Abstract

Security is a leading factor for establishing and maintaining customer trust in mobile money services (MMSs). MMSs in Tanzania rely on the use of Personal Identification Number (PIN) as an authentication method. However, a PIN can be easily guessed, forged or misused. This paper explores security challenges in MMSs and weaknesses associated with the current Mobile Money Authentication (MMA) method. Further, the study proposes the use of two-factor authentication model as an alternative method. The proposed model combines the current approach of using PIN and adds another layer of security that uses fingerprint recognition technology. Evaluation of the proposed model shows that it mitigates security vulnerabilities that exist in the current MMA method.

References

- Alex Dobie. How to Tell If Your Samsung Phone is Vulnerable to Today’s USSD Hack. Android Central, Retrieved 20 September 2014.
Improving Mobile Money Security with Two-Factor Authentication


- Smartphone: Information security risks, opportunities and recommendations for users, ENISA Report (December 2010).
- Bauckman, Dena Terry, Nigel Paul Johnson, and David Joseph Robertson. 
- B. Schneier. "Two-Factor Authentication: Too Little, Too Late." In Inside Risks 178, 
- T. Venkat NarayanaRao, Vedavathi K. Authentication Using Mobile Phone as a Security 
- Shon, T. H., & Swatman, P. M. C. Identifying effectiveness criteria for Internet 
- Nadarajah Manivannan, Celalettin Tigli, Azad Noor, Shahzad Memon. Fingerprint 
  Biometric for Identity management. International Journal of Industrial Engineering and 
  Management (IJIME), Vol. 2 No 2, pp. 39-44, 2011

Index Terms

  Computer Science         Security

Keywords

  Authentication  Biometric  Fingerprint  Mobile Money Services  PIN  Two-Factor Authentication