INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

*Corresponding author.

owusu.nyarkoboateng@uenr.edu.gh

A Fraud Prevention and Secure Cognitive SIM Card Registration Model

Owusu Nyarko Boateng[1]*, **Boadu Nkrumah**[2], **Victoria Boafo**[3], **Akwasi Amponsah**[3], **Lord Anertei Tetteh**[4], **Justice Aning**[5], **Kornyo Oliver**[1], **Adebayo Felix Adekoya**[1], **Isaac Kofi Nti**[6], **Faiza Umar Bawah**[1], **Nicodemus Awarayi Songose**[1], **Boateng Samuel**[1], **Patrick Kwabena Mensah**[1], **Peter Nimbe**[1], **Vivia Akoto Adjepong**[1], **Ricardo Agbedanu**[7], **Benjamin Asubam Weyori**[1]

1 The Department of Computer Science and Informatics, University of Energy and Natural Resources, Ghana
2 The Department of Computer Science, Kwame Nkrumah University of Science and Technology, Ghana
3 The Department of ICT & Mathematics, Mampong Technical College of Education, Ghana
4 The Department of Computer Engineering, Koforidua Technical University, Ghana
5 The Department of Computer Science, Sunyani Technical University, Ghana
6 School of Information Technology, University of Cincinnati, Ohio, USA
7 African Centre of Excellence in Internet of Things, University of Rwanda, Rwanda

Abstract

Background: Most subscriber identification module (SIM) which usually finds their way to mobile phone users are primarily unregistered or pre-registered. Criminals buy these SIM cards, which have fake personal information, activate them and then use them as a channel of attacking vulnerable mobile phone users. **Objective:** to investigate the existing standards of the registration process, the weakness and how fraudsters leverage the shortcomings of the existing registration to attack unsuspecting subscribers. **Methods:** The study also proposed an automated theoretical model as an augmented model to ensure the SIM registration process and implementation become secure. **Results:** In our investigation, we identified that there had been a rise in fraudulent activities in Ghana, and the criminals have adapted to the new trend of committing a crime using mobile phones. The research presented a proposed conceptual model and algorithm for the new SIM registration. The study further conducted a comparative analysis of the principal component adopted to measure the robustness of the registration platform. The criminals mostly use social engineering tactics to trick their victims into disclosing sensitive information or sending money for services yet to be rendered. MNOs request an ID card before registering and activating SIMs, yet criminals can outwit the registration processes and get SIM cards registered through unapproved channels. **Conclusion:** We found out that the robustness of our model shall prevent SIM pre-registration and unapproved SIM activation due to verification mechanisms in the proposed model. A cognitive learning

system has automated the registration process that can identify multiple registrations and prevent unapproved activation.

1 Introduction

The Subscriber Identity Module (SIM) card is a circuitry module that stores the subscriber's information and connects the subscriber's phone to the mobile network operator's (MNO) communication systems. A SIM card is an essential unit in a cellular communication system. It plays a vital role in voice, data, and many other value-added services for the MNOs. Subscribers must provide their data upon SIM purchase before the modules' services are activated. The role of the SIM in communication is critical because, without the module, one cannot access any service provided by the MNOs. The process that links the subscriber's personal information to his SIM is called SIM registration [1]. SIM registration is the process of recording and verifying mobile phone numbers and the personal data of a subscriber by MNO. Such information includes the subscriber's photograph, name, date of birth, gender, residential address and other valid identifiable documents. The SIM registration exercise aims primarily to reduce mobile phone-related crimes such as prank calls, cybercrime, kidnapping, mobile money fraud, and general security matters. It is also intended to help law enforcement agencies identify SIM card owners and track criminals who use phones for illegal activities. In addition, the registration process also helps curb incidents such as phone theft, hate text messages, mobile fraud activities, and inciting violence and probably help MNOs know their subscribers better.

Furthermore, the registration exercise further helps combat crime, such as SIMBox fraud. Therefore, SIM registration is essential for both the subscriber and the MNO, as enshrined in the Legislative Instrument (LI) 2006 for the subscriber identity SIM of Ghana in 2011. This paper proposes a new SIM registration framework with an integrated cognitive system to prevent pre-registration and fake registration. The proposed registration platform is an advanced SIM registration framework that offers all the MNOs a common platform to monitor the process of new registration and the statistical summary of valid registered subscribers.

A mandatory SIM registration exercise between 2008 and 2011 saw countries like Ghana, Nigeria, Kenya, etc., initialize the SIM registration process with much effort and assistance from the respective regulatory national authorities [2]. However, these compulsory registrations perhaps were not adequately executed, so fraudsters across the sub-region continued to perpetrate criminal activities using SIM cards. Moreover, the technique deployed in the registration has not been effective because of the designated state regulatory agencies' lack of a proper monitoring mechanism.

Succinctly, this paper presents a theoretical model for an automated SIM registration system using cognitive computing technology to augment, accelerate, and scale human expertise to enable a new era of genuine human-machine collaboration in the SIM registration process. It is instructive to note that cognitive systems are not programmed but are instead trained, acquiring knowledge through experience and improving with time [3].

In other words, the systems can determine the meaning of data inputs - structured and unstructured, text-based, or sensory - by interpreting context and classifying the data as information or knowledge. Furthermore, the system can also learn continuously, accumulating data and insight through human interactions to provide an efficient automated registration system.

2 Literature Review

There are few written academic papers on mandatory SIM registration in Ghana. Other African countries, such as Botswana, Kenya, Nigeria, Zimbabwe, Sierra Leone, South Africa, and Cameroon, have implemented mandatory SIM card schemes[4]. Compulsory SIM registration in Nigeria started in 2008 in response to several mobile crimes perpetrated by fraudsters. However, the country's current decentralised systems lack the flexibility to register heterogeneous SIM cards and encourage multiple registrations. In their publication entitled 'design and development of a centralized, unified subscribers SIM registration platform', the authors proposed to address these loopholes. The new system surpasses the existing one. It could register all SIM cards of the four (4) major telecommunication operators in Nigeria and verify if a SIM card had already been registered[5], thus bringing stability, flexibility, and a single platform for all. Authors recommended an end to the SIM card availability and sales on the roadside, or such SIM cards are denied access to the network until they are appropriately registered[6,7].

Sub-Saharan Africa ranks among the top regions in terms of the high penetration rate of internet utility and the growth of mobile phone users. The success of mobile telephony is attributed to the opening of private players' markets and lenient regulatory policy. However, markets may be increasingly saturated, and new regulations introduced across Africa could negatively impact future growth. For example, since 2006, most countries in the African-Sub region have introduced mandatory registration of prepaid SIM cards with their identity details. This potentially increases the costs of using mobile telephony. Herein, a fixed-effects model for estimating the impact of mandatory registration on mobile subscription penetration growth is presented based on a panel dataset of 32 countries in Sub-Saharan Africa from 2000 to 2010. The results show that the introduction of mandatory registration depresses growth in mobile penetration. Further, the potential impact of compulsory registration on competition and consumer privacy is critically discussed[8,9].

Subscribers of mobile telephony services in Africa in the early 2000s did not have to register their SIM. However, in recent years, concerns regarding using mobile phones for illegal purposes have led to several opinions to adopt comprehensive measures to mitigate fraud in the mobile communication space[10]. Hence, the need to introduce a strict directive to register all SIMs to enhance subscriber security.

2.1 Unapproved form of SIM Registration

Security agencies such as the criminal investigations department (CID) and the cybersecurity unit mostly find it extremely difficult to investigate a crime committed with fake registered SIM and related offences. For instance, SIMBox fraud, Mobile money fraud and scratch card theft are ascending in Ghana. Still, the security agencies mandated to handle such crimes have no clue where to begin the investigations because the SIM used by these criminals were registered with fake information. This has made it extremely difficult for security agencies to combat crime involving mobile money, mobile banking and related cases.

This study identified two major SIM registration flaws: false identity and pre-registered SIM registrations. Pre-registered SIM is when agents mandated registration officers of the MNOs, of MNOs, intentionally use fake information to register SIM cards, activate the services on the SIM and sell to unsuspecting subscribers. The danger here is that the subscriber's detail will not be found in the MNO's database in case of fraud or crime. Moreover, when there is a loss of SIM, the subscriber is expected to prove his identity, which usually does not match the information on the pre-registered SIM[9,10]. On the other hand, false identity is when subscribers provide fake personal data during the registration process[11].

In the last nationwide SIM registration exercise in 2011, some MNO agents who operated in part of the country connived with fraudsters and allowed them to register SIMs with fake identity cards. These agents primarily did not demand identification numbers and pictures of subscribers before registration, and even when they did, the identification numbers of the subscribers provided were not verifiable. As a result, MNOs and the security agencies found it extremely difficult to track and prevent those involved in the false identity SIM registration regarding these falsified registration processes. This SIM registration process is a recipe for disaster in the mobile communications ecosystem because those who possess fake registered SIMs usually use fraudulent means to commit criminal activities[5,11].

2.2 Issues in Other Regions

The severity of improper SIM registration techniques in Africa and other low and middle-income countries has become a significant problem that governments, financial institutions, and other civil society organizations are battling to find a lasting solution. To ensure subscriber-based data monitoring and evaluation, SIM registration has not been done efficiently in Ghana and elsewhere in Africa. An adequately registered SIM can be used to track the activities of criminals. When fraudsters notice the SIM card acquisition process is subject to stringent requirements, they are likely to focus on countries with less strict requirements[12].

Some African countries, including the Ghana government, have announced that all mobile networks' subscribers must re-register their SIM cards again. The government's new directive is part of moves to fight mobile money fraud, which has gained momentum over the past few years. The SIM re-registration exercise was supposed to have rolled out in 2019. However, this general SIM registration was considered to be rolled out but without any contingency plan to mitigate the fake registrations. This paper proposes an integrated registration scheme of SIM registration with the national identification card. Hence, there is a need for an automated cognitive SIM registration framework to ensure that all unregistered SIMs can not be activated. The state telecommunications regulatory agencies such as the National Communication Authority (NCA), must verify the subscriber details before the MNOs activate registered SIM cards.

2.3 Fraud Detection and Prevention

Fraud involves deceit to illegally or unethically gain at the expense of another. The act includes theft, misuse of property, corruption, the alteration of services or other records or any unauthorized activity which results directly or indirectly in gain, whether financial or otherwise, to the perpetrator or a third party. Fraud can be perpetrated against the MNOs, subscribers, suppliers, government agencies or departments, or the public[13].

The detection and prevention of fraudulent activities are only possible where strong control structures are constantly applied. Routine checks and monitoring mechanism to ensure that procedures are being followed is essential. Implementation of a cognitive system in the telecommunications industry has added firm management control. The cognitive system's prime responsibility to detect and prevent fraud in the industry is to foster an 'anti-fraud automated cognitive system[14].

2.4 The Need for New Sim Registration in Ghana

The rate at which criminals and some MNO staff defraud mobile service subscribers has reached an alarming stage. Mobile telephony services, such as mobile money, which has been touted as an innovative technology that brings banking to the doorstep of the unbanked, are turning out to be a monster that is depriving most people of their little money[3,4]. This worrying trend is complicated, and security agencies find it extremely difficult to track down the perpetrators due to fake identities on SIM cards. The result of fake identification has severely contributed to the high crime rate, and only a few reported cases could be thoroughly investigated and prosecuted[11,12].

It has been estimated by[3,4] that at least 5 out of 10 mobile money subscribers have either experienced fraud or have been a target for mobile money scams. The most disturbing part of mobile crime is that fraudsters arrested by security agencies are believed to be the staff of MNOs. These staff allegedly infiltrate their employers' database, retrieve information from subscribers and deliberately disclose it to scammers. Based on these facts from the state's institution, it is reasonable on the government's part, too, as a matter of urgency, to initiate getting all existing SIM cards and new SIM cards[15] registered using our cognitive SIM registration system.

2.5 Secure SIM Registration Process

The National Communication Authority (NCA), as an authorized body, is mandated to monitor and regulate the MNOs in Ghana; the authority also ensures the MNOs implement proper SIM registration standards. In this paper, NCA has been assigned a specific regulatory task. It must be directly involved in the automated SIM registration process to be implemented in Ghana to ensure full compliance with the automated registration scheme. Unstructured Supplementary Service Data (USSD) protocol shall be created as a common platform to link NCA, MNOs and subscribers' interactions. The integrated platform will offer all stakeholders the opportunity to interact with each other smoothly. The intelligent registration system will enable new subscribers to access the automated registration system by texting their National Identification (NID) number to a short code for verification, authorization and registration by NCA and MNO respectively. NCA has been given the sole responsibility and privileges to manage and implement specific authentication mechanisms to verify new subscribers to prevent malicious people from using someone's NID to register. The new SIM registration process is based on cognitive learning science. It has an embedded intelligent system to identify and prevent fake SIM registration and make things difficult for fraudsters to carry out any criminal activity like SIMBox and mobile money fraud.

2.6 The proposed Automated SIM Registration Model (ASRM)

As presented in Figure 1, the architecture of the automated SIM registration model has a complex and robust cognitive system that mimics human intelligence. The framework comprises a learning algorithm that is based on the cognitive short-term and long-term memory motor. The period a subscriber initiates a SIM registration process and the response time shall be kept in the

short-term memory; the long-term memory, on the other hand, keeps all subscribers' information in the centralized information system. The ability to reason to make near-perfect decisions has been integrated into the automated SIM registration system's design framework. However, computational memory and decision-making systems aim to support learning, and autonomous attention (unsupervised learning) focuses on a specific task's direct learning. The combination of unsupervised attention and learning addresses the existing SIM registration process's challenges and implements automated reasoning and decision-making system.
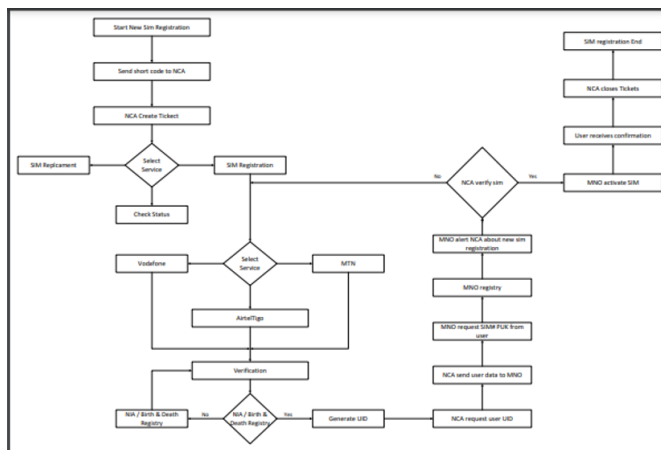

Fig 1. Conceptual model for ASRM

Algorithm for the Proposed Automated SIM Registration Model (ASRM)
1. Start new SIM registration
2. Send short code to NCA
3. NCA create ticket
4. Select service
5. if (service = = check status) then
6. Process check status
7. else if (service = = replacement) then
8. Process SIM replacement
9. else if (service = = SIM registration) then
10. Select network
11. SIM verification by NIA/BDR
12. if (SIM verification is unsuccessful) then
13. Goto step 11
14. else
15. Generate UID
16. NCA requests user UID
17. NCA send user data to MNO
18. MNO request SIM PUK from the user
19. MNO registry
20. MNO alert NCA about new SIM registration
21. if (NCA is unable to verify SIM) then
22. Goto step 10
23. else
24. MNO activate SIM
25. User receives confirmation
26. NCA closes tickets
27. End SIM registration
28. else
29. Stop

3 Cognitive Dashboard for ASRM

A dashboard is an information management tool that visually tracks, analyzes and displays key performance indicators (KPI), metrics and key data points to monitor a business's health, department or specific process. Dashboards are customizable to meet the particular needs of a department and company. The Dashboard has two ends; at the back end, which is the view behind the scenes, the tool connects to institutional files, attachments, services and APIs, but at the surface, it displays the data in the form of tables, line charts, bar charts and gauges. The cognitive dashboard h designed to have a well-built Visual Display of Quantitative Information.

A data dashboard is the most efficient way to track multiple data sources from the various state institutions and the MNOs because it provides a central location for NCA to monitor and analyze performance and the SIM registration progress. The Dashboard will have real-time monitoring of current registrations' progress to reduce the long hours of data. The Dashboard has an integrated display unit that outputs the cognitive system's computational learning and decision-making. These are some of the information to be displayed: The statistics of registered subscribers on a real-time basis, A determining index that displays a graphical representation of the market share of the MNOs, real-time information on the progress of SIM registration, and detection and prevention the use of pre-registered SIM cards

National Identification ID Card Data

The government of Ghana has directed that the first step to acquiring a national ID card in Ghana is to first register with the National Identification Authority (NIA). NIA is mandated by law to provide national ID cards to citizens. The mandate of the NIA is to create a national database of all citizens and foreigners with digital identities. NIA in the recent registration in 2020 issued national ID to individuals who fulfilled the basic requirement for registration by providing the information such as: Name/Gender, Date/Place/ District/Region/ Nationality of Birth, Occupation/Religion/Denomination/Education, Residential Digital Address/TIN/SSN/Tel.#, Marital Status/Spouse/Children, Car#/House#/Passport#, Biometric features/passport photograph.

Data Transmission

The growth of high-speed internet connectivity has made it possible for data transmissions to be achieved through a secure transmission system[16,17]. End-to-end data transmission and storage are key in the SIM registration exercise. The current state-of-the-art mobile telephony technology is an enhanced infrastructure which supports quality service delivery through optical fiber transmission networks[18],[19] For NIA to successfully appropriately protect data retrieved from the SIM registration exercise, enhance secure transmission protocols such as TLS/SSL would be deployed to ensure data interception and malicious attacks are prevented[17],[19].

Comparative analysis

The computational memory of ASRM supports cognitive learning and autonomous attention (unsupervised learning) focused on the direct learning of a specific task in the ASRM processes. The combination of unsupervised learning schemes aims to address the challenges in the existing SIM registration processes and implement automated reasoning and decision-making system. The proposed model has theoretical been designed to overcome the shortfalls in the current SIM registration method as indicated in the literature[5,20,21]. The proposed registration system also offers a robust, secure registration as the process ensures the verification of the subscriber's data with the national database of NIA.

The study presents a comparative analysis between ASRM and other existing models. The key components the study considered for the comparative analysis includes cognitive reasoning (CR), system robustness (SR), verification (V), security (S), implementation (I) and Usability (U) for the Integrated SIM Registration (ISIM), and Unified Subscribers' SIM Registration (USSR).

Table 1. Comparison of ASRM and other SIM registration standards

Registration Standard	CR	SR	V	S	I	U
ISIM	No	No	No	Secure	Complex	Complex
USSR	No	No	No	Secure	Complex	Complex
ASRM	Yes	Yes	Yes	Secure	Easy	Easy

Visitors who plan to stay within 30 days can register for a new SIM using their passport and temporal residence address. However, to ensure that visitors/foreigners are not mistreated if their stay is prolonged, they can submit a permit to Ghana Immigration Service (GIS) for SIM re-activation for the next 30/60 days. Visitors' SIM registration can not be used beyond 90 days period; else, the visitor must apply for a resident permit GIS.

4 Conclusion

The proposed system is a new model, and if implemented in the real world, it will solve several problems, including tracking criminals and crime rate reduction. The work's novelties are the modelling of an automated SIM registration system, monitoring statistics of registered subscribers on a real-time basis, A determining index to display a graphical representation of the market share of the MNO, and real-time information on the progress of SIM registration.

The MNOs must ensure that subscribers' privacy is always protected. The situation where MNOs release subscriber details to third-party companies must be addressed by NCA. NCA must also ensure that any Telco that releases its subscriber information to a third-party marketing organization shall receive some form of stern punishment and the subscribers involved compensated appropriately. The introduction of punitive measures will deter the networks from releasing such data. Until this is done, MNOs will not enforce policies that protect subscriber data. A mix of disciplinary and reward actions can be applied to MNOs who flout or enforce their privacy policies. The implementation of the proposed solution will go a long way to sanitize the entire SIM registration process in Ghana.

References

1) Ameen AO, Akanni OA, Alimi OM, Haliru S. *Design and development of a unified subscribers' SIM registration platform using top-down approach Information Technologist (The)*. 2016;13(2):91–96.
2) Lieto A, Radicioni DP. From human to artificial cognition and back: New perspectives on cognitively inspired AI systems. *Cognitive Systems Research*. 2016;39(16):1–3. Available from: https://doi:10.1016/j.cogsys.2014.11.001.
3) Otu P, Sogbordjor. Enhanced Secure Transaction for Mobile Money Services. *Owusu Nyarko-Boateng & Lord Anertei Tetteh*. 2020;8(4):1275–1288.
4) Beck T, Ramrattan R, Pamuk H, Uras BR. 2016.
5) Donovan KP, Martin AK. The rise of African SIM registration: The emerging dynamics of regulatory change. *First Monday*. 2014;19(2). Available from: https://doi.org/10.5210/fm.v19i2.4351.
6) Nyarko-Boateng O, Kuranchie A, Anning J. The Relevance of E-Library Facility to the Delivery of Education at the High School: An Example from Ghana. *International Journal of Scientific & Engineering Research*. 2017;8(5):910–918.
7) Nyarko-Boateng O, Kuranchie A, Anning J. The Relevance of E-Library Facility to the Delivery of Education at the High School: An Example from Ghana. *International Journal of Scientific & Engineering Research*. 2017;8(5):910–918.
8) Sumbwanyambe M, Nel A. Assessing the implications of SIM card registration policy in the SADC region. IST-Africa Conference & Exhibition, Nairobi. 2013. Available from: https://ieeexplore.ieee.org/abstract/document/6701720.
9) Makoza F. An Exploratory Study on Policy Transfer for SIM Card Registration in Malawi. *International Journal of Technology Diffusion*. 2015;6(1):33–45. Available from: https://doi.org/10.4018/IJTD.2015010102.
10) Makulilo A. Registration of SIM cards in Tanzania: a critical evaluation of the Electronic and Postal Communications Act. *Computer and Telecommunications Law Review*. 2010.
11) Nyarko-Boateng O. SIM Registration Fraud Prevention Mechanism Mobile Communication Space in Ghana. 2019. Available from: https://iipgh.org/sim-registration-fraud-prevention-mechanism-mobile-communication-space-ghana/.
12) Oyediran O, Omoshule A, Misra S, Maskeliūnas R, Damaševičius R. Attitude of mobile telecommunication subscribers towards sim card registration in Lagos State, Southwestern Nigeria. *International Journal of System Assurance Engineering and Management*. 2019;10(4):783–791. Available from: https://doi.org/10.1007/s13198-019-00809-6.
13) Nyarko-Boateng O, Asante M, Nti IK. Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization. *International Journal of Science and Engineering Applications*. 2017;6(3).
14) Krishnakumar T. Missed Connections? Evaluating the Global Spread and Legality of Mandatory SIM Registration in a Modern National Security Context. Denv. *J Int'l L & Pol'y*. 2021;49:57–57.
15) Oladipo F, Abdu, & Haruna, Obansa AA. Integrated Subscriber Identification Module Registration. *International Journal of Science and Engineering Investigations*. 2018;7(75).
16) Nyarko-Boateng O, Weyori BA, Tetteh LA. Optimized Authentication Model for Online Transaction Payments. *Journal of Computer Science*. 2020;16(2):225–234.
17) Nyarko-Boateng O, Adekoya AF, Weyori BA. Investigating QoS and Performance of Received Signal Strength Indicator in Fiber Optics Broadband Data Communication. *American Journal of Engineering and Applied Sciences*. 2019;12(3):391–401. Available from: https://doi.org/10.3844/ajeassp.2019.391.401.
18) Nti IK, Adakoya AF, Nyarko-Boateng O. A Multifactor Authentication Framework for the National Health Insurance Scheme in Ghana using Machine Learning. *American Journal of Engineering and Applied Sciences*. 2020;13(4):639–648. Available from: https://doi.org/10.3844/ajeassp.2020.639.648.
19) Nyarko-Boateng O, Adekoya AF, Weyori BA. Adopting Intelligent Modelling to Trace Fault in Underground Optical Network: A Comprehensive Survey. *Journal of Computer Science*. 2020;16(10):1355–1366. Available from: https://doi:10.3844/jcssp.2020.1355.1366.
20) Cheesman M. Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. 2020. Available from: https://doi:10.1080/14650045.2020.1823836.

21) Martin A, Taylor L. Exclusion and inclusion in identification: regulation, displacement and data justice. *Information Technology for Development*. 2021;27(1):50–66. Available from: https://doi.org/10.1080/02681102.2020.1811943.