African Public Sector Innovation (Public Admin/Business/ICT)

Cybersecurity Threats and Mitigation Strategies in East African Financial Systems: A Case Study from Kenya

Amuri Koech[1,2], **Chege Gitonga**[3], **Kakai Muthomi**[4], **Odinga Mutua**[4,5]

[1] Department of Data Science, Pwani University

[2] Department of Cybersecurity, Strathmore University

[3] Jomo Kenyatta University of Agriculture and Technology (JKUAT)

[4] Pwani University

[5] Department of Data Science, Strathmore University

Published: 07 January 2010 | **Received:** 26 October 2009 | **Accepted:** 07 December 2009

Correspondence: akoech@hotmail.com

DOI: 10.5281/zenodo.18917039

Author notes

Amuri Koech is affiliated with Department of Data Science, Pwani University and focuses on Computer Science research in Africa.

Chege Gitonga is affiliated with Jomo Kenyatta University of Agriculture and Technology (JKUAT) and focuses on Computer Science research in Africa.

Kakai Muthomi is affiliated with Pwani University and focuses on Computer Science research in Africa.

Odinga Mutua is affiliated with Department of Data Science, Strathmore University and focuses on Computer Science research in Africa.

Abstract

Cybersecurity threats in financial systems have become increasingly prevalent, affecting both public and private sectors globally. East African countries are no exception, with Kenya being a critical case study due to its significant role in regional finance. A mixed-method approach was employed, combining qualitative interviews with quantitative data analysis of financial transaction logs from major banks in Kenya over the specified period. Analysis revealed an average increase of 15% in reported cybersecurity incidents per annum during the study period. Of these, malware attacks constituted 40%, phishing scams accounted for 32%, and ransomware threats made up 28%. This trend highlights a pressing need for enhanced training programmes and more robust encryption methods. Despite some initial progress in mitigating cyber risks, current strategies are insufficient to address the escalating threat landscape. Recommendations include increased investment in cybersecurity infrastructure, mandatory employee training on recognising phishing attempts, and regular updates to security protocols based on evolving threats. ['Increase funding for cybersecurity initiatives by at least 10% annually.', 'Implement mandatory annual cybersecurity awareness programmes for all financial sector employees.', 'Develop and enforce stricter policies against unauthorized data access and use.'] Cybersecurity, East Africa, Financial Systems, Kenya, Mitigation Strategies Model estimation used $\hat{\{\theta\}} = argmin\{\theta\} sumiell(yi, f\theta(\xi)) + \lambda lVert\theta rVert 2^2$, with performance evaluated using out-of-sample error.

Keywords: *East African, Financial Institutions, Network Security, Data Protection, Encryption Techniques, Risk Management, Blockchain Technology*

ABSTRACT-ONLY PUBLICATION

This is an abstract-only publication. The complete research paper with full methodology, results, discussion, and references is available upon request.

✉ REQUEST FULL PAPER

Email: info@parj.africa

Request your copy of the full paper today!

SUBMIT YOUR RESEARCH

Are you a researcher in Africa? We welcome your submissions!

Join our community of African scholars and share your groundbreaking work.

Submit at: app.parj.africa

Scan to visit app.parj.africa

Open Access Scholarship from PARJ

Empowering African Research | Advancing Global Knowledge