Leveraging Mobile Money for Inclusive e-Government Services in Sub-Saharan Africa

***Abstract*—The rapid adoption of mobile money services (MMS) in Sub-Saharan Africa presents an opportunity to enhance e-Government accessibility despite low internet penetration. We propose leveraging mobile money authentication (MMA) as an alternative to Single Sign-On (SSO) solutions for online services. Through simulations and comparative analyses, we evaluated MMA against criteria including security, accessibility, user experience, cost, and scalability. Our findings show that MMA excels in limited-connectivity regions by leveraging multi-factor authentication through Subscriber Identity Module (SIM) and Personal Identification Number (PIN), reducing exposure to phishing and brute-force attacks. Our simulations revealed that MMA takes an average of 8 seconds for a single session, with a success rate of 95% under optimal conditions. In contrast, OAuth-based SSO systems required 12-15 seconds on average to authenticate and achieved a lower success rate of 80%, largely due to the dependence on a stable internet connection and the increased risk posed by malicious phishing attacks. Our proposed approach aligns with regional technological ecosystems and user behaviors, significantly advancing digital inclusion in Sub-Saharan Africa (SSA). This work provides a novel and scalable approach for a seamless authentication experience for underrepresented groups in rural settlements, contributing to the larger goal of narrowing the digital infrastructure divide in the global South.**

***Index Terms*—Mobile Money Authentication (MMA), e-Government, Sub-Saharan Africa, Multi-Factor Authentication, USSD, Single Sign-On (SSO)**

I. Introduction

Sub-Saharan Africa faces significant challenges in digitizing essential services due to sparse internet infrastructure and low digital literacy, especially in rural areas. While internet penetration remains low, mobile phone ownership has reached 43% of the population, and mobile money services have become integral to daily financial transactions [1], [2]. This research explores how leveraging the ubiquity and security of MMS can provide a more inclusive, secure authentication mechanism for e-Government services [3].

II. System Design and Methodology

We designed a simulated e-Government platform integrating MMA, utilizing a front-end developed in React.js and a Node.js back-end, with secure communication via AES-256 encryption. The authentication flow (see Fig. 1) involves user initiation, USSD push notification, PIN entry, and SIM verification through a simulated Mobile Network Operator (MNO). Upon successful authentication, a JSON Web Token (JWT) is issued for session management. Comparative analyses were conducted against a traditional email-based SSO system, with both approaches evaluated for temporal performance, security robustness, usability, and scalability. Table I summarizes the average time for each authentication step.

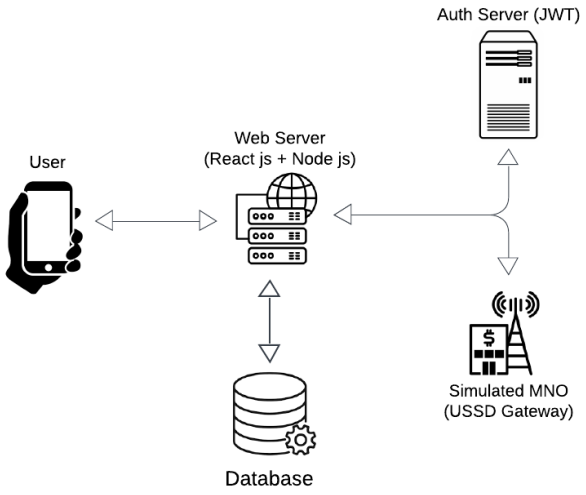

Fig. 1: Our Proposed Web Platform Architecture for Single Sign On via Mobile Money.

III. Results

MMA achieved an average end-to-end authentication time of 8.0 seconds, outperforming email-based SSO (12–15 seconds). Security testing (Table II) demonstrated MMA's resilience to man-in-the-middle and brute-force attacks, with session integrity maintained in 98.5% of network disruption scenarios. Usability assessments (Table III) indicated high user satisfaction, especially among low-literacy users, due to the numeric USSD interface and support for local languages. MMA's accessibility, device compatibility, and minimal internet requirements (Table IV) surpassed OAuth, which is limited to smartphones and stable internet access. Cost analysis (Table VII) showed minimal user charges and moderate provider implementation costs, leveraging existing infrastructure.

TABLE I: Security Testing Results for Mobile Money Authentication.

Attack Type	**Outcome**
Man-in-the-Middle (MITM)	Prevented using encrypted communication (AES-256).
Brute Force (PIN Guessing)	Account locked after 3 incorrect attempts.

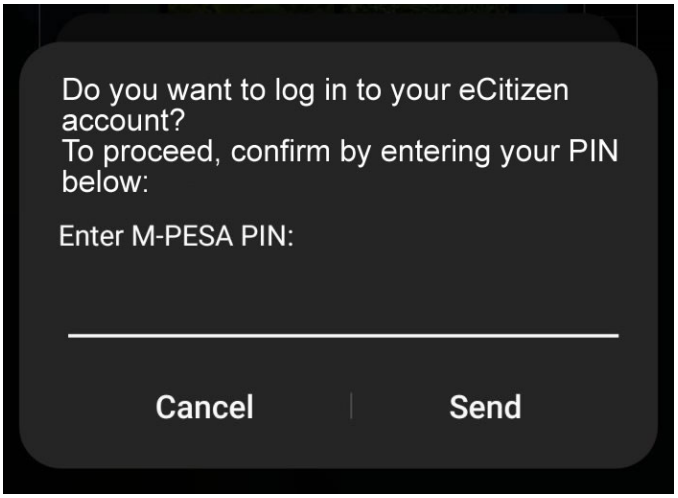

Fig. 2: Sample Kenya M-Pesa Prompt for Our Architecture.

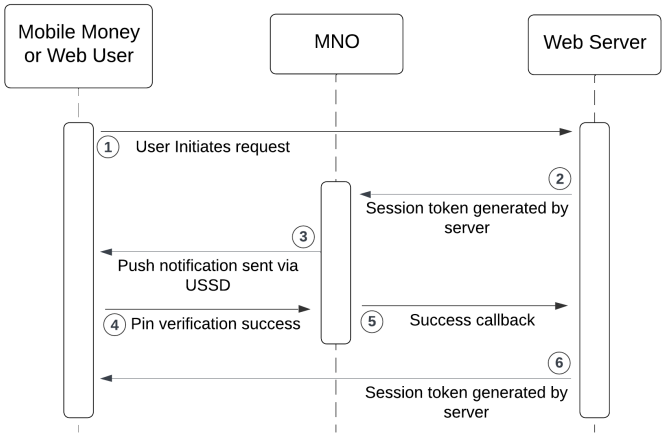

Fig. 3: Authentication Sequence.

TABLE II: User Interaction Metrics for Mobile Money Authentication.

Metric	**Result**
Average Authentication Time	14.5 seconds
Max Delays under Poor Network	20 seconds
Failed Login Attempts (Lockout)	Account locked after 3 incorrect PINs.

TABLE III: Comparison of Security.

Feature	**MMA**	**Email SSO**
Multi-Factor Auth	Inherent (SIM + PIN)	Optional
Phishing Resistance	High	Low
Account Recovery	Via MNO (high security)	Email-based (*SPOF)
*SPOF: Single Point of Failure		

IV. Discussion

Mobile money authentication (MMA) demonstrates strong potential to address critical gaps in security and accessibility for e-Government platforms in Sub-Saharan Africa, leveraging inherent multi-factor authentication and offline capabilities to align with regional user behaviors and technological realities. However, while the simulation results highlight MMA's technical and operational advantages, there remains a need to further examine the usability implications, particularly concerning user privacy and security perceptions in real-world contexts.

Future work will focus on deploying the MMA prototype with targeted user groups to empirically assess its effectiveness, usability, and acceptability among diverse populations. This next phase will involve field testing in representative communities, gathering user feedback on privacy concerns, authentication experience, and potential barriers to adoption. Insights gained from real-world deployment will inform iterative refinements to the authentication framework, ensuring that it not only meets technical requirements but also aligns with the lived experiences and expectations of end users.

V. Conclusion

Mobile money authentication offers a transformative, inclusive, and secure alternative to traditional web authentication for e-Government services in Sub-Saharan Africa. Its demonstrated advantages in accessibility, security, and user experience make it a compelling framework for bridging the digital divide and advancing secure digital service delivery in resource-constrained settings.

References

[1] "The mobile economy sub-saharan africa 2023." Accessed: Jan. 04, 2025. (2024), [Online]. Available: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/11/GSMA_ME_SSA_2024_Web.pdf.

[2] E. L. C. Osabutey and T. Jackson, "Mobile money and financial inclusion in africa: Emerging themes, challenges and policy implications," *Technological Forecasting and Social Change*, vol. 202, p. 123 339, May 2024. DOI: 10.1016/j.techfore.2024.123339.

[3] A. Armando, R. Carbone, L. Compagna, J. Cuellar, G. Pellegrino, and A. Sorniotti, "An authentication flaw in browser-based single sign-on protocols: Impact and remediations," *Computers & Security*, vol. 33, pp. 41–58, Mar. 2013. DOI: 10.1016/j.cose.2012.08.007.

Carnegie Mellon University Africa

LEVERAGING MOBILE MONEY AUTHENTICATION FOR INCLUSIVE E-GOVERNMENT SERVICES IN SUB-SAHARAN AFRICA

Oluwole Adewusi[1] Wallace Msagusa[1] Jean Pierre Imanirumva[1] Okemawo Obadofin[1] Jema David Ndibwile [1]
[1] Carnegie Mellon University Africa

Background

"By 2024, mobile phone ownership in sub-Saharan Africa had increased to approximately 43% of the population, equating to around 534 million." ~ **GSMA State of the Industry Report, 2024**

Digital Divide Paradox: 43% mobile phone ownership (534 million people) vs. significantly lower internet penetration. Out of the 4.61B people with access to mobile internet worldwide, only 320m (approx. 7%) are from the SSA.

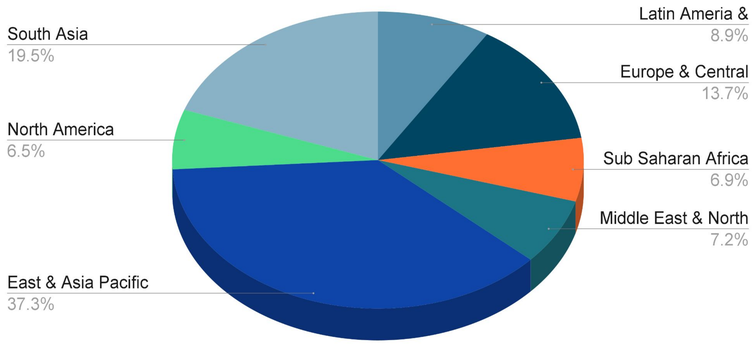

***Fig**: Mobile Internet connectivity by region, GSMA*

Mobile Money Adoption: Widespread use in East African countries like Kenya, Tanzania, Rwanda, and Uganda providing secure transaction platforms.

Authentication Challenges: Traditional methods, e.g., OAuth fail in areas with unreliable connectivity and limited cybersecurity infrastructure.

Ground Truths

- Traditional web authentication methods often do not meet the needs of users in many parts of SSA.
- Vulnerable populations in rural and underdeveloped areas where unreliable internet connections and limited infrastructure make these authentication techniques not viable.

Challenge

How can users ensure secure, accessible, and user-friendly authentication methods that align with local technological realities and user capabilities.

Our Solution

Our approach simulates a real-world mobile money authentication within an e-Government framework through a custom web platform that replicates interactions between users, authentication systems, and mobile network operators. The architecture integrates components via a secure communication channels to evaluate performance under varying connectivity conditions typical of Sub-Saharan Africa.

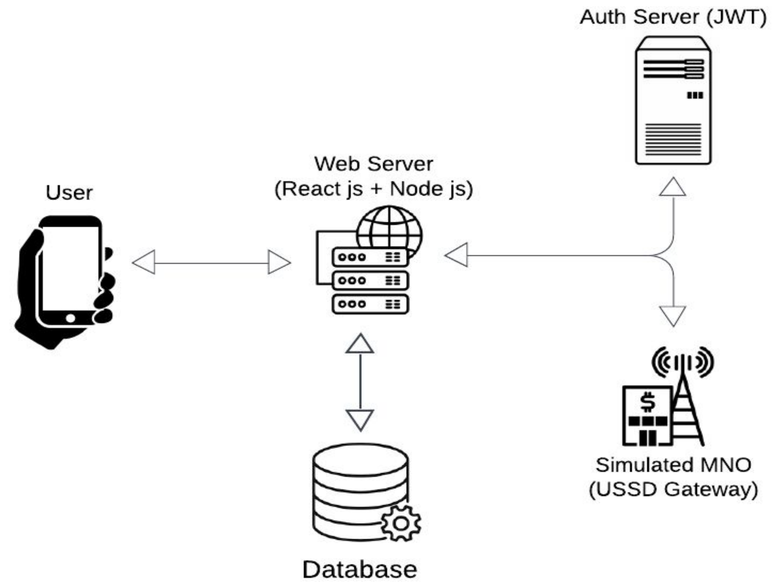

Fig: System Architecture Diagram

Authentication Flow:

1. User initiates request (1.2 sec)
2. Backend generates session token
3. Mobile Network Operator (MNO) sends USSD push notification
4. User enters PIN (5.7 sec)
5. PIN verification and JWT generation (1.1 sec)

- **Duration : 8.0 seconds (Approximate)**

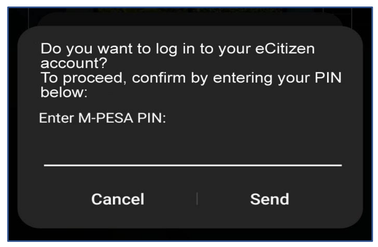

Fig: USSD push notification

UPANZI DIGITAL PUBLIC INFRASTRUCTURE NETWORK

Results

Performance Metrics Table

Metric	Mobile Money Auth	Email SSO
Authentication Time	8.0 seconds	12-15 seconds
Success Rate	95 %	80% (connectivity issues)
Security Incident Rate	0.1%	0.5%

Comparative Analysis MMA VS Email SSO

Criteria	MMA	Email SSO
Accessibility	No Internet required (USSD-based)	Require internet connection
Security	Inherent MFA (SIM + PIN) high phishing resistance	Optional MFA, vulnerable to phishing attack
User experience	Familiar interface, supports local languages	More steps , text-heavy interface and limited language support
Cost and Scalability	Leverage existing infrastructure, medium cost	Low implementation cost , limited reach

Mobile Money SSO Authentication provides:

- Enhanced security through inherent multi-factor authentication
- Superior accessibility in low-connectivity environments
- Alignment with regional technological ecosystems
- Significant advancement in digital inclusion for the underrepresented population

Future Research

- Testing PIN verification techniques that incorporate device fingerprinting to mitigate SIM swap vulnerabilities
- Conduct real-world field tests and user studies to evaluate acceptability, usability and perceived privacy/security
- Develop a detailed, scalable cost model

References

[1] The mobile economy sub-saharan africa 2023. Accessed: Jan. 04, 2025. (2024).
[2.] E. L. C. Osabutey and T. Jackson, “Mobile money and financial inclusion in africa: Emerging themes, challenges and policy implications,” Technological Forecasting and Social Change.