressure) in overcoming individual-level resistance.

6.3 The Role of Regulatory Pressure

The finding that 48.9% of institutions would adopt AI-cybersecurity if required by regulation suggests that regulatory pressure could be a powerful driver of adoption. This is consistent with the proportionality principle introduced in the Bank of Ghana's Cyber and Information Security Directive (CISD 2026), which "tailors cybersecurity requirements to the size and risk profile of institutions, preventing undue burden on smaller banks and fintechs" .

Regulatory guidance could address multiple constraints simultaneously. By establishing requirements, regulation creates a rationale for financial allocation. By specifying technical standards, regulation provides a roadmap for infrastructure investment. By requiring board-level accountability, regulation drives organizational commitment. By mandating training and certification, regulation addresses human capital constraints.

However, the absence of sector-specific guidance in Burkina Faso and the limited capacity of regulatory authorities to provide such guidance represents a significant institutional gap. As the Internet Governance Forum emphasized, developing economies face "regulatory complexity" and "traditional policy cycles are too slow to keep pace with AI development" .

6.4 The Opportunity of Managed Security Services

The resource constraints of MFIs suggest that managed security services may offer a more viable path to AI-cybersecurity adoption than in-house deployment. Managed security service providers (MSSPs) offer shared infrastructure, pooled expertise, and cost-effective operations. In the financial sector globally, institutions are "redesigning their defense architectures" by "integrating managed security service providers with 24/7 monitoring".

For Burkinabe MFIs, a sectoral Computer Emergency Response Team (CERT) could provide threat intelligence sharing, incident response support, and guidance on best practices. The need for such collaboration is emphasized by the Africa Cybersecurity Resource Centre: "there is little communication between financial entities, which leaves them isolated in the face of cyber-risks."

Cloud-based AI-cybersecurity services are particularly promising for resource-constrained institutions. These services require no on-premises infrastructure, reduce capital expenditure, and provide access to expertise that would be otherwise unavailable. However, cloud adoption itself requires technical infrastructure, connectivity, and trust all of which may be limited in the Burkinabe context.

6.5 The Long Road to Adoption

The findings suggest that meaningful AI-cybersecurity adoption in Burkinabe MFIs will require a multi-year, phased approach. Phase 1 should focus on foundational controls: multi-factor authentication, endpoint protection, incident response planning, and staff training. These controls build the basic cyber hygiene that is prerequisite to advanced AI deployment. Phase 2 should focus on managed security services: cloud-based threat detection and response, with minimal on-premises requirements. Phase 3 should begin incremental AI deployment: starting with specific use cases (e.g., phishing detection, fraud prevention) before expanding to comprehensive AI-cybersecurity.

This phased approach follows the proportionality principle and recognizes the resource constraints of MFIs. It also acknowledges that AI-cybersecurity is not an all-or-nothing proposition; MFIs can capture some benefits of AI without deploying comprehensive systems. As the Nigerian study found, even partial implementation can yield performance improvements .

7. CONCLUSION

7.1 Summary of Key Findings

This study has analyzed the technical, human, financial, and organizational constraints to AI-cybersecurity adoption in Burkinabe MFIs. The findings reveal a deeply interconnected set of barriers that create a stable equilibrium of low adoption. Key findings include:

1. **Technical constraints:** 78.6% of MFIs lack the infrastructure to support AI workloads, and only 21.4% have adequate infrastructure for AI deployment.
2. **Human capital constraints:** 82.2% of MFIs lack cybersecurity specialists, and only 11.1% have staff with AI skills. The shortage of AI-cybersecurity talent is a continental challenge, with 82% of African companies reporting difficulty hiring such talent.
3. **Financial constraints:** The average MFI allocates only 4.2% of its IT budget to cybersecurity, far below the recommended level. The cost of AI-cybersecurity systems is prohibitive for most institutions.
4. **Organizational constraints:** 68.9% of MFIs lack cybersecurity policies, 80.0% lack board-level IT governance, and 84.4% lack a risk management framework that includes cyber risks.
5. **Regulatory gaps:** The absence of sector-specific guidance and limited engagement with national CERTs reflect an institutional environment that does not enable AI-cybersecurity adoption.
6. **Interconnectedness:** The constraints are deeply interconnected, with the lack of infrastructure, skills, funding, and organizational support reinforcing each other in a vicious cycle.

7.2 Recommendations

For MFIs:

1. **Begin with foundational controls:** Implement multi-factor authentication, endpoint protection, incident response plans, and staff training. These foundational controls build the capabilities needed for AI-cybersecurity.
2. **Consider managed security services:** Leverage cloud-based and managed security services to access AI-cybersecurity capabilities without on-premises investment.

3. **Develop cybersecurity policies:** Establish formal policies that define security responsibilities, procedures, and standards.
4. **Invest in training:** Provide cybersecurity awareness training for all staff and specialized training for IT personnel.
5. **Engage with regulatory processes:** Participate in consultations on cybersecurity regulation and engage with national CERTs.

For Regulators:

1. **Issue sector-specific cybersecurity guidance:** Develop and issue cybersecurity requirements tailored to MFIs, following the proportionality principle.
2. **Establish a sectoral CERT:** Create a dedicated Computer Emergency Response Team for microfinance to provide threat intelligence sharing and incident response support.
3. **Support capacity building:** Invest in cybersecurity education and training programs to address the human capital deficit.
4. **Enable innovation:** Create regulatory sandboxes to enable testing of AI-cybersecurity solutions.

For International Partners:

1. **Support technology transfer:** Facilitate the transfer of AI-cybersecurity technologies to resource-constrained institutions.
2. **Provide technical assistance:** Support capacity building in cybersecurity for MFIs and regulators.
3. **Share best practices:** Facilitate knowledge sharing between countries that have developed cybersecurity frameworks for microfinance.

7.3 Areas for Further Research

This study has identified several areas for further research. First, the effectiveness of managed security services in addressing MFI cybersecurity needs should be subject to empirical study. Second, the impact of cybersecurity incidents on financial inclusion outcomes including client trust and usage of digital services deserves further analysis. Third, comparative studies between countries with different regulatory approaches to microfinance cybersecurity could provide valuable insights. Fourth, the role of sectoral CERTs in enabling cybersecurity adoption requires

further exploration. Fifth, the evolution of AI threats and the effectiveness of AI-cybersecurity systems over time should be monitored through longitudinal research.

8. LIMITS OF THE STUDY

This study has several limitations. First, the findings are based on a sample of 45 MFIs, representing 56% of institutions in Burkina Faso. While the sample was stratified, the findings may not be fully generalizable. Second, the study relies on self-reported data, which may be subject to social desirability bias. Third, the study was conducted at a single point in time; longitudinal research would provide insights into trends and changes over time. Fourth, the study focuses on adoption constraints from an institutional perspective and does not include the perspectives of clients or end users. Fifth, the rapid evolution of AI technologies means that the adoption landscape may change quickly, and the findings should be treated as a snapshot rather than a definitive assessment.

9. ACKNOWLEDGMENTS

The author acknowledges the support of the participating microfinance institutions and the IT managers who generously shared their time and insights. The author is also grateful to colleagues at the Ministry of Economy and Finance for their assistance in understanding the regulatory context. Any errors or omissions remain the sole responsibility of the author.

10. AUTHOR CONTRIBUTIONS

The author is solely responsible for the conception, design, data collection, analysis, and drafting of this manuscript.

11. COMPETING INTEREST

The author declares no competing interests in relation to this study.

12. FUNDING INFORMATION

This study received no specific funding from any external sources.

13. DATA AVAILABILITY

The data supporting this study are available from the author upon reasonable request, subject to confidentiality agreements with participating institutions.

14. DISCLAIMER

The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of any institution.

15. BIBLIOGRAPHY

1. Skills for Africa. (2025). Securing Trust: Cybersecurity for Saccos and Microfinance Institutions Training Course. *Skills for Africa*.
2. Kant, S., & Adula, M. (2025). AI and ML Application in Cybersecurity Hazard Recognition: Challenges, Opportunities, and Future Perspectives in Ethiopia, Horn of Africa. In S. N. Mohanty, S. Satpathy, M. Yang, & D. K. Vali (Eds.), *Protecting and Mitigating Against Cyber Threats*. Wiley. <https://doi.org/10.1002/9781394305216.ch28>
3. Fakunle, S. O. (2025). AI-Enabled cybersecurity and its influence on organisational performance in the financial services sector: an empirical investigation. *International Journal of Contemporary Economics and Social Sciences*, 12(3). <https://doi.org/10.22399/ijcesen.5009>

4. Lemos, R. (2025, August 6). With Eyes on AI, African Orgs Push Security Awareness. *Dark Reading*.
5. Tariq, S., Ali, N., & Sadiq, M. N. (2025). Threats in adopting financial technologies: Unlocking the role of technological literacy. *Business Review*, 20(2), 1-21.
6. Internet Governance Forum. (2025). IGF 2025 Open Forum #3: Cyberdefense and AI in developing economies. [Intgovforum.org](https://intgovforum.org).
7. Jones, D., & Smith, J. (2018). Data security and consumer trust in FinTech innovation in Germany. *Journal of Financial Innovation*, 4(2), 78-95.
8. Davies, D. (2026, April 1). Nigerian cyber security expert highlights Africa's AI shortfall. *Ghana News Agency*.
9. McCulloch, S. (2025). Cloud Computing Adoption and Sustaining Strategies for a Texas Financial Institution (Doctoral dissertation). Walden University.
10. Okonji, E. (2026, January 8). Report: AI-driven Cyber Threats Outpacing Africa's Defence Capabilities. *THISDAYLIVE*.
11. Africa Cybersecurity Resource Centre. (2023). Annual Report on Cyber Resilience in African Financial Institutions. *ACRC*.
12. West African Economic and Monetary Union. (2024). Interoperability Framework for Digital Financial Services. *UEMOA*.
13. Bank of Ghana. (2026). Cyber and Information Security Directive (CISD 2026). *Bank of Ghana*.
14. International Finance Corporation. (2024). Cybersecurity for Financial Inclusion: A Guide for Microfinance Institutions. *IFC*.
15. World Bank. (2024). Digital Financial Services and Financial Inclusion in Africa. *World Bank Group*.

16. European Union Agency for Cybersecurity. (2025). AI and Cybersecurity in Financial Services. *ENISA*.
17. United Nations Capital Development Fund. (2024). Digital Financial Services and Cyber Resilience. *UNCDF*.
18. Nsaibia, A., & Mounji, A. (2023). Cybersecurity Challenges in African Financial Institutions. *Journal of African Business*, 24(3), 412-429.