International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 1, pp 68-76, January-2022

https://doi.org/10.47001/IRJIET/2022.601014

An Integrated Mobile Identity Authentication Model

[1]Abwao Donatus, [2]Abeka Silvance, [3]Agola Joshua

[1,2,3]Jaramogi Oginga Odinga University of Science and Technology, Kenya
Authors Email IDs: [1]dabwao@jooust.ac.ke , [2]silvancea@jooust.ac.ke, [3]sagola@jooust.ac.ke

***Abstract* - Theft of personal identity is an unlawful act, a criminal in this case possesses or attempts to be in possession of an identity of a victim without their knowledge nor consent. Mobile identity theft the problem that inspires this study is just one of the types of identity theft and refers to having control of a mobile subscriber identification through SIM card registration and replacement services again without the authority of the sole owner. This study provides a solution to solve a gap that is addressed by empirical studies from both academia and the industry for a problem that researchers feel should be a none issue in the twenty first century. The study besides interprets the course of mobile identity theft problem going by the literature reviewed to be orchestrated by criminals who leverage vulnerabilities at Subscriber Identity Module registration and replacement processes. The study then proposes, develops and tests an integrated authentication scheme based on existing models and inspired by theory of human identification to hypothesize that addition of Integrated population registration records would mitigate the problem.**

The simulation process of the proposed model is guided by an algorithm that employs a formula which determines strength of authentication score, using data generated by constructs of the scheme various results provide clarification on the safety of the model when various parameters are changed. The study observer's a maximum authentication score at 96.43% when level of security is highest for all parameters in the new authentication model against that of 95.37% when security levels of the current authentication model are highest. The study hereby confirms that highest level of authentication can be achieved by introducing an integrated population records to the already existing authentication model while their levels of security are maximum.

Keywords: SIM Card – Subscriber Identity Module, Integrated authentication model, Mobile network operator, ATM – Automatic teller machine.

I. INTRODUCTION

Mobile Identity theft is a problem that is currently in the public domain and an issue that is observed amongst academic scholars whose interest fall within the telecommunications, cyber security and relevant domain. In the public domain, the problem is on the rise with statistics and supporting studies citing overwhelming evidence on theft, how it has metamorphosized and mitigation initiatives trying to curb the issue. Several research outputs, observation reports and industry initiatives have reported the problem and trying to put forward diverse solutions to help.

An Australian empirical output in which 211 theft cases related to identity theft reveals lack of coordination in the response system dealing with threat mitigation, a national Identity and cybercrime support service initiative [1]. An empirical study that determines compromise types related to identity theft and as to whether majority of the respondents are unaware of how their details are compromised reveal that 31% of the cases are mobile number related cases [2]. Mobile Identity theft come in complex scenarios given the emergence of vast technology for various services with the demanding needs for customers and thirst for entrepreneurship, different businesses want a level playing field with innovation at hand. A typical example is Unstructured supplementary services data (USSD) which is a menu based and real-time mobile based electronic service that facilitates access to various services has been reportedly noted to have a number of challenges and the same USSD service is also reportedly used by fraudsters to commit identity theft through Subscriber Identification Module (SIM) swap, phone theft and kidnap, in other cases funds in the bank [3]. As the author continues to narrate the story of malicious actions of criminals who manipulate a currently weak authentication service in the USSD service that used by the ATM through use of PIN concludes that compromises the ATM channel and violates one of the stated guidelines for USSD operation in Nigeria [3].

In Kenya recent studies reveal a number of mobile identity thefts. A case study that identifies various systems that support electronic means of money transfer, their effects on profitability, liquidity and the business network of financial institutions finds the main challenge to be security issues particularly theft of mobile identity and money laundering while blaming it on the sophisticated technology [4].

Efforts to address cases of identity stealing that are mobile related is first addressed in a proposal that develops a methods of early detection and prevention of identity theft in which the author argues that when use of identity is attempted, a record