MoBiSafe: an obfuscated single factor authentication mode to enhance secured USSD channel transaction in Nigeria

Amaka Patience Binitie[1], Sebastina Nkechi Okofu[2], Margaret Dumebi Okpor[3], Kizito Eluemunor Anazia[4], Arnold Adimabua Ojugo[5], Francesca Avwuru Egbokhare[6], Annie Egwali[6], Peace Oguguo Ezzeh[1], Rita Erhovwo Ako[5], Victor Ochuko Geteloma[5], Tabitha Chukwudi Aghaunor[7], Eferhire Valentine Ugbotu[8], Sunny Innocent Onyemenem[1]

[1]Department of Computer Science, School of Science, Federal College of Education (Technical) Asaba, Asaba, Nigeria
[2]Department of Marketing and Entrepreneurship, Faculty of Social Science, Delta State University Abraka, Asaba, Nigeria
[3]Department of Cybersecurity, Faculty of Information Technology, Delta State University of Science and Technology, Ozoro, Nigeria
[4]Department of Info Tech, Faculty of Information Technology, Delta State University of Science and Technology, Ozoro, Nigeria
[5]Department of Computer Science, Federal University of Petroleum Resources, Effurun, Nigeria
[6]Department of Computer Science, Faculty of Physical Science, University of Benin, Benin, Nigeria
[7]Department of Data Intelligence and Technology, Robert Morris University, Pennsylvania, United States
[8]Department of Data Science, University of Salford, Salford, United Kingdom

Article Info

Article history:

Received Oct 8, 2024
Revised Mar 28, 2025
Accepted Jul 3, 2025

Keywords:

MoBiSafe
Single factor authentication
System usability
USSD channel
USSD security

ABSTRACT

The flexibility of the unstructured supplementary service data (USSD) across mobile phones has caused its adoption surge as a payment channel. Its usage accommodates financial inclusivity and extends customer reach irrespective of their specific phone capabilities. With data conveyed on the USSD channel in plaintext–this has raised vulnerability issues with shoulder surfing attacks. The use of password yielded extra layer of security as authentication to USSD-based services. But, the rise in password guess attacks has necessitated a new scheme. This study is a randomized-obfuscated single factor authentication (SFA) mode via a 5-digit PIN-entry as requisite for the USSD channel. It yields a list via which users select a key-array that corresponds to their PIN as concealed in a 10-digit array. Expert assess of MoBiSafe's usability and security against shoulder-surf yielded 10.1 msecs and 2.26 msecs respectively to outperform existing models that utilize direct/indirect PIN-entry as in USSD transactions. And this was found to be both secure, usable and acceptable.

Corresponding Author:

Amaka Patience Binitie
Department of Computer Science Education, Federal College of Education (Technical) Asaba
Asaba, Delta State, Nigeria
Email: amaka.binitie@fceatasaba.edu.ng

1. INTRODUCTION

Society today is rippled with various transactions that allows the exchange of goods and services for money, which often occurs between 2-parties usually referred to as a buyer and a seller [1]. A transaction is deemed complete once both parties conclude a bargain that allows for the exchange of money so that purchased good are delivered [2], and allied services are rendered [3]. Our society today continues to witness an increased number of daily transactions, which has in turn–necessitated the need for third-party actor often referred to as the bank, to act as a witness of the bargained conclusions therein arrived at and to provision the safe habitat of the monies, pending further actions [4]. As transaction occurs across rural and urban dwelling, banks in their quest to reach many users [5], [6] provide payment channels as modes that authorize exchange of monies and foster more transactions. With customer's account domiciled within these financial house (or banks)–inherent channels created today includes credit-cards, automated teller machines (ATM) [7], point-of-sales (POS), unstructured supplementary service data (USSD), online apps/platform, and wallets. These provide modes for financial inclusivity with a transactions beyond borders paradigm – and to extend a bank's reach to her customers, at any time and place [8]. These digital channels are today, cornerstones that facilitate payments for transactions – empowering account holders to consolidate their prowess into easily manageable form(s) [9]. Such convenience and ease, continues to propel these digital products as the preferred choice for use in a variety of transaction scenarios; Rather, than the traditional exchange of printed monies in many instances.

With the proliferation of smartphones that has continued to ease mobility, portability, usage ease and flexibility of transaction processing [10]–reliance on these digital products has consequently, raised security concerns as adversaries are continually on the look-out to explore and exploit unsuspecting user whose device have been compromised. Thus, with access gained, these adversaries exploit such compromised-user-device as entry point to explore network resources for personal gains. With telephony advances in 3G, 4G and 5G respectively – tele-penetration disparities still exist across rural/urban dwellers. Even with the increased use in smartphone users, many still restrict themselves to less sophisticated phone due to various reasons which include: (a) tele-penetration coverage, (b) status disparities [11]. These prevailing reasons has seen a surge in customer adoption of USSD. The USSD is an interactive communication protocol between mobile devices and their service providers. Its simplicity, broad compatibility and usage ease with basic features inherent in mobile phones, render it effective to facilitate payment across a vast collection of customers [12]. Such phones are simplistic in their design, and features: (a) limited computational power, (b) restrictive memory capability, (c) absence of biometrics [13], and (d) modest camera [14]. The utilization of USSD is devoid of a robust security mechanism for user data. USSD is vulnerable to shoulder surfing attacks. Thus, it poses significant security risk that currently drives extensive studies in lieu of deploying robust authentication schemes (i.e. text-based passwords, graphical methods, and biometrics) to protect user data from unauthorized access and/or theft [15].

Studies have proven that amongst the various authentication methods utilized with USSD – the most common used is the personal identification number (PIN) mode, which is a text-based authentication approach [16], [17]. These are plaintext authentication data keyed in by a user at the mobile device interface during the USSD transaction [18]. Other forms of graphical methods [19] and biometrics [20] cannot be implemented in USSD channel due to the simplistic design and authentication data format. Thus, account holders explore unconventional modes such as screen-covering with hand, to secure their data from close-by associates. These offer no significant secure solution and portends financial loss [21]. To avert these, various PIN modes posited by [22], [23] failed to resolve inherent constraints in the USSD channel namely: (a) the need for authentication method to secures user data at mobile interface against shoulder-surfing [24], and (b) resolve interoperability issues that transmits only in plaintext data as channel prerequisite [25]. With literature discussed, USSD adoption is still growing, and can achieve enhanced security and performance. This study contributes thus:

a) Review of existing USSD model with a view to optimizing its utilization as payment channel in Nigeria.
b) Construct the randomized obfuscation-based authentication approach for the USSD payment channel
c) Comparing the performance of our proposed ensemble in payment transaction tasks

For the remainder part–section 2 deals with methodology for the Proposed MobiSafe via existing system analysis, proposed system workings, and evaluation metrics. Section 3 shows results with findings implication, comparison of results and findings discussed. Study concludes with recommendations to USSD channel.

2. METHOD

The USSD is a mobile-based, interactive transaction service that utilizes the direct PIN-entry mode with plaintext data factor authentication [26]. Its menu-based approach allows keyed in data to yield interactive queries for the transaction channel, which elicits response from the device user [27], [28]. Usually 4-to-5 digits in length, the numeric plaintext, keyed in values are called PIN. If a PIN is matched against a predefined user-chosen USSD template of a user secure PIN stored during USSD registration). With a match – the payment is authenticated and money sent to the designated party: Else, the transaction is terminated [29], [30]. This scheme has proven to be insecure from adversaries that explore shoulder surfing [31], and there is the need to resolve its interoperability issue that transmits only in plaintext data as channel prerequisite [32], [33]. With these drawback, we proposed the use of an indirect, random-obfuscated pin entry factor authentication approach as in Figure 1:

a) Stage 1: User Registration – creates and affirms the 5-digit PIN. Each user responds to queries that are retrieved via challenge response mode as commonly used in the USSD framework, and stored as a bag of soft biometrics (BoSB). The first dialed USSD code initializes registration of a new mobile number via the 'create account option'. Once successful, a new USSD wallet is created and linked to the SIM.

To avoid misuse, each BoSB retrieved is stored and continually updated with every transaction until all queries are exhausted; And new queries are initiated [34]. See Algorithm 1 listing for actions taken by the proposed obfuscated USSD. A new user triggers this action by dialing any USSD code. With menu-driven, interactive task, a new user provides answers to each BoSB [35]. This creates the 5-digit-PIN via a SHA-256 hash algorithm. The dialed USSD code is validated via the USSD API gateway; And if affirmed as correct, it registers the user phone number as newly created account, and stored in the bank database for verification [36]. Number is then linked to the account, so that each BoSB generated at USSD server is passed to a customer. And responses keyed are stored back on the cloud server; And generated OTP is passed to a user phone number as short message vis-à-vis stored both in cloud and bank's database with a registration successful message therein [37].

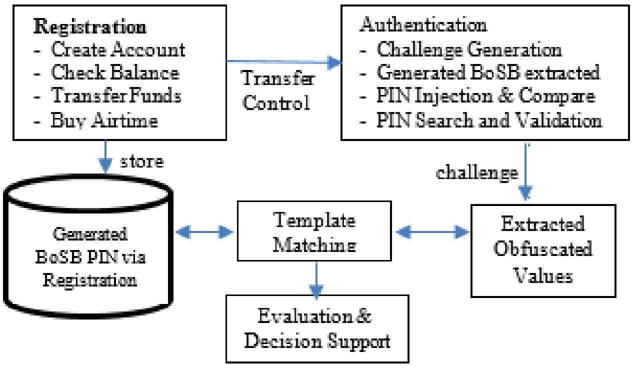

Figure 1. Proposed methodology for MobiSafe ensemble

Algorithm 1. Listing for the proposed USSD registration framework

```
INPUT: get user_info()
function get_option (input): 1 - create_account, 2 - check_bal, 3 - tranfer_funds, 4 -
buy_airtime; START
if (option_default = 1) then
register_value: return true: ussd_API_verify == phone_nos_registered()
else (input_value = others) // for returning registered users
endif
function option_default(create_account()):
if option_default == true ← function get (user_name, phone_nos, user_PIN, user_cardID)
then
return userID ←record_a_transaction (sha256(new_record))
create user_obfuscated_PIN = digits_five
verify user_obfuscated_PIN == true
challenge_question_response == true
store user_data == cloud
end
function create_wallet (user_info): START
if true ←function check (user_name, phone_nos, user_PIN, user_cardID) then
return user_details ← wallet(user_info, verified user_obfuscated_PIN)
message 'congratulations - your account has been successfully created'
cloud_API = get(OTP, phone_number) //send details to user phone number
endif
```

b) Stage 2: Authentication – Our challenge response approach uses a randomized obfuscation technique, which obscures the original user-keyed in PIN. Thus, as opposed to a user directly inputting their PIN, our proposed approach proffers a 2-step challenges derived from randomly generated digits. The users' 5-digit PIN is obfuscated via 10-random generated number mode at each instance or case of the single factor authentication (SFA) at each instance. The generated integers are transformed and ordered into an array of digits [26], and then – randomly shuffled to disrupt the original sequence of digits. Thus, making it tedious to identify the original PIN. The PIN is obfuscated via embedding it within the 10-digit number such that the position of the PIN within the 10-digit number is randomly determined for each authentication attempt. This adds extra security against shoulder surfers – making it difficult to guess, identify and extract the actual PIN. The user is only thus, required to select the array-key representing his/her PIN. The mode successfully generates 10 different 10-digit arrays, with only one containing the user first/last 3-digit PIN in a left-to–right order; And in turn – places strenuous recall burden on adversaries, though easier for the user. This technique sets a high security standard against shoulder surfing attack without revealing users PIN through-out the session [38]. Thus, each has an array key per authentication session as in the Algorithm 2 Listing.

c) Stage 3: Evaluation – 30-experts assessed the usability, and security of the proposed USSD model. Sample profiles were utilized to complete registration-to-transaction processes. Both capabilities were tested both on the proposed system and the existing direct PIN-entry method in USSD channel. For usability test, each participant had an adversary (poised for shoulder surfing attack) standing behind them. Participants were instructed to repeat this process 15-times to give each shoulder-surfer ample time of retrieving the PIN with break intervals. For "Transfer fund Option", the system had 10-to-11hops (i.e. a hop is the number of steps required to complete a transaction). For usability, the error-percent (β) and response time (t) were achieved as (0.1, 10) that agrees with [39], [40]. For security test, we adapt the hardness (security) factor as in [41], [42] as the ratio of the time taken by an attacker to capture relevant data from user's response to the time taken by a user to submit a valid response. If the value of the security factor is > 1, it implies the shoulder surfer was unsuccessful [43]; And, a security factor ≤ 1, implies success by the adversary. Thus, we utilized the performance model for cognitive, perceptual, motor and goals, operators, methods and solution (CPM-GOMS) tool. The CPM-GOMS seeks to can be used in modelling the behavior of a user or/ and an attacker. It has three main operators known as Perceptual, Cognitive and Motor.

Algorithm 2. Listing of the proposed USSD authentication framework

```
OUTPUT: get user_info()
function generate (10-digits) //to inject PIN in various order
convert array == map_array('intval', str_split);
get numset == map_array(array_walk, dnum, 'replacenum') //for i = 1 to 10 digit arrays
function inject_PIN(number_set(map_array):
for inject_real_PIN == true ←function get(number_set(map_array))
dnum = rand(1000000000, 9999999999)
oneopt = map_array('intval', str_split(dnum))
realopt = array_walk(oneopt, 'insertreal_n'): newrealopt = getreal(n): array_key =
rand(0.9)
PIN(3) = LTR: numset[arraykey] = newrealopt
return PIN ←record_transaction (sha256(numset[arraykey] = newrealopt))
end
function get_num_set()
numshow = shuffle(numset): return numshow()
end
function PIN_validation()
convert response_array == map_array('intval', str_split($urnum))
search num_order = array(): num_order[] = array_search(pinno_$urnum_array)
compare result = array_diff_associate(num_order_pin_order)
if Is_Empty == true
return(true): else return(false) //error message
end
```

3. RESULTS AND DISCUSSION

3.1. Usability analysis feature

Usability is the time it takes a user to efficiently key in his/her PIN without an adversary successfully capturing it and/or even with the error of mis-entry. With 15-random experts selected – we compute usability via (1)-(3) respectively [44] using a standard 8-hops per session. Table 1 displays the time taken to complete each session via the USSD_API gateway, for a certain bank in Nigeria.

Table 1. The time taken to complete each session in milliseconds

Users	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Time	62	60	50	60	51	53	46	45	46	51	48	45	46	46	45

$$Average\ Time\ to\ complete\ Transaction = \sum_{i=1}^{n} x_i = x_1 + x_2 + \cdots + x_{15} \quad (1)$$

$$T_{session} = \frac{\sum 62+60+50+60+51+53+46+45+46+51+48+45+46+46+45}{8} = \frac{754sec}{15} = 50.3msec$$

Thus, it takes an average 50.3 msecs/session to complete a transaction. Next, we seek to ascertain the average time spent on each hop–bearing in mind that there exists 8-hops per session as in (2):

$$Time_{hop} = \frac{total\ time\ spent\ during\ a\ session}{total\ number\ of\ hops\ for\ each\ session} = \frac{50.3}{8} = 6.3msecs \quad (2)$$

$$Usability_{factor} = \frac{50.3}{8} = 6.3msecs$$

With the existing direct PIN-entry, we clocked each participant to ascertain the time taken to complete each session [45], [46], and compared the obtained result with the gateway feedback. With 8-hops to complete a session–MoBiSafe reached an average 6.3msecs spent on each session. Since direct PIN-entry for USSD banking takes just a hop to enter PIN–it implies that only 6.3msecs was used; and this agrees with [47]. Thus, the total time spent for PIN entry as in (3) as thus:

$$Total_{time} = Number\ of\ PIN_{tries} * average\ time\ to\ hop \quad (3)$$
$$= 2 \times 6.3 = 12.6msecs$$

3.2. Proposed system throughput

The throughput is defined as the actual transfer rate of data in a medium over a period of time. As a performance metric – throughput tests a system's capacity to be impacted by interference and errors. Thus, it determines the application response time to user request in relation to the variety of attack times.

From Figure 2, we observed that the total task time following the critical path to determine the duration for the completion of each task schedule is 830ms for the user response time; while, the attack time yields 1880 ms. Thus, the security factor is computed as in (1).

$$Security_{factor} = \frac{response\ time}{attack\ time} = \frac{1880}{830} = 2.265msec \quad (4)$$

With the computed value that MoBiSafe yields a security factor of 2.265 msecs – it implies that the method is rather very difficult for an adversary to succeed in retrieving users' PIN. This is so stipulated and agreed by [48] – that for user response time utilizing the direct PIN-entry for USSD that exceeds a value threshold above 1secs ensures that the system is secure from adversarial attacks [49], [50].

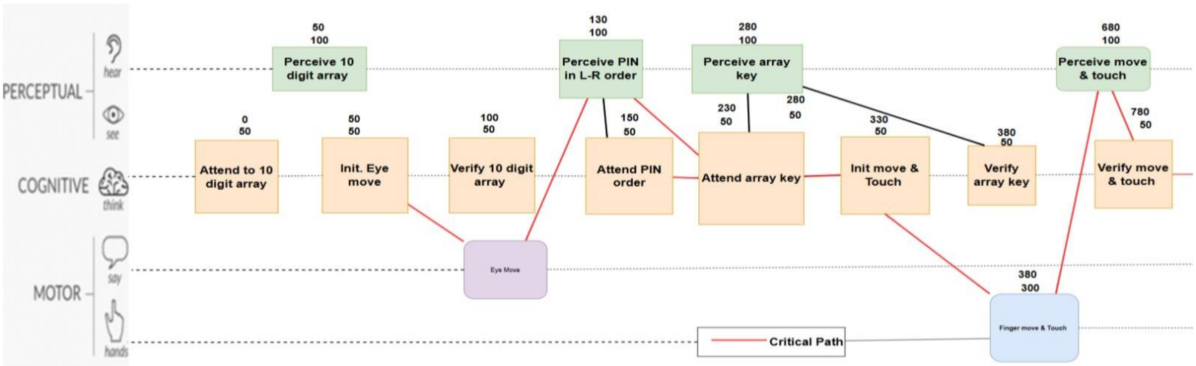

Figure 2. User response time using MoBiSafe

3.3. Comparison

As we explore the high performance of our proposed USSD system, we benchmark it against previous methods that have utilized the same USSD channel mode. To this end–we found none. However, we decided to benchmark the proposed ensemble against similar design constructs that utilized both the (in)direct mode of USSD channel. Some domain tasks have proven easier to evaluate its usability and security features; While, others are more painstaking especially in scenarios for which the chosen system design metric strongly impacts on the security and usability [51] of the system cum platform. Thus, both measures become critical feats to be evaluated – using either the direct-or-indirect-mode PIN-entry for the USSD channel. These have also been found to be prone to shoulder surfing attacks as well as password guessing attacks as seen in Table 2.

Table 2. Benchmarking and comparative testing of proposed system

Methods	Usability Feature(s)				Security Feature(s)		
	Transaction per msec	Time per Hop	Usability factor	Total time for PIN-Entry	User resp. time	Attack time	Secure factor
Eboka and Ojugo [43]	74.8msecs	17.9msecs	32.2msecs	9.8msecs	872msecs	1754msecs	2.00msecs
Geteloma *et al.* [52]	94.5msecs	23.8msecs	43.4msecs	9.80msecs	831msecs	1453msecs	1.75msecs
Binitie and Babatunde [53]	57.7msec	8.9msecs	24msecs	10.3msecs	883msecs	1748msecs	1.98msecs
Hadi *et al.* [54]	64.3msecs	12.4msecs	28.2msecs	11.3msecs	871msecs	893msecs	1.03msecs
Proposed MoBiSafe	50.3msec	6.30msecs	12.6msecs	10.1msecs	830msecs	1880msecs	2.27msecs

From the Table 2–it is observed that many existing system explore the direct pin entry method in USSD mobile banking with users response time is benchmarked at 871msecs; But, the study by [55] yielded user response of 831msecs; while MoBiSafe resulted in 830msecs to outperform others. With our focal attribute on data security against password guessing and shoulder surf attacks–our benchmark systems yielded a security-factor above 1.00msecs [56]. This implies that an attacker will not be able to capture user's response. Thus, yielding a secure channel against shoulder surf and password guessing.

4. CONCLUSION

Our proposed MoBiSafe utilizes the indirect pin mode to enhance security. It maintains the usability of direct pin entry mode for the USSD-channel; while, providing enhanced security against adversaries that exploit shoulder surf attack and password guessing attacks. Unlike some existing pin entry methods, MoBiSafe places a recall burden on adversaries; while, users can simply select a single 10-digit array key that contains a user's chosen PIN. Results affirmed that the time required to perform recall operation prevents an adversary from penetrative and intrusive issue to its security protocols. The use of (β, t) yields a (0.1, 10) ensures that MoBiSafe usability. Its security as tested via CPM-GOMS yields enhanced security against shoulder-surfing attacks and password guessing with a security factor of 2.265msecs, which is greater than 1. Despite being designed to mitigate shoulder surfing attacks, this model presents a promising foundation for further research and development in the domain of password-based attack prevention. Its underlying principles and mechanisms can be explored and adapted to address the growing threat of camera-based shoulder surfing attack.

ACKNOWLEDGEMENTS

This section should acknowledge individuals who provided personal assistance to the work but do not meet the criteria for authorship, detailing their contributions. It is imperative to obtain consent from all individuals listed in the acknowledgments.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Amaka Patience Binitie	✓	✓			✓	✓		✓	✓	✓		✓		✓
Sebastine Nkechi Okofu		✓			✓	✓	✓	✓	✓	✓		✓		✓
Margaret Dumebi Okpor		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
Kizito Eluemunor Anazia			✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
Arnold Adimabua Ojugo	✓	✓		✓				✓	✓	✓	✓	✓	✓	✓
Francesca Avwuru Egbohkare	✓	✓		✓		✓		✓	✓	✓		✓	✓	✓
Annie Egwali	✓	✓		✓		✓		✓	✓	✓	✓	✓	✓	✓
Peace Oguguo Ezzeh	✓		✓			✓		✓	✓	✓	✓			
Rita Erhovwo Ako		✓	✓			✓		✓	✓	✓	✓	✓	✓	✓
Victor Ochuko Geteloma		✓	✓	✓			✓	✓	✓	✓		✓	✓	✓
Tabitha Chukwudi Aghaunor	✓		✓	✓	✓		✓	✓	✓	✓	✓		✓	
Eferhire Valentine Ugbotu	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
Sunny Innocent Onyemenem			✓		✓		✓		✓			✓		✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

- Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] S. N. Okofu *et al.*, "Pilot study on consumer preference, intentions and trust on purchasing-pattern for online virtual shops," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 7, pp. 804–811, 2024, doi: 10.14569/IJACSA.2024.0150780.

[2] M. I. Akazue *et al.*, "Handling transactional data features via associative rule mining for mobile online shopping platforms," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 3, pp. 530–538, 2024, doi: 10.14569/IJACSA.2024.0150354.

[3] D. A. Obasuyi *et al.*, "NiCuSBlockIoT: sensor-based cargo assets management and traceability blockchain support for nigerian custom services," *Advances in Multidisciplinary and Scientific Research Journal Publications*, vol. 15, no. 2, pp. 45–64, Jun. 2024, doi: 10.22624/aims/cisdi/v15n2p4.

[4] E. Altman, "Synthesizing credit card transactions," in *ICAIF 2021 - 2nd ACM International Conference on AI in Finance*, Nov. 2021, pp. 1–9, doi: 10.1145/3490354.3494378.

[5] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "DeLClustE: protecting users from credit-card fraud transaction via the deep-learning cluster ensemble," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 6, pp. 94–100, 2023, doi: 10.14569/IJACSA.2023.0140610.

[6] E. A. Otorokpo *et al.*, "DaBO-BoostE:enhanced data balancing via oversampling technique for a boosting ensemble in card-fraud detection," *Advances in Multidisciplinary and Scientific Research Journal Publications*, vol. 12, no. 2, pp. 45–66, 2024, doi: 10.22624/aims/maths/v12n2p4.

[7] S. E. Brizimor *et al.*, "WiSeCart: sensor-based smart-cart with self-payment mode to improve shopping experience and inventory management," *Advances in Multidisciplinary Scientific Research Journal Publications*, vol. 10, no. 1, pp. 53–74, Mar. 2024, doi: 10.22624/AIMS/SIJ/V10N1P7.

[8] D. A. Al-Qudah, A. M. Al-Zoubi, P. A. Castillo-Valdivieso, and H. Faris, "Sentiment analysis for e-payment service providers using evolutionary extreme gradient boosting," *IEEE Access*, vol. 8, pp. 189930–189944, 2020, doi: 10.1109/ACCESS.2020.3032216.

[9] R. De', N. Pandey, and A. Pal, "Impact of digital surge during COVID-19 pandemic: A viewpoint on research and practice," *International Journal of Information Management*, vol. 55, no. June, p. 102171, 2020, doi: 10.1016/j.ijinfomgt.2020.102171.

[10] A. Z. Nugraha, R. F. Salsabila, A. N. Handayani, A. P. Wibawa, E. Hitipeuw, and K. Arai, "Decision tree based algorithms for Indonesian Language Sign System (SIBI) recognition," *Applied Engineering and Technology*, vol. 3, no. 2, pp. 86–101, 2024, doi: 10.31763/aet.v3i2.1536.

[11] M. A. Haque *et al.*, "Cybersecurity in Universities: an evaluation model," *SN Computer Science*, vol. 4, no. 5, 2023, doi: 10.1007/s42979-023-01984-x.

[12] K. Fartash and B. Modiriat, "A historical analysis on Iran's industrial policy documents and proposing policy imperatives for the years ahead," *Journal of Improved Management*, vol. 15, no. 3, pp. 1–26, 2021, doi: 10.22034/JMI.2021.305149.2655.

[13] C. Abernathy, "Face recognition policy development template for use in criminal intelligence and investigative activities," 2021. [Online]. Available: www.it.ojp.gov.

[14] S. Liu, X. Li, H. Lu, and Y. He, "Multi-object tracking meets moving UAV," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 8866–8875, 2022, doi: 10.1109/CVPR52688.2022.00867.

[15] F. O. Aghware *et al.*, "Enhancing the random forest model via synthetic minority oversampling technique for credit-card fraud detection," *Journal of Computing Theories and Applications*, vol. 1, no. 4, pp. 407–420, Mar. 2024, doi: 10.62411/jcta.10323.

[16] H. A. Abdulmalik and A. A. Yassin, "Secure two-factor mutual authentication scheme using shared image in medical healthcare environment," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 4, pp. 2474–2483, 2023, doi: 10.11591/eei.v12i4.4459.

[17] P. A. Onoma *et al.*, "Attrition rate prediction using a frequency-recency- monetization-based SMOTEEN-boosted approach," MSIS - *International Journal of Advanced Computer Intelligence Systems*, vol. 3, no. 1, pp. 1–11, 2025, [Online]. Available: https://msis-press.com/paper/ijacis/3/1/20

[18] A. P. Binitie, D. N. Akhator, and K. K. Chukwubueze, "Design of a resilient system against shoulder surfing attack : adaptable to USSD channel," *Research Square*, pp. 1–19, 2023, doi: 10.21203/rs.3.rs-2793844/v1 License:

[19] D. Carrillo-Torres, J. A. Pérez-Díaz, J. A. Cantoral-Ceballos, and C. Vargas-Rosales, "A novel multi-factor authentication algorithm based on image recognition and user established relations," *Applied Sciences (Switzerland)*, vol. 13, no. 3, 2023, doi: 10.3390/app13031374.

[20] T. Edirisooriya and E. Jayatunga, "Comparative study of face detection methods for robust face recognition systems," *5th SLAAI - International Conference on Artificial Intelligence and 17th Annual Sessions, SLAAI-ICAI 2021*, no. December, 2021, doi: 10.1109/SLAAI-ICAI54477.2021.9664689.
[21] E. U. Omede, A. E. Edje, M. I. Akazue, H. Utomwen, and A. A. Ojugo, "IMANoBAS: an improved multi-mode alert notification IoT-based anti-burglar defense system," *Journal of Computing, Theory and Applications*, vol. 1, no. 3, pp. 273–283, Feb. 2024, doi: 10.62411/jcta.9541.
[22] Y. K. Mali and A. Mohanpurkar, "Advanced pin entry method by resisting shoulder surfing attacks," *Proceedings - IEEE International Conference on Information Processing, ICIP 2015*, pp. 37–42, 2016, doi: 10.1109/INFOP.2015.7489347.
[23] W. A. Hammood, R. A. Arshah, S. Mohamad Asmara, and O. A. Hammood, "User authentication model based on mobile phone IMEI number: a proposed method application for online banking system," *Proceedings - 2021 International Conference on Software Engineering and Computer Systems and 4th International Conference on Computational Science and Information Management, ICSECS-ICOCSIM 2021*, vol. 13, no. August, pp. 411–416, 2021, doi: 10.1109/ICSECS52883.2021.00081.
[24] S. K. Sahu, A. K. Dalai, and S. K. Jena, "Varying password based scheme for user authentication," *Advances in Computer Networks and Informatics*, vol. 2, no. July 2015, pp. 1–3, 2014, doi: 10.1007/978-3-319-07350-7.
[25] J. K. Oladele *et al.*, "BEHeDaS: a blockchain electronic health data system for secure medical records exchange," *Journal of Computing Theories and Applications*, vol. 1, no. 3, pp. 231–242, 2024, doi: 10.62411/jcta.9509.
[26] B. O. Malasowe, F. O. Aghware, M. D. Okpor, E. B. Edim, R. E. Ako, and A. A. Ojugo, "Techniques and best practices for handling cybersecurity risks in educational technology environment (EdTech)," *NIPES - Journal of Science and Technology Research*, vol. 6, no. 2, pp. 293–311, 2024, doi: 10.5281/zenodo.12617068.
[27] R. E. Yoro *et al.*, "Adaptive DDoS detection mode in software-defined SIP-VoIP using transfer learning with boosted meta-learner," PLoS One, vol. 20, no. 6, p. e0326571, Jun. 2025, doi: 10.1371/journal.pone.0326571.
[28] A. P. Binitie, O. S. Innocent, F. Egbokhare, and A. O. Egwali, "Implementing existing authentication models in USSD channel," in *International Conference on Electrical, Computer, and Energy Technologies, ICECET 2021*, Dec. 2021, pp. 1–5, doi: 10.1109/ICECET52533.2021.9698659.
[29] G. Tchouassi and C. Reads, "Can mobile phones really work to extend banking services to the unbanked ? Can Mobile Phones Really Work to Extend Banking Services to the Unbanked ? Empirical Lessons from Selected Sub-Saharan Africa Countries," *International Journal of Developing Societies*, vol. 1, no. 2, pp. 70–81, 2021.
[30] N. Kausar, I. U. Din, M. A. Khan, A. Almogren, and B. S. Kim, "GRA-PIN: A graphical and PIN-based hybrid authentication approach for smart devices," *Sensors*, vol. 22, no. 4, p. 1349, 2022, doi: 10.3390/s22041349.
[31] K. Fartash, T. Baramaki, M. S. Khayytian, and N. R. Salekdeh, "Investigating diffusion of USSD technology in Iran," *Journal of Science and Technology Policy*, vol. 16, no. 2, pp. 41–58, 2023, doi: 10.22034/jstp.2023.11271.1632.
[32] K. Bindhu, C. Chaithra, K. . Lakshmi, D. . Namratha, and Y. . Manu, "Preventing a shoulder surfing attack using graphical authentication system," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 5, pp. 2458–2462, 2023.
[33] D. R. I. M. Setiadi, A. Susanto, K. Nugroho, A. R. Muslikh, A. A. Ojugo, and H. S. Gan, "Rice yield forecasting using hybrid quantum deep learning model," *Computers*, vol. 13, no. 8, pp. 1–18, 2024, doi: 10.3390/computers13080191.
[34] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, vol. 7, no. 2, pp. 229–233, Jun. 2021, doi: 10.1016/j.icte.2020.09.002.
[35] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *SSRN Electronic Journal*, 2015, doi: 10.2139/ssrn.2580664.
[36] D. R. I. M. Setiadi *et al.*, "Single qubit quantum logistic-sine XYZ-rotation maps: an ultra-wide range dynamics for image encryption," *Computers, Materials & Continua* vol. 83, no. 2, pp. 1–28, 2025, doi: 10.32604/cmc.2025.063729.
[37] M. Prakash, "A Study on consumer perception towards digital payment," *East Asian Journal of Multidisciplinary Research* vol. 1, no. 6, pp. 1033–1044, Jul. 2022, doi: 10.55927/eajmr.v1i6.688.
[38] P. A. Onoma *et al.*, "Investigating an anomaly-based intrusion detection via tree-based adaptive boosting ensemble," *Journal of Fuzzy Systems and Control*, vol. 3, no. 1, pp. 90–97, 2025, doi: 10.59247/jfsc.v3i1.279.
[39] A. Hussain and A. Matcharan, "The challenges of mobile banking application on novice users," *In AIP Conference Proceedings* no. September, 2022, doi: 10.1166/jctn.2019.7876.
[40] R. E. Ako *et al.*, "Pilot study on fibromyalgia disorder detection via XGBoosted stacked-learning with SMOTE-Tomek data balancing approach," *NIPES - Journal of Science and Technology Research*, vol. 7, no. 1, pp. 12–22, 2025, doi: 10.37933/nipes/7.1.2025.2.
[41] S. Sinha, "Blockchain for enhancing IoT privacy and security," *International Journal of Innovative Research in Computer Science and Technology*, vol. 12, no. 2, pp. 106–110, Mar. 2024, doi: 10.55524/ijircst.2024.12.2.18.
[42] A. Setiawan and Y. Y. Kerlooza, "Designing authorization procedures for multi-channel and public participation-based system architecture for civil registration and population data," *IOP Conference Series: Materials Science and Engineering*, vol. 662, no. 4, 2019, doi: 10.1088/1757-899X/662/4/042017.
[43] A. O. Eboka and A. A. Ojugo, "Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view," *International Journal of Modern Education and Computer Science*, vol. 12, no. 6, pp. 29–45, 2020, doi: 10.5815/ijmecs.2020.06.03.
[44] F. O. Aghware *et al.*, "Effects of data balancing in diabetes mellitus detection: a comparative XGBoost and random forest learning approach," *NIPES - Journal of Science and Technology Research*, vol. 7, no. 1, pp. 1–11, 2025, doi: 10.37933/nipes/7.1.2025.1.
[45] S. Kim, H. Noh, C. Kim, and S. Kim, "Study on analysis of commercial mobile keypad schemes and modeling of shoulder surfing attack," *Computer Science and Information Technology*, pp. 93–112, 2014, doi: 10.5121/csit.2014.41208.
[46] S. A. Sharna and S. A. Ali, "Image based password authentication system," *arXiv preprint arXiv:2205.12352*, pp. 1–5, 2022.
[47] S. K. Sahu, A. K. Dalai, and S. K. Jena, "Novel scheme for user authentication," no. February 2014, 2015.
[48] A. E. Ibor, E. B. Edim, and A. A. Ojugo, "Secure health information system with blockchain technology," *Journal of the Nigerian Society of Physical Sciences*, vol. 5, no. 2, p. 992, Apr. 2023, doi: 10.46481/jnsps.2023.992.
[49] P. A. Onoma *et al.*, "Voice-based dynamic time warping recognition scheme for enhanced database access security," *Journal of Fuzzy Systems and Control*, vol. 3, no. 1, pp. 81–89, 2025, doi: 10.59247/jfsc.v3i1.293.
[50] J. Agboi *et al.*, "Lung cancer detection using a hybridized contrast-based xception model on image data: a pilot study," *MSIS - International Journal of Advanced Computer Intelligence Systems*, vol. 4, no. 1, pp. 1–11, 2025, [Online]. Available: https://msis-press.com/paper/ijacis/4/1/21
[51] D. R. I. M. Setiadi, S. Widiono, A. N. Safriandono, and S. Budi, "Phishing website detection using bidirectional gated recurrent unit model and feature selection," *Journal of Future Artificial Intelligence and Technologies*, vol. 1, no. 2, pp. 75–83, Jul. 2024, doi: 10.62411/faith.2024-15.

[52] V. O. Geteloma *et al.*, "Enhanced data augmentation for predicting consumer churn rate with monetization and retention strategies: a pilot study," *Applied Engineering and Technology*, vol. 3, no. 1, pp. 35–51, 2024, doi: 10.31763/aet.v3i1.1408.
[53] A. P. Binitie and O. J. Babatunde, "Adapting user interface design to mitigate shoulder surfing attacks in USSD channel," *African Journal of Environment and Natural Science Research*, vol. 7, no. 1, pp. 13–27, 2024, doi: 10.52589/ajensr-dpcgwn0x.
[54] M. A. Hadi, I. A. Al-Baltah, and A. T. Zahary, "A survey on mobile payment applications and adopted theoretical models," *Sustainable Engineering and Innovation*, vol. 4, no. 2, pp. 112–126, 2022, doi: 10.37868/sei.v4i2.id163.
[55] A. P. Binitie, D. N. Akhator, and K. K. Chukwubueze, "Design of a resilient system against shoulder surfing attack : adaptable to USSD channel," *Research Square*, pp. 1–19, 2023, doi: 10.21203/rs.3.rs-2793844/v1.
[56] B. O. Malasowe, M. I. Akazue, E. A. Okpako, F. O. Aghware, A. A. Ojugo, and D. V. Ojie, "Adaptive learner-CBT with secured fault-tolerant and resumption capability for nigerian universities," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 8, pp. 135–142, 2023, doi: 10.14569/IJACSA.2023.0140816.

BIOGRAPHIES OF AUTHORS

Amaka Patience Binitie received her BSc in 2007 from Nnamdi Azikiwe University Awka, Nigeria, in 2007. She obtained her MSc degree in Computer science from Adamawa State University, Nigeria in 2015 and her Ph.D in computer Science from the University of Benin, Nigeria in 2023. She currently a Lecturer at the Federal College of Education Technical Asaba. She has lots of publications to her name. Her research interests are in the areas of cyber security, information technology, and artificial intelligence. She can be contacted at email: amaka.binitie@fcetasaba.edu.ng.

Sebastina Nkechi Okofu is a staff in the Department of Marketing and Entrepreneurship, Delta State University, Abraka, Nigeria. She studied at the University of Nigeria, Enugu State, for a BSc degree in Management, the University of Benin, Benin City, for an MSc. degree in Marketing, and the University of the Witwatersrand South Africa, for PhD in Marketing. She has a journey of almost eight years in academics and consistently strives to create an engaging learning environment where students become lifelong scholars. She is a dedicated teacher and researcher, and her research interests are mobile commerce, consumer behaviour, market research, and agricultural marketing. She can be contacted at email: okofuseb@gmail.com.

Margaret Dumebi Okpor received her B.Sc. and M.Sc. (Computer Science) in 1997 and 2014 respectively from the University of Benin; and Ph.D. in 2023 from the Ignatius Ajuru University of Education in Port-Harcourt, Rivers State. She lectures with the Department of Cybersecurity at the Delta State University of Science and Technology Ozoro. Her research interests include AI-driven identity management and access control, data science, and machine learning. She is also a member of the Nigerian Computer Society, and the Computer Professionals of Nigeria (CPN). She can be contacted at email: okpormd@dsust.edu.ng.

Kizito Eluemnor Anazia received his B.Sc. in 2001 from Ambrose Alli University, Ekpoma in Edo State; His M.Sc. in 2011 from the University of Port Harcourt, Rivers State, and Ph.D. in 2021 from Nnamdi Azikiwe University, Anambra State. He currently lectures with the Department of Information Systems and Technology at the Delta State University of Science and Technology, Ozoro. He is a member of the Nigerian Computer Society (NCS), Computer Professionals of Nigeria (CPN), Cyber Security Experts Association of Nigeria (CSEAN) and Information Technology Systems and Security Professionals (IT&SP). His research interest includes machine learning, data science, e-commerce, database management and analysis. He can be contacted at email: anaziake@dsust.edu.ng.

Arnold Adimabua Ojugo received his B.Sc. in 2000 from the Imo State University Owerri; M.Sc. in 2005 from the Nnamdi Azikiwe University Awka in Anambra State, and Ph.D. (all Computer Science) in 2013 from the Ebonyi State University Abakiliki respectively. He is a Professor with the Department of Computer and Data Science at the Federal University of Petroleum Resources Effurun. His research interest includes: Machine Intelligent Systems Computing, CyberSecurity, IoTs and Ubiquituous Computing. He serves as Academic Editor for: the Frontiers In Big Data – Database Management Section, PLOSOne, International Journal of Modern Education in Computer Science, Blockchain in Health Technology, Journal of Computing Theories and Application, Future of Artificial Intelligence and Tech., and Progress for Intelligent Computation and Application. He is a member of Nigerian Computer Society, Council of Computer Professionals of Nigeria, and International Association of Engineers. He can be contacted at email: ojugo.arnold@fupre.edu.ng.

Francisca Egbokhare is a Professor of Computer Science at the University of Benin, Nigeria. Her current research focus on software engineering with particular interest in software requirement elicitation. She is a full-time lecturer, a public speaker and an advocate for encouraging women in computing. She can be contacted at email: fegbokhare@uniben.edu.

Annie Egwali is a highly accomplished academia in Cybersecurity. She is a Professor at the Department of Computer Science, University of Benin in Nigeria. She has served as the Head of the Department, Dean of the Faculty of Science, and currently – a part of a research team at the University of Benin and CERN in Geneva, working on the Compact Muon Solenoid experiment. She has several textbooks and publications in reputable journals. She is an active member of various professional organizations, and has supervised numerous MSc and PhD. Her research interests are in Artificial Intelligence, Quantum Computing, and Internet of Things. She has also received several research grants, including the National Information Technology Development Agency and TETFund in Nigeria. She can be contacted at email: annie.egwali@uniben.edu.

Peace Oguguo Ezzeh obtained her BSc in 2009 from the Nnamdi Azikiwe University, Awka; MSc (Information Technology) in 2017 from the National Open University of Nigeria (NOUN). She is currently on her Doctoral Studies in Computer Science with a specialization in Software Engineering. She currently also Lecturer at Federal College of Education (Technical) Asaba, Nigeria. Her journey reflects a dedication to education, a passion for technology, and a commitment to empowering others, making her a significant figure in her community and academic world, with several publications. She can be contacted at email: peace.ezzeh@fcetasaba.edu.ng.

Rita Erhovwo Ako received her B.Sc. Industrial Mathematics in 2000 from the Delta State University Abraka in Delta State, Nigeria; M.Sc. Computer Science in 2005 from the University of Ibadan in Oyo State; M.Sc. Internet-Computer and System Security in 2006, and Ph.D. Computer Science in 2013 respectively from the University of Bradford, Bradford, United Kingdom. She is currently a Senior Lecturer with the Department of Computer Science at The Federal University of Petroleum Resources Effurun. She has several publications to her credit with research interests in: artificial intelligence, cybersecurity, e-commerce, and risk management. She is a member of Nigerian Computer Society. She can be contacted at email: ako.rita@fupre.edu.ng.

Victor Ochuko Geteloma received his B.Sc. in Computer Science from the Federal University of Petroleum Resources Effurun, Delta State, Nigeria in 2015; M.Sc. in Computer Science in 2019 from the Covenant University, Ogun State. He currently Lectures with the Department of Computer Science at the Federal University of Petroleum Resources Effurun. He has several publications to his credit. His research interests include: cyber security, cloud computing, e-government, technology adoption, and digital inclusion. He is also a member of the prestigious Nigerian Computer Society (NCS). He can be contacted at email: geteloma.victor@fupre.edu.ng.

Tabitha Chukwudi Aghaunor received her B.Sc. and M.Sc. in Computer Science from the University of Benin in Edo State in 2014 and 2017 respectively. She is currently a PostGraduate student at the School of Data Intelligence and Technology of the Robert Moriss University Pittsburg, Pennsylvania in United States. She also lectures with the Department of Computer Science at the University of Maritime Okerenkoko. She is a member of the Nigeria Computer Society (NCS) and the Council for the Registration of Computer Professionals of Nigeria (CPN). She can be contacted at email: tabitha.aghaunor@gmail.com.

Eferhire Valentine Ugbotu received his B.Sc. in 2017 and M.Sc. in 2022 (in Computer Science) from the Federal University of Petroleum Resources Effurun, Delta State in Nigeria; He also received a second M.Sc. (Data Science) in 2024 from the Department of Data Science at the University of Salford in United Kingdom. He currently is a Research Assistant with the University of Salford in United Kingdom. His research interests are in: data science with machine learning approaches, IoTs and cybersecurity. He can be contacted at email: eferhire.ugbotu@gmail.com.

Sunny Innocent Onyemenem received his B.Sc. Computer Science from the University of Nigeria Nssukka in 20026; MSc in Info Technology from the University of Aberdeen in 2022. He currently lectures with the Department of Computer Science at The Federal College of Education (Technical) Asaba in Nigeria. He has several publications to his credit with research interests in: Information Technology, Cybersecurity, e-commerce, and risk management. He is a member of the Nigerian Computer Society and the Council for the Registration of Computer Professionals in Nigeria. He can be contacted at email: innocentsunnyonyemenem@gmail.com.