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

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

associated with the identity is retrieved and a request sent to the registered mobile device for location information verification (Dustin & Bruce, 2003).

In a separate proposal that attempts to address MIT develops an enacted view on mobile identity management with an opinion that MIM play an important role in addressing usability and trust issues in mobile business growth. The author in the development feels that MIM should be used to identify, acquire, access and pay for services that follow the user from device to device, location to location and context to context [5].

Other efforts to address identity theft is supported by theory of human identification in which the author describes as the association of verification data with a particular human being and identifies three basic means for making human identifications namely; knowledge-based identifications, token-based identifications and biometric identification [6]. Despite the fact that certain constructs within this theory have been implemented in majority of MNO's for authentication of customer identity, perpetrators of mobile phone identity theft still innovate around the weaknesses of the authentication system and are able to get away with stolen mobile phone identities. In this regard, this research extends a currently existing authentication model, adds, Integrated population registration records and inspired by theory of human identification to the problem of mobile phone identity theft of the current age.

II. CURRENT MOBILE AUTHENTICATION MODELS

Adversary model for computer device authentication

A review study that analyzes various mobile authentication models, classification and comparison between various mobile device authentication models reveals a number of gaps in security of the models and that security protocols in the models lack a comprehensive security analysis. In the model analysis, user-to-device (U2D) authentication is addressed and involves a user authenticating him or herself before accessing mobile device functions [7]. The author acknowledges that U2D authentication is possible by one or combination of four factors, a summary of parameters used in authentication namely:

1) Something a user knows (passwords, PIN codes, graphical patterns, e.t.c)
2) Something a user possesses (hardware tokens, keys, etc)
3) Something a user is (static biometric, e.g. fingerprint, face, iris, hand geometry, vein patterns)
4) Something a user does (dynamic biometric, e.g. gait, handwriting, speech)

The author admits that despite the fact that numerous authentication methods have been proposed for mobile devices, none has been established as a canonical U2D authentication.

While dig deep in the models review study and considering authentication on mobile devices in particular, the focus on the individual threats seem to match this study; the author cites brute-force, password guessing, installing malware and hardware-level exploits to bypass authentication just to mention a few. The application of the models' review to this work is significant bearing in mind that the study points out explicitly the key factors that enable authentication, this study is persuaded to pick these as the key constructs of the study even though it is supported by the theory of human identification [8].

Mobile payment authentication model

A study admits that human behavior characteristics or how different people conduct themselves is unique and very difficult to reproduce hypothesizes that none of existing research has considered the influence of user posture on users' gesture behavior authentication [9]. The study monitors user's gesture behavior overtime and based on authentication system architecture reveals that it is possible to monitor from a user login to the entire usage process for improving the payment of mobile devices by using authentication and continuous authentication comprehensively. I tend to agree with the authors effort in developing the model to consider human gesture, however this does not is not give a generic flow to as considered in an empirical study which acknowledges that it is a challenging task to have gesture security given the complex of its usability [10]. Additionally, while the author apparently uses "user IS" as a means of authentication token all through the study it is still falling short of three other modes of authentication contexts as identified in the base model of this study; user does, user knows and possess. It is worth considering that the complexity of this authentication mode is only workable in a smart mobile device as explained by the author who may not be convenient for those with feature phones and according to CA report 2021 puts it that 20% of Kenyans while 25% of Africans still use feature phones.

A Hybrid blockchain based authentication model for Multi-WSN

A study that analyzes the security and performance of a blockchain based multiple wireless sensor network shows that the model has security that is very comprehensive and with better performance [11]. The study divides the nodes of the proposed Internet of things of authentication model, the blockchain based Multi-WSN model into base stations, cluster head nodes and ordinary nodes according to their capability

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

differences which are formed to hierarchical network. In the construction of the model, various communication nodes are able to sustain mutual authentication in the network, an approach that strengthens and re-assures the security within the nodes. Even though the model improves the security and performance of the communication in a mobile network, the model does not mention the fundamental constructs that guide this research. However, further analysis of the model suggests that the model operates within user possess or knowledge based operational classification context. A deeper understanding according to the technical explanation of the author is that the tokens that are generated for authentication at various nodes is possessed by the various hierarchical authentication level makes the model strong. This study suggests that this approach leaves a gap of more authentication contexts as reviewed in a previous model that suggest four contexts; suffice to suggest that in as much as the model is perceived by the author that it has a comprehensive security and better performance, this study still yarns more of three other authentication operational contexts of user knows, user is and user does that are deemed to improve its strength.

Radio frequency fingerprinting identification scheme

In a review paper where an authentication scheme consisting of light-weight radio frequency fingerprinting combines with a two-layer model is proposed to realize authentications for a large number of resource-constrained terminals under the mobile edge computing (MEC) scenario without relying on encryption-based methods, results indicate that the new authentication scheme can achieve higher recognition rate than that of traditional RFFID method by using wavelet feature effectively enough to realize the efficiency of the model [12]. The author continues that a machine learning algorithm is implemented in the video recognition and that is performed by remote cloud to generate decision models from the features profiled in the model. The author recon that this combination of authentication technique may improve the authentication rate by leveraging on the machine learning training functions together with computing resources supported of the cloud.

Lightweight knowledge-based authentication scheme

A video surveillance study that intends to combine a system based on facial recognition by utilizing CCVT machine learning with radio-frequency identification (RFID) to correct challenges of identifying objects in poor video quality or low level of similarity still find a challenge in producing an accurate facial detection [13].

The fault as reported by the author in the model is realized when face recognition rate in the CCTV does not produce an accurate measurement or correlation with that in the video produced by the CCTV equipment for mobile computing. Elements that justify this phenomenon are profiled by the author citing personal posture, hairstyle, bad weather, facial expression among others including fears of subjecting private information of an object that may present that of a human or something that may lead to erroneous judgement of an object as expressed. This acknowledgement of a gap of this magnitude is not only a hindering factor in considering using the model described here in place, but the complexity of its technical application and environment under which the model is expected to be used leaves nothing much to desire when considering mobile authentication at the processes of SIM card enrollment and replacement.

User Authentication Model for Online Banking System

Review findings from a study that involves a critical outlook of current existing authentication access for users using online banking through mobile phones reveals that whereas current security authentication model uses biometric or PIN as authentication tokens, none of similar authentication model chain propose use of International Mobile Equipment Identity (IMEI) number, a factor that the author perceives to strengthen the security of user authentication [14]. As well put by the author, the IMEI number uniquely identifies mobile phone handsets while adding extra security to online banking security. Another observation by the author puts it that previous studies in the authentication arena have predominantly considered a conventional use of username and passwords, biometrics like fingerprint, facial recognition and notices that online banking authentications where mobile systems are involved would need extra security feature to enhance it. In as much as the author considers that addition of the IMEI number enhances the security in online banking system, this study hypothesizes that an integration of the previously mentioned authentication items mentioned by the author would make a stronger authentication. From the analysis of the adversary authentication models, Usernames and passwords are authentications used in the cluster user knows in their operation scope, biometrics and facial are in the "user is" authentications while IMEI number is in the "user possess" cluster [7]. It therefore means that is it only "user does" constructs in the authentication model for which this study is based on that the author has not considered using. This study hereby takes cognizance of the magnitude of effort the author has put in the model review however, the feeling that more authentication clusters would increase the strength of user authentication has not been fully met by this review.

Authentication scheme for smart mobile devices

A comprehensive investigation that identifies open challenges of authentication schemes for mobile devices

ISSN (online): 2581-3048
Volume 6, Issue 1, pp 68-76, January-2022
https://doi.org/10.47001/IRJIET/2022.601014

classifies authentication models involving smart mobile devices in their context of threat models and reveals five classification categories; identity based attacks, service based attacks, manipulation based attacks, eavesdropping based attacks and combined eavesdropping and identity based attacks [15]. In the same study, the author reviews and gives description of multiple existing threat models to find relevance and whether that can play a contributory element in the mobile authentication, a move that possess challenges in the authentication models as presented below. It is interesting that the model review recognizes and categorizes authentication schemes for smart mobile devices into four classes namely; biometric, channel-based, factors-based and ID-based authentication schemes which somehow resonates with authentication clusters of adversary model for computer device authentication which this study bases its study on whereas this approach the study does not find generic to accommodate non-smart devices.

Mobile based behavioral authentication model

In a model design review study in which a mobile terminal APP browsing behavioral authentication system architecture that synthesizes several factors reveal that the architecture is suitable for users using the mobile terminal APP in the daily life [16]. The author in his explanation mentions that the architecture includes data acquisition, data processing, feature extraction, and sub model training and that the architecture best works in an environment that continuously authenticates a user when using the APP.

Whereas the study explained in the model development addresses the problem faced by challenges of passwords for unlocking mobile devices which are easily stolen and causes serious security problems potentially as revealed by the author, this study addresses mobile identity theft and concentrates at the subscriber authentication process. The study that develops the model explain here as reviewed does not contribute sufficient effort in mitigating the problem that inspires this study even though it seems to be addressing a problem within the mobile authentication domain.

Anonymous identity model, a pseudonym-based scheme for mobile sensing

A proposal that develops an unidentified authentication model that uses assumed names instead of real ones and applied in mobile crowd sensing reveals the effectiveness of the solution which is said to contribute to protection of privacy with regards to the process of authentication by means of a pseudonym [17]. The study develops the model by combining public key infrastructure and combined public key technology to manage key and certificates in solving challenges of large-scale key management. The study evaluates the proposed identity authentication scheme using functional testing and performance testing. I tend to support the author in the study mentioned given the acknowledgement that security and privacy protection as a key area in mobile crowd sensing However, the background of the problem addressed by the author seems to be putting more weight on challenges of mobile crowd sensing whereas this study attempts to solve challenges of mobile identity theft at mobile authentication processes.

Anonymous identity-based model for mobile edge computing

A mobile authentication model development meant to fix challenges of rapid growth and increased user experience needs in mobile edge computing environment proves to be secure and efficient [18]. The model is developed by designing a new architecture for authentication for mobile edge computing environment typically for light-weight devices and comparisons of time consumption from communicational costs provided. The study acknowledges that a computing environment that leverages on mobile edge computing takes into consideration that besides machine-based instructions, secure data storage for users within a range of wireless access network is guaranteed. The study additionally reveals that user anonymity is protected, a virtue that is key in information communication security environment [19].

The study as further elaborated by the author takes a little more step and a comparison of conventional cloud computing and mobile edge computing is done. This provides notable differences in data center, data processing, network bandwidth and scalability.

User authentication model for IOT networks based on app traffic patterns

In a model development study where a user authentication scheme for IoT networks that uses network traffic pattern is developed and when tested, an average F-measure of 95.5% is realized, a deduction that the initiative is promising with effectiveness and usability [20]. The Authors recognizes that access to many Internets of things networks may be done through use of end-user technologies such as mobile phones, tablets which are potentially susceptible to loss and theft and which in turn may pre-dispose them to illicit users accessing valuable information. In this regard, an identity authentication scheme that continuously verifies users in the background overtime is essential and is the backbone of the study as explained by the Author and supported in a smartphone development authentication [21].

ISSN (online): 2581-3048
Volume 6, Issue 1, pp 68-76, January-2022
https://doi.org/10.47001/IRJIET/2022.601014

While the Author considers a continuous authentication model which is validated to be 95.5% effective, its worth considering that the authentication process is on device likely to suggest that this may allow the user to interact with features of the device whereas this study aims at securing user identity at device's service provider interface.

Identity management and authentication model based on redactable blockchain for mobile networks

A proposal which considers mobile users' concerns about losing their personal identity information addresses fears of who can access their sensitive information and susceptibility to compromise by developing a blockchain-based identity management and authentication model for mobile networks and involves an experiment whose results confirm that the model greatly reduces revocation and communication overhead [22].

The Author explains that the model allows users to generate their own self sovereign identities (SSIs) and corresponding public keys and private keys for authentication. That the private key as mentioned authenticates user information only known to a user and that blockchain is used to record SSIs and public keys originating from legitimate user which adopts chameleon has to delete illegal uses information on the blockchain. The security of the model confirms its application to secure and effectiveness. The technical complexity of the model apparently addresses challenges as posed by the author despite the fact the scheme emphasizes on “user knows” as the authentication.

Two factor authentication model for mobile money

A review output that aims at analyzing threat models and their mitigation measures in an authentication scheme that uses two-factor in mobile money identity verification categorizes threat models in the two factor authentication scheme for money into five, namely, attacks against privacy, attacks against authentication, attacks against confidentiality, attacks against integrity and attacks against availability [23].

Additionally, the study reveals there exists a gap to be addressed that amounts from use of personal identification number and subscriber identity module (SIM) to authenticate users which according to the research are susceptible to attacks. The study profiles the processes involved in the authentication scheme and elaborates categorically the enrollment processes, the authentication processes, the vulnerabilities involved and what attack points and goes ahead to provide the mitigation measures of the attack types for the susceptible attack points.

I support the immense work done by the Author after reviewing 97 papers with several related mobile authentication models, revealing the weak points, designing the appropriate vindication measures whilst summarizing the gaps existing however, the author does not seem to mention any integration with external databases containing information that is used by attackers for countercheck especially during authentication.

Theory of Human identification

[8] Defines human identification as “the association of data with a particular human being”. The author identifies three basic means for making human identifications. First, in "knowledge-based" identification, individuals are "recognized by demonstrating that they are in possession of information which only that particular person would be expected to know". Giving examples of such information and contextualizing includes a person's mother's maiden name, the person's social security number, or a password give to them at an earlier time. Second means for making human identification, in "token-based" identification, where persons are recognized by their possession of some items such as their national identity card, a driver’s license or a passport.

The Author argues that each of these tokens contain a description particular to that individual to be identified and that adds an additional degree of security; that an imposter might not be able to use the token because the description in the token would not match the imposter’s persona. Third means of human identification is "biometric" identification which refers to “a variety of techniques which are based on some physical and difficult-to-alienate characteristics." The Author adds that this includes descriptions of appearance, measurements of social behavior or bio-dynamics, retinal scans, DNA patterns and "imposed physical characteristics" such as brands, bracelets and anklets, embedded micro-chips and transponders.

This theory inspires the study given that its constructs are similar parameters used in the current customer authentication. Additionally, the theoretical constructs as explained are similar to the constructs whose models are reviewed which are hypothetically enhanced to produce an integrated model as mitigation to the current mobile identity problem.

KENYA Integrated Population Registration Records (K-IPRS)

A digital national population register referred to as Integrated population registration system is a central database that brings together over a dozens of databases held by various government agencies on population recording, national identification records among others [24]. The author further explains that IPRS combines data from birth and death

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

register, citizenship register, ID card register, aliens register, passport register, and the marriage and divorce register. The birth and death register has all the information of the registration details on births and deaths in Kenya.

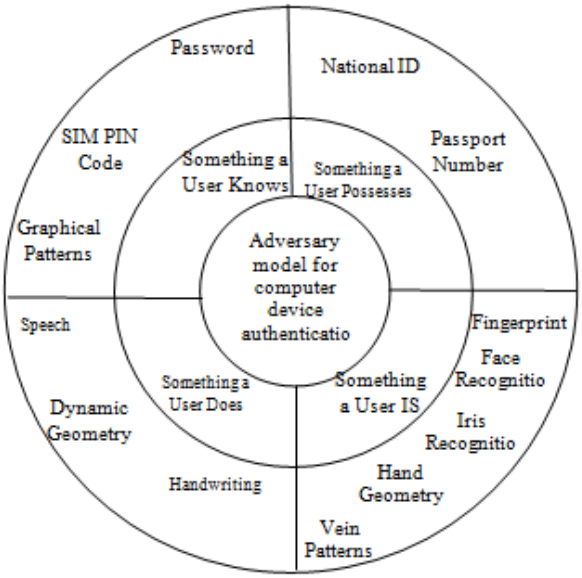
Contribution of integrating this component into an authentication model will filter any attempts by perpetrators to acquire irregular identities through SIM registration and replacement. This would then play a very important role in authenticating wrong information within the process of acquiring mobile phone identity thus making sure that legitimate owners have the so said identities.

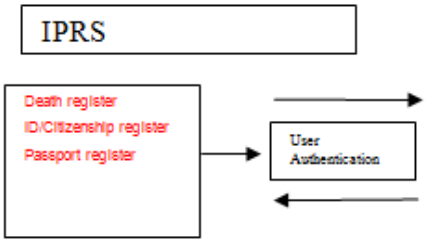
Additionally the so provided information is very relevant for a more secure mobile customer identity validation for a player who is out for a precise validation process and if telecommunication companies will integrate its databases with the integrated population registry in Kenya, then it is undisputed that Kenya will successfully mitigate mobile identity theft and online fraudsters by ensuring that only those validated against the integrated system, IPRS acquire identity profiles with the MNOs and that nobody can illegally or unlawfully own and use a mobile phone identity of someone else. This would be applied on SIM SWAP as well, another process that is used by criminals to steal mobile phone identities for illegal activities.

III. CONSTRUCTION OF THE INTEGRATED MOBILE AUTHENTICATION MODEL

The conceptual design borrows from Adversary model for computer device authentication which states that a user to user authentication is possible by one or combination of four factors namely (1) something a user knows (passwords, PIN codes, graphical patterns, e.t.c), (2) something a user possesses (hardware tokens, keys, etc), (3) something a user is (static biometric, e.g. fingerprint, face, iris, hand geometry, vein patterns), (4) something a user does (dynamic biometric, e.g. gait, handwriting, speech) and tow factor authentication model and is supported by the theory of human identification which proposed that the identification process is determined by the three variables namely knowledge based authentication, token based authentication, bio-metrics authentication used by existing systems and adds Integrated Population Records, which according to the research is also a factor hypothesized to be a contributory factor towards the integrated mobile authentication model to mitigate the problem of mobile phone identity theft.

IV. THE INTEGRATED MOBILE IDENTITY AUTHENTICATION MODEL





V. FORMULAS

Formulas and equations should be centered and numbered consecutively.

The authentication strength is calculated by a formulae that expresses the Strength of authentication score = $\sum_{n=1}^{m}(C_n V_n)$ which details a weighing system C□ and scoring mitigation strategies for each vulnerability point V□ s [25].

Implementation of the formulae in determining the strength of the authentication in the current model.

Percentage of authentication in relation to vulnerability susceptibility can now be calculated as $\left(\sum_{n=1}^{m}(C_n V_n)\right) * 100$

VI. PROGRAM CODE

```
function
strengthAuth(scoremitign,weighratio)

{
```


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

```
    $scoreval = '';

      $('.cu-
mid','.authstrength.'+"userknows").
computeval                    (vulnerablevul
*succeptibilityratio);

   $('.cu-mid','.
authstrength.'+"useris").computeval(vulne
rablevul * succeptibilityratio);

   $('.cu-mid','.
authstrength.'+userdoes).       computeval
(vulnerablevul* succeptibilityratio);

   $('.cu-mid','.
authstrength.'+userpossesses).  computeval
(vulnerablevul* succeptibilityratio);

}
```

VII. COMPUTATIONS OF THE STRENGTH OF AUTHENTICATION SCORE

Determining the strength of authentication score for different scenarios provides results from

Simulation of the existing scheme at nominal:

This test exercise involves computation of the strength of authentication score at vulnerable SIM-card mounting points with the following results: (user knows =0) + (user possess =0) + (user does =0) + (user IS=0) to get the sum of the authentication strength score = 0

This result results at nominal has an authentication strength scoring zero, this applies for both current and integrated schemes which mean that both authentication models have to function at some substantial or absolute value injection but not nominal.

Simulation at absolute level: this test procedure involves a mockup test of the schemes with considerable values which reveals a 40.5% of the strength in the current schemes whereas 43.75% authentication score in the new integrated model is realized.

The contribution of the integration of population record systems to the current schemes can be seen to realize an increase in strength of authentication score by 3.25%, an improvement from what we have currently.

Test at absolute level of security reveals a 96.43% in the integrated scheme and a 95.37% in the current scheme.

The revelation that the new authentication scheme in an overall test produces as increase on authentication score by 1.06%. Shows that the tested model has some significant change in the current scheme to contribute to mitigation of the challenges of the current scheme as revealed by gaps existing in literature review.

VIII. DISCUSSION AND CONCLUSION

Assessment of mobile identity theft at subscriber identity module security processes

This discussion builds from the test results of the current existing customer authentication schemes. The strengths and weaknesses of the current authentication model affects security of the SIM card security processes involved at registration and replacements. The susceptibility of the identity theft at these processes is a factor of the vulnerability of the factors that control the security at these processes.

- SIM card security of the current mobile identity authentication model at registration and replacement processes are susceptible to vulnerabilities which include mobile identity theft at 59.5% considering that an authentication score of 40.5% is realized when all values in the current model against Level of Authentication are considerably significant.
- SIM card security of the current mobile identity authentication model at registration and replacement processes are susceptible to vulnerabilities which include mobile identity theft at 35.88% considering that an authentication score of 64.12% is realized when “user knows” are maximum and are not combined with other authentication factors.
- SIM card security of the current mobile identity authentication model at registration and replacement processes are susceptible to vulnerabilities which include mobile identity theft at 54.63% considering that an authentication score of 45.37% is realized when “user possesses” are maximum and are not combined with other authentication factors.
- SIM card security of the current mobile identity authentication model at registration and replacement processes are susceptible to vulnerabilities which include mobile identity theft at 56.25% considering that an authentication score of 43.75% is realized when “user does” are maximum and are not combined with other authentication factors.
- SIM card security of the current mobile identity authentication model at registration and replacement

ISSN (online): 2581-3048
Volume 6, Issue 1, pp 68-76, January-2022
https://doi.org/10.47001/IRJIET/2022.601014

processes are susceptible to vulnerabilities which include mobile identity theft at 35.88% considering that an authentication score of 64.12% is realized when "user IS" are maximum and are not combined with other authentication factors.

- SIM card security of the current mobile identity authentication model at registration and replacement processes are susceptible to vulnerabilities which include mobile identity theft at 4.75% considering that an authentication score of 95.25% is realized when "user knows" are maximum and are not combined with other authentication factors.

Simulation of the integrated mobile identity authentication model

The development of the integrated model builds from the first and second objectives and is inspired by theory of human identification which is actualized in the current model and integrated population registration records which bring in new parameters to validate the feasibility of the integrated model.

Considering the tests for the new integrated mobile authentication model at significant levels, authentication strength of 306.25 a 43.75% is achieved which is higher than the current mobile authentication strength at 283.5 reflecting a 40.5%. The integrated authentication model has a significant score strength with an increment of significant values at 3.125%.

At maximum values, when all factors of authentication values are engaged, the integrated model scores a strength factor of 675 reflecting a score 96.43% compared with the current authentication model which scores a strength factor of 381.5 reflecting a 95.375 %. The integrated authentication model has a maximum score difference of 1.055%.

Conclusion

The study hereby confirms that maximum level of authentication can only be achieved by introducing an integrated population records attributes to the already existing authentication model while their level of security is maximum. The study also points out that the security level of user knows are not dependent on user IS, implying that where static biometry is used for authentication, knowledge-based authentication may not make much significance.

REFERENCES

1. Wyre, M., et al., *The identity theft response system.* 2020(592): p. 1-18.
2. Wyre, M., D. Lacey, and K.J.C.R.G. Allan, *Australia's Identity Theft Response System: Addressing the Needs of Victims.* 2020.
3. Otor, S.U., et al., *An Improved Security Model for Nigerian Unstructured Supplementary Services Data Mobile Banking Platform.* 2020.
4. Wangui, M., D.J.I.R.J.o.B. Nzuki, and S. Management, *THE EFFECT OF ELECTRONIC MONEY TRANSFER SYSTEMS ON THE FINANCIAL PERFORMANCE OF FINANCIAL INSTITUTIONS IN KENYA (CASE STUDY OF SUMAC DEPOSIT TAKING MICROFINANCE LTD).* 2021. **2**(1).
5. Roussos, G., D. Peterson, and U.J.I.J.o.E.C. Patel, *Mobile identity management: An enacted view.* 2003. **8**(1): p. 81-100.
6. LoPucki, L.M.J.T.L.R., *Human identification theory and the identity theft problem.* 2001. **80**: p. 89.
7. Mayrhofer, R., V. Mohan, and S.J.a.p.a. Sigg, *Adversary Models for Mobile Device Authentication.* 2020.
8. Funcion, D.G.J.J.o.S., Engineering and Technology, *Content Analysis of Online Documents on Identity Theft Using Latent Dirichlet Allocation Algorithm.* 2017. **5**: p. 56-68.
9. Jiang, C. and Z. Li, *Mobile Payment Authentication*, in *Mobile Information Service for Networks*. 2020, Springer. p. 207-242.
10. Feng, T., et al. *Continuous mobile authentication using touchscreen gestures*. in *2012 IEEE conference on technologies for homeland security (HST)*. 2012. IEEE.
11. Cui, Z., et al., *A hybrid BlockChain-based identity authentication scheme for multi-WSN.* 2020. **13**(2): p. 241-251.
12. Chen, S., et al., *Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication.* 2019. **19**(16): p. 3610.
13. Kim, J., N.J.P. Park, and U. Computing, *Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing.* 2019: p. 1-9.
14. Hammood, W.A., et al. *A review of user authentication model for online banking system based on mobile IMEI number*. in *IOP Conference Series: Materials Science and Engineering*. 2020. IOP Publishing.
15. Amine Ferrag, M., et al., *Authentication schemes for Smart Mobile Devices: Threat Models, Countermeasures, and Open Research Issues.* 2018: p. arXiv: 1803.10281.
16. Chen, D., et al., *A behavioral authentication method for mobile based on browsing behaviors.* 2019. **7**(6): p. 1528-1541.
17. Ma, P., D. Tao, and T. Wu. *A pseudonym based anonymous identity authentication mechanism for mobile crowd sensing*. in *2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*. 2017. IEEE.
18. Li, Y., et al., *A Secure Anonymous Identity-Based Scheme in New Authentication Architecture for Mobile Edge Computing.* 2020.
19. Xue, K., et al., *A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture.* 2014. **80**(1): p. 195-206.
20. Ashibani, Y. and Q.H. Mahmoud. *A user authentication model for IoT networks based on app traffic patterns*. in

ISSN (online): 2581-3048
Volume 6, Issue 1, pp 68-76, January-2022
https://doi.org/10.47001/IRJIET/2022.601014

2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). 2018. IEEE.
21. Mufandaidza, M., T. Ramotsoela, and G.P. Hancke. *Continuous user authentication in smartphones using gait analysis*. in *IECON 2018-44th Annual Conference of the IEEE Industrial electronics society*. 2018. IEEE.
22. Xu, J., et al., *An identity management and authentication scheme based on redactable blockchain for mobile networks.* 2020. **69**(6): p. 6688-6698.
23. Ali, G., M. Ally Dida, and A.J.F.I. Elikana Sam, *Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures.* 2020. **12**(10): p. 160.
24. Chege, A.M., *Implementation of the national population registry system in Kenya*. 2015, University of Nairobi.
25. Information Technology Laboratory, N., *Measuring Strength of Authentication*, in *Advanced Identity Workshop*. 2015, National Institute of Standards and Technology (NIST): Gaithersburg, Maryland. p. 9.

Citation of this Article:

Abwao Donatus, Abeka Silvance, Agola Joshua, "An Integrated Mobile Identity Authentication Model", Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 1, pp 68-76, January 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.601014

****

