AI-POWERED INCIDENT RESPONSE MODEL FOR DIGITAL FINANCE IN ZAMBIA

Amohelang Marry Ntjanyana*, Alice P. S. Shemi†
*MSc Student, Department of Computer Science, School of ICT,
The Copperbelt University, Zambia
Email: amohelangntjanyana@gmail.com

†Senior Lecturer and Supervisor, Department of Computer Science, School of ICT,
The Copperbelt University, Zambia
Email: shemiap@gmail.com

Abstract

Zambia's digital finance ecosystem including mobile money, fintech platforms, and online payments has expanded rapidly, raising exposure to fraud, insider compromise, and data breaches. Current incident response remains reactive and human dependent, leading to delayed containment. This study relies exclusively on secondary data; peer-reviewed research, industry reports, and policy frameworks to propose a contextualized, AI-powered incident response model for Zambia's financial sector. The framework integrates machine learning into existing Security Information and Event Management (SIEM) workflows, emphasizing modularity and phased adoption. Synthesized evidence highlights gains in detection accuracy and response speed, while also identifying challenges in data availability, organizational trust, and regulatory clarity. The main contribution is a secondary data-driven conceptual architecture designed for resource-constrained contexts, providing a foundation for pilot evaluations and regulatory engagement. This work contributes to building resilient digital finance systems in Sub-Saharan Africa.

Index Terms - Artificial Intelligence, Incident Response, Digital Finance, Cybersecurity, Zambia, Sub-Saharan Africa

I. INTRODUCTION

Zambia's financial sector is undergoing rapid digitization through mobile money, fintech services, and online transactions, improving inclusion yet widening the attack surface for adversaries [1], [2]. Common incidents include SIM-swap fraud, phishing, account takeover, and unauthorized access to payment platforms. In many institutions, incident response (IR) is manual and reactive, which struggles against high- velocity threat.

Global literature shows Artificial Intelligence (AI) can automate detection and triage, reduce analyst burden, and cut response latency [3]–[5]. However, most implementations assume well-resourced environments, abundant labeled data, and stable governance. This paper responds by proposing, from secondary sources only, an AI-powered incident response framework adapted to Zambia's resource and regulatory context.

II. RELATED WORK

Surveys of ML for intrusion detection report strong performance for anomaly and misuse detection across sectors [3]. More recent reviews emphasize AI's ability to detect zero-day behavior and reduce alert fatigue [4], [5]. Policy and sector guidance in the region highlight cybersecurity modernization needs and governance considerations [1], [2], [6]. A clear gap remains: few studies translate global AI-powered incident response practices into localized, resource-conscious frameworks for Sub-Saharan financial systems.

III. RESEARCH METHODOLOGY

A design science approach grounded entirely in secondary sources is adopted:

Systematic Literature Review: AI-powered incident response and anomaly detection in finance/cybersecurity.

Comparative Benchmarking: Reported performance and properties of Random Forests, Gradient Boosting, and Neural Networks.

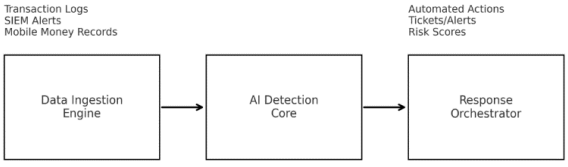
Contextual Mapping: Alignment with Zambia's ecosystem using Bank of Zambia guidelines and regional policy reports [1], [2], [6].

Framework Development: A modular architecture suitable for incremental adoption and data constraints.

No interviews, surveys, or proprietary datasets were collected; all claims derive from published sources.

IV. PROPOSED SYSTEM DESIGN

Fig. 1. Conceptual AI-powered incident response model for Zambia's digital finance sector.



 ISBN: 978-9982-95-500-3

A. Data Ingestion Engine

Aggregates transaction logs, authentication events, SIEM alerts, and-where feasible-mobile money telemetryD. Preprocessing covers normalization, feature extraction, and simple privacy-preserving transformations

B. AI Detection Core

Implements supervised/unsupervised routines for anomaly scoring. Ensemble methods (Random Forest, Gradient Boosting) are favored due to strong reported accuracy (90–97%) and robustness in mixed-feature settings [4], [5]. Where labeled data are scarce, semi-supervised and thresholder anomaly scoring can bootstrap detection.

C. Response Orchestrator

Automates triage and escalation using a hybrid severity–business-risk score. Integrations include ticketing, containment playbooks (e.g., credential reset, session revocation), and analyst feedback loops for continuous improvement.

V. FINDINGS FROM SECONDARY DATA

Synthesis of prior work suggests three themes:

Effectiveness: AI-powered models frequently surpass static/rule-only baselines, reporting 90–97% anomaly detection accuracy and reduced mean time to respond (MTTR) [4], [5]

Operational Benefits: Automated prioritization and deduplication mitigate alert fatigue and focus analyst effort.

Constraints: Data scarcity, limited trust in automated actions, and evolving governance remain adoption barriers in Sub-Saharan contexts [2], [6]

VI. DISCUSSION

Opportunities include strong policy momentum, a growing digital finance user base, and the ability to leverage proven AI methods without wholesale system replacement. Key constraints are infrastructure variability, shortage of labeled local datasets, and regulatory clarity for AI-in-the-loop decisions. A phased strategy is recommended: (i) instrument data ingestion and baselines, (ii) pilot ensemble anomaly detection with open/synthetic data, (iii) integrate explainable AI (XAI), and (iv) co-develop governance with regulators.

VII. CONTRIBUTION AND FUTURE WORK

This paper contributes a secondary-data-driven, context-aware AI-powered incident response architecture for Zambia, consolidating global evidence into a practical, modular design for resource-constrained settings. Future work will include pilot evaluations with anonymized datasets, XAI for analyst/regulator trust, and impact assessments on MTTR and loss avoidance. In addition, collaboration with the Bank of Zambia and regional regulators will be critical to ensure adoption aligns with evolving governance frameworks.

VIII. CONCLUSION

AI-powered incident response can strengthen cyber resilience in Zambia's digital finance by improving detection accuracy and response speed while reducing analyst burden. A staged path grounded in secondary evidence aligned with governance can enable responsible adoption and lay the foundation for empirical validation and scale-out.

REFERENCES

[1] Bank of Zambia, "National financial cybersecurity guidelines," Regulatory Guidance, Lusaka, 2023.

[2] International Monetary Fund, "Digital finance and cybersecurity risks in emerging markets," Washington, DC: IMF, 2022.

[3] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cybersecurity intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[4] A. Khan, S. U. Rehman, A. Z. Khan, and M. F. U. Rehman, "A comprehensive review of AI-based intrusion detection systems," Preprint/Technical Report, 2023.

[5] A. Patel and S. Kumar, "Advancing cybersecurity: A comprehensive review of AI-driven intrusion detection systems," Journal of Big Data, vol. 10, no. 1, pp. 1–23, 2024.

[6] African Union, "Continental cybersecurity strategy for Africa," Addis Ababa: AU, 2022.

 ISBN: 978-9982-95-500-3