International Journal of Science and Research Methodology (IJSRM)
Volume 29, Issue 5, May 2026 ijsrm.humanjournals.com ISSN: 2454-2008

# Robust Multi-Factor Authentication Mechanisms for Effective Attack Mitigation

**Amaka Eugenia Ngozi[1], Ezea Jonathan Ikechukwu[2], Okpalla Chidimma Lilian[3] Theodora Onwuama[4], Ibeneme-Sabinus Ifeoma Livina[5], Atomatofa Emmanuel Oghenero[6]**

[(1,5,6)] Department of Cybersecurity, School of Information and Communication Technology, Federal University of Technology, Owerri, Imo State, Nigeria.
[(2)] Department of Information Technology, First Bank Nigeria Ltd, 35 Marina Lagos, Nigeria.
[(3)] Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Owerri, Imo State, Nigeria.
[(4)] Toronto Business College, 4000 Victoria Park Avenue, Toronto ON M2H 3P4. Canada

Received: 21 March 2026 Revised: 11 April 2026 Accepted: 23 April 2026

**ABSTRACT:**

The mobile app authentication processes are faced with significant security challenges, primarily due to the focus of its authentication on user-centric verification methods. Hence, various attack mechanisms such as OTP interception, SIM swap, and SMS vulnerabilities among others underscore the urgent need for more robust security measures. However, the existing research highlights the limitations stemming from weaknesses of the transmission medium in the security chain and prompting the development of innovative approaches to minimize these vulnerabilities. Therefore, this research introduces a novel multi-factor authentication mechanism designed to mitigate the risks associated with conventional authentication methods. Thus, the system framework aims to enhance security at multiple layers, such as PIN authentication, device authentication and facial recognition authentication respectively. This research presents a comprehensive methodology for enhancing effective mobile app authentication through object-oriented analysis and design (OOAD) with Unified Modeling Language (UML), Leveraging tools such as Java programming language, Android Studio IDE, Google Cloud Fire store, and Android devices with camera features. Also, the research methodology comprises three modules: PIN factor design, device design, and facial image design. A successful completion of each module is a prerequisite to advancing to the next phase of design, ensuring systematic development and integration of authentication components. However, the system testing involving 200 users demonstrated the system's efficacy; with 89.5% of users successfully entering credentials below the expected time, 8.5% of users entered their credentials above the expected successfully and 2% of users entered their credentials at equal expected time, indicating efficient authentication performance. Similarly, the graphical representation of test data highlighted variations in timing across each batch module, which emphases the need for optimization and standardization to enhance user experience.

**Keywords:** Vulnerabilities, Interception, user Impersonation, Sensitive information, Transmission medium

## I. INTRODUCTION

The ubiquity of mobile banking apps deployment in this digital era has hugely transformed the transactional services of the banking operations to unparalleled conveniences. [17]. Though digital transformation ushered in both unprecedented conveniences and avenues for exploiting vulnerabilities in the banking systems [10]. Also, its growth has continuously posed a serious challenge to both customers and service providers due to incessant fraudulent attacks. [5]. Hence, the Short Message Service (SMS) attacks targeted at mobile apps users are exploding due to various attack mechanisms, such as Man-in-the-middle (MITM), replay, eavesdropping attacks among others. Similarly, the SMS-based authentication scheme is vulnerable since One –Time-Password (OTP) transmitted through SMS could be intercepted by the fraudsters to execute attacks. [6].

However, taking preventive measures to avert unauthorized users of mobile apps from accessing the authentication processes for transactions are fundamentally the goal of establishing the authentication settings and approaches**. [9]**. Unfortunately, the existing mobile apps authentication processes are solely user-centered, which is vulnerable to attack mechanisms as users compromise their sensitive information. [12]. Also, other attack mechanisms include One-Time-Process(OTP) interception, SMS-based vulnerabilities, user impersonation among others. [7]. Furthermore, [11] concurred with other researchers to ascertain that SMS lacked built-in mechanism to authenticate text messages and concludes that there is no security measure protecting the text messages as its been transmitted as data.

Similarly, the existing authentication factors, protocols, and methods of transmitting sensitive information to the legitimate users are vulnerable to various attack mechanisms, [5]. Unfortunately, the user's authentications are done through the user's registered SIM, which could be impersonated by the illegitimate users on SIM swap or theft, [9]. Besides, the users authentication requires generating OTP on any request initiated and transmits to the users SIM through Short Message Service (SMS), [16]

Obviously, SMS is one of the most accepted communication medium for mobile apps users, [17]. Unfortunately, it is vulnerable since the device where the SMS is transmitted could be stolen, or not at the possession of the legitimate user now the SMS is being delivered, [9]. Thus, all these attacks are not limited to human weakness, which include third-party involvement, compromise, transmission medium, rather it cuts across other attack mechanism such as Man-in-the-middle (MITM), replay, eavesdropping among others, [5]

However, having seen the weaknesses of the existing system, which majorly attributes to the vulnerabilities of both SMS-based authentication and its transmission medium, necessitated the need for this research. Hence, this research aimed at enhancing the mobile app authentication processes, focusing on the user authentication and user's device authentication. Therefore, a robust multi-factor authentication mechanism was designed for effective attack mitigation. Thus, the authentication processes were focused on both the user on 1st and 3rd authentication levels, and user's device on 2nd authentication level for secured communication.

Additionally, the research leverages the user's knowledge (K), possession (P), and Inheritance (I) factors respectively for the design of the multi-factor authentication mechanism. The KPI factors include personal identification number (PIN), device identities and facial image of the users. Nonetheless, the prospective user registers the PIN, device identities and facial image captured. The data collected are stored at the backend and intending users initiating request are authenticated accordingly. On successful authentication, grants the user an access to perform a transaction, otherwise, declines when the authentication is unsuccessful.

## II. Literature Review

Establishing customer satisfaction in the banking services requires diligent and efficient commitment, and a major key factor to survive in global banking industries demands a very high focus on the quality of service given to customers. [1]. Hence, a customer, who is satisfactorily impressed with the services of the banking systems, displays customer loyalty and this increases the global survival of the banking systems. [1]. Also, the growth and advancement of the banking systems are determined by the quality of services rendered to customers. [2]. However, technology has rapidly advanced the banking services, specifically on the customer's seamless access to their accounts through internet access and mobile devices usage. [8]. Contrarily, the emergence of the technological innovations equally introduced lots of security challenges, such as security breaches, cyber-attacks, among others. Hence, this deters the customer satisfaction and the reputation of the banking system. [8].

Thus, on the quest to maintain this customer satisfaction in the mobile app operational services has made other researchers think of various enhancement techniques for developing the authentication factors ranging from 1-2-3 and multi factor authentications, [3]. Unfortunately, the fraudsters have made the efforts of these researchers unfruitful by attacking the transmission medium, [15]. Nevertheless, irrespective of these security challenges, SMS-communication medium, remains a widely deployed communication technology [14]. Notably the customer's mobile devices are used in authentication, as One-Time-Password (OTP) is transmitted to the customers through SMS [9]. Though, many researchers, including [14], ascertained that SMS-communication medium is unsafe since the text messages are not encrypted and attackers utilize the loophole identified to defraud banking customers, resulting to account drainage.

Furthermore, SMS usage as a communication medium has been ascertained invalid to transmit sensitive information by many governmental bodies, such as National Institute of Standards and Technology (NIST) and National Cybersecurity Center (NCSC), in both United States and United Kingdom respectively [14]. Nonetheless, [13] noted in research titled "development and implementation using end-to-end encryption for SMS app', that encrypting only the bank SMS messages would be enough to avert the security challenge. Although,[9], contrarily opined that SMS as a communication medium of the banking systems will consistently face the security challenge, since the sensitive information is being transmitted. However, other closely related works reviewed such as [4,9,5,13], revealed that mobile banking apps are faced with lots of security challenges due to poor authentication medium.

## III. Materials and methods

### a. Research materials

Object oriented Analysis and design (OOAD), incorporating Unified Modeling Language (UML) was adopted in this research to aid the effective design communication of the research. Also, other tools used in this research are not limited to Java programming language, Android studio Integrated Development Environment (IDE) Google cloud Fire store, and Android devices with camera features.

b. Composition of the authentication factors and its processes.

The user's data regarding the PIN, device identity and facial image are collected at the registration phase and stored at the backend for subsequent authentication references. Hence, the first factor composition is Knowledge factor: the user was allowed to choose a maximum of 4 digit numbers ranging from (0-9) as Personal Identification Number (PIN) for the first authentication factor. Thus, the chosen PIN was registered with the system and as well used as a gateway access to the system on any request initiation. Hence, when a user initiates a request, the PIN authentication starts its processes and has maximum of two attempts of authentications. However, if both attempts fail on its authentications, the process declines, otherwise, if either of the authentication attempts is successful, it calls for user's device authentication, which is done automatically.

Similarly, as the user's device authentication is processing, whether successful or unsuccessful, there must be a pop-up indicating the processing status. So, when the authentication is unsuccessful, the pop-up will be device not registered, while the pop-up on successful authentication instructs the user to position the face well for capturing. Lastly, when the user's facial image is captured; it undergoes an authentication process and the successful authentication grants the user access to perform a transaction otherwise, declines the process if unsuccessfully done.

c. Design Process

The research design was captured on Figure 1.

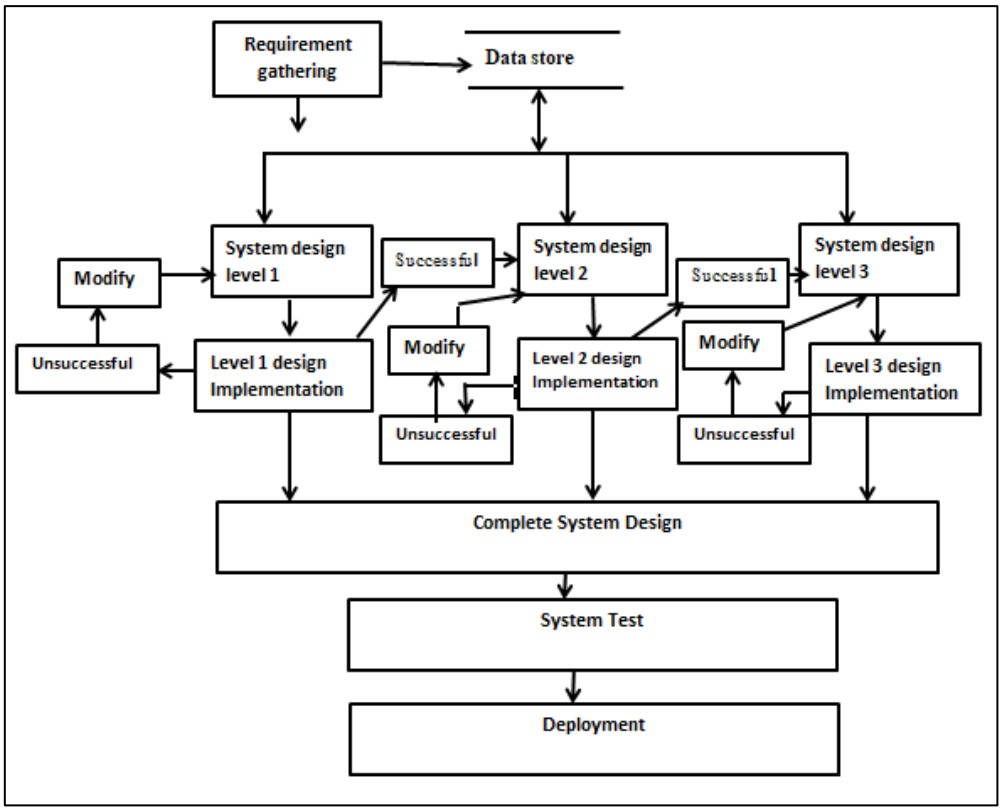


**Figure 1: System design**

The research design as depicted on figure 1, is designed in three modules but prior to the first module design, is a requirement gathering, where the user's data are collected and stored at the backend. Then at the first module design, the system design level 1, which is the PIN factor design, was carried out with its implementation to ascertain the design status. However, the successful design of the first module leads to the system design level 2, which is the device design, otherwise, its failure requires modification and re-implementation, which must be recorded successfully before proceeding to the device design module. Also, the successful module design of the device, demands for the last module design of the facial image of the user. Therefore, at successful design of these modules requires integration to put them together and have a complete system design. The design process is captured on Figure 2.

**Stage 1: Registration**
**Step 1:**
$U_i \rightarrow (PIN)$
$U_i \rightarrow Fri$
**Step 2:**
$CS \rightarrow (PIN, Fr_i)$
$CS \rightarrow U_{TK} = h(PIN_i||Fr_i) \bmod P$
$CS \leftarrow U_{TK}$
**Step 3:**
$U_i \rightarrow (D_{in}, D_T, D_N)$
$CS \rightarrow (Din, D_T, D_N)$ and computes $D_{TK} = h(D_{IN} || D_T || D_N) \bmod P$
$CS \leftarrow D_{TK}$
**Stage 2: User Login and Authentication**
$U_i \rightarrow (PIN_i, Fr_i)$
$CS \rightarrow U_{uid}$ and computes for $U_{TK} = h(PINi||Fri||Pu||ni||ti||) \bmod P$
$CS \oplus U_{TK}^* = U_{TK}$, to query $D_{uid}$, othw abort the operation when $U_{TK}^* \neq U_{TK}$
$CS \rightarrow (D_{in}, D_T, D_N)$
$CS \rightarrow D_{TK} = h(D_{IN}||D_T||D_N||ni||ti||Pu) \bmod P$
$CS \oplus D_{TK}^* = D_{TK}$ to generate $SK_{uid}$ and $S_{ui}$ othw abort the process when $D_{TK}^* \neq D_{TK}$
$SK_{UID} = h(U_{TK}||D_{TK}||ni||Pui||ti) \bmod P$
$S_{ui} = h(P_k||ni||U_{TK}||D_{TK}||ti) \bmod P$
$CS \leftarrow (SK_i, S_{ui})$
**Stage 3: Device Identity Update**
User requests for change of device
$U_i \rightarrow D_{Vi}^*$ to $D_{Vi}^{**}$
$CS \rightarrow D_T^*, D_N^*, D_{IN}^*$ and computes $D_{TK} = h(D_T||D_N||D_{IN}) \bmod P$
$CS \oplus D_{TK}^* = D_{TK}$ to request for $D_T^{**}, D_N^{**}, D_{IN}^{**}$ othw abort the operation if $D_{TK}^* \neq D_{TK}$
$U_i \rightarrow D_T^{**}, D_N^{**}, D_{IN}^{**}$
$CS \rightarrow D_{TK}^{**} = h(D_T||D_N||D_{IN}||ni||ti||Pu) \bmod P$
$CS \rightarrow D_{TK}^* - D_{TK}^{**}$
**Stage 4: User Identity Update**
User requests for identity update
$U_i \rightarrow PIN_i^*$
$CS \rightarrow Sq_i$
$U_i \rightarrow Sq_i$
$CS \oplus U_i^{res*} = U_i^{res}$ to proceed, othw, aborts when $U_i^{res*} \neq U_i^{res}$
$U_i \rightarrow PIN_i^{**}$ and $\rightarrow PIN_i^{**}$
$CS \rightarrow U_{TK} = h(PIN_i||Fr_i||n_i||t_i||P_u) \bmod P$
$CS \rightarrow U_{TK}^* - U_{TK}^{**}$

**Figure 2: Design process**

The design process of this research was done on four stages, which includes stage 1 - 4 respectively. The stage 1 was the registration where the user's PIN, and facial image were captured on step 1, while step 2 generated the user's token $U_{TK}$ and step 3 captured the device identities and generated the device token $D_{TK}$. However, the stage 2 was the user login and authentication processes, where the three authentication factors must be successfully authenticated before secret key (SK) will be generated for onward transmission to complete the transaction. Hence, stage 4 gives the user update, which requires both user's identity and device update.

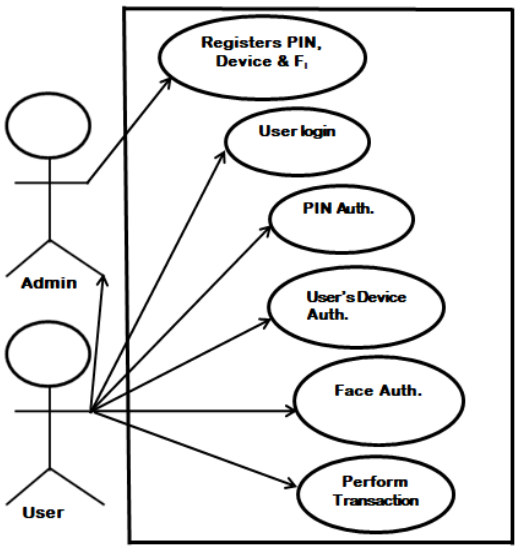


**Figure 3: Use case diagram of the system**

Figure 3 provides a graphical depiction of how a user interacts with the system. Thus, the user participates actively in both the first and third authentications, while the second authentication of the device is done on the background. However, a PIN is used for the first user authentication, and a facial image is used for the third. As a result, the user's PIN authentication is verified when they log in. After a successful authentication, the device's IMEI number of the initiator is verified, and finally, the user's face image is verified before access is granted to that user. Though the user's first and third authentication has maximum of two attempts and device authentication is only done once. Consequently, a failure of each factor authentication declines the process.

3.4 System Scheme

**Table 1: Parameters of the system's authentication scheme**

| Symbols for the parameters | Definitions of the symbols |
|---|---|
| A | "Registered PIN" |
| Λ | "Inputted PIN" |
| B | "Registered Facial Image" |
| Φ | "Captured Facial Image" |
| ∞ | " Backend/Registered IMEI number" |
| δ | "Device Auth." |

**Authentication scheme**

Input ("Enter PIN")
If $\alpha = \lambda$, then
If $\infty = \delta$, then
Input ("Position your face for capturing")
If $\beta = \Phi$, then
Perform Transaction
Else output ("Face Mismatch")
End
Else output ("device not registered")
End
Else output ("Incorrect PIN")
End.

Authentication Logic Table - AND GATE

In Table 2, 0 represents failed authentication while 1 represents successful authentication. Transactions can only happen if the three authentication layers are successful, hence we have result output authentication of 1. It is an AND table and only produces a positive result when all conditions are fulfilled.

**Table 2 : Authentication Logic Table - AND GATE**

| PIN | DEVICE | FACIAL | RESULT |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 |

3.5: Research design

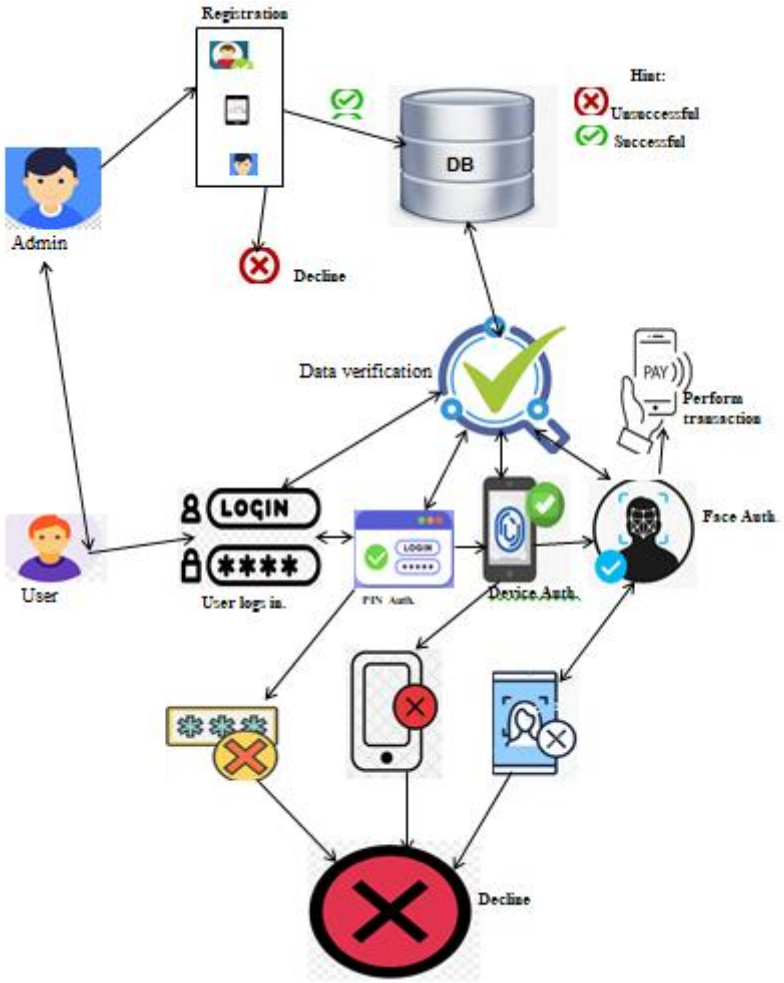


**Figure 4: System Architecture**

The design of the system as captured on Figure 4 shows where a prospective user approaches the Admin for registration, while presenting correct credentials. Hence, the admin registers the user's PIN, device IMEI number and captures the facial image of such user. All these data when collected are stored at the backend. When the user wishes to initiate a request, he logs into the system with the PIN, which is authenticated to ascertain the legitimacy of the user's claim. Thus, the authentication of the PIN has a maximum of two attempts, and if either of the attempts is successful, calls for user's device authentication, otherwise, the process declines at the failure of the two attempts. Similarly, the successful authentication of the device, which is automatically done once, leads to the user's face authentication. Though the process declines at each specified failure of the authentication process and performs a transaction at the successful authentication of the three processes.

IV. Results

Stratified sampling technique was adopted for testing the new system. Perhaps, only 200 users were selected and grouped into subgroups of 20users in a batch, given a total of 10 batches. Though the user's age, gender, educational level and knowledge of information technology were strictly considered. Also, the testing focused on the users' pace on PIN entering, adherence of users to instructions, device authentication speed and system's processing speed. Thus, the expected time allotted to each user for entering the credentials successfully was 20 seconds, which was an aggregate time generated from pre-testing of the system. Hence, the test scores as obtained were recorded as above, below, and equal expected time respectively.

However, the summary of the unit testing is given on Table 2. Each batch module specifies the total number of users that successfully entered their credentials below the expected time, above or equal expected time as the case may be. The result obtained showed that 179 users of 89.5% were able to enter their credentials successfully below the expected time, irrespective of the users' knowledge of information technology. Similarly, other results obtained showed 17 users of 8.5% and 04 users of 2% entered their credentials successfully at above and equal expected time respectively. Also, the test score obtained on the test of user's device speed for

authentication and processing speed equally showed a very high speed on both the authentication and processing speed. Though network challenge posed a severe drawback to maintain consistency on the systems' performance.

Nonetheless, the percentage ratio of the test scores as captured on Table 2 is calculated as follows:

N = 200, (total number of test users). Below expected time ($B_{ET}$) = 179 ( total number of users below the expected time).

Thus, $(B_{ET} /N) X 100$ (i)

$= (179/200) X 100$

$= 89.5\%$

Furthermore, 17 users as seen on the same Table, successfully entered their credentials above the expected time ($A_{ET}$). Thus, figuring out the given number's percentage ratio yields the following result:

N = 200, (total number of test users). $A_{ET}$ = 17 (number of users above the expected time).

Therefore, $(A_{ET} /N) X 100$ (ii)

$= (17/200) X 100$

$= 8.5\%$

Finally, only nine (04) users were able to successfully enter their login information at the scheduled equal-expected time ($E_{ET}$). As a result, the following is the stated number's percentage ratio:

N = 200, which is the total number of test users. $E_{ET}$ = 04

This gives us $(E_{ET}/N) X 100$ (iii)

$= (04/200) X 100$

$= 2\%$

**Table 3: Summary of the unit testing**

| Batch Module Test | Below Expected Time ($B_{ET}$) | Above Expected Time ($A_{ET}$) | Equal with Expected Time ($E_{ET}$) |
|---|---|---|---|
| 1st batch module | 18 | 2 | 0 |
| 2nd batch module | 19 | 1 | 1 |
| 3rd batch module | 16 | 4 | 0 |
| 4th batch module | 19 | 1 | 0 |
| 5th batch module | 19 | 1 | 0 |
| 6th batch module | 17 | 3 | 0 |
| 7th batch module | 18 | 2 | 1 |
| 8th batch module | 19 | 1 | 2 |
| 9th batch module | 20 | 0 | 0 |
| 10th batch module | 18 | 2 | 0 |
| **Total** | **179** | **17** | **04** |

Also, the graphical representation of Table 3 is given in Figure 2.

The test data elements were depicted on the graphical representation on figure 2. Thus, the graphical bar charts showed the test data as captured below the expected time, above expected time, and equal expected time respectively. Hence, the 9th batch module recorded 100% from the inputs of all the users that entered their credentials successfully. On the other, 3rd batch module recorded the least with 80% from 16 users that entered their credentials successfully. Similarly, it is only the 9th batch module that recorded "0" input on above expected time, whereas other batch modules had their inputs recorded. Also, only batch modules 2nd, 7th, and 8th

had their inputs recorded at equal expected time, while other batch modules, such as 1st, 3rd - 6th and 9th – 10th had zero inputs at equal expected time.

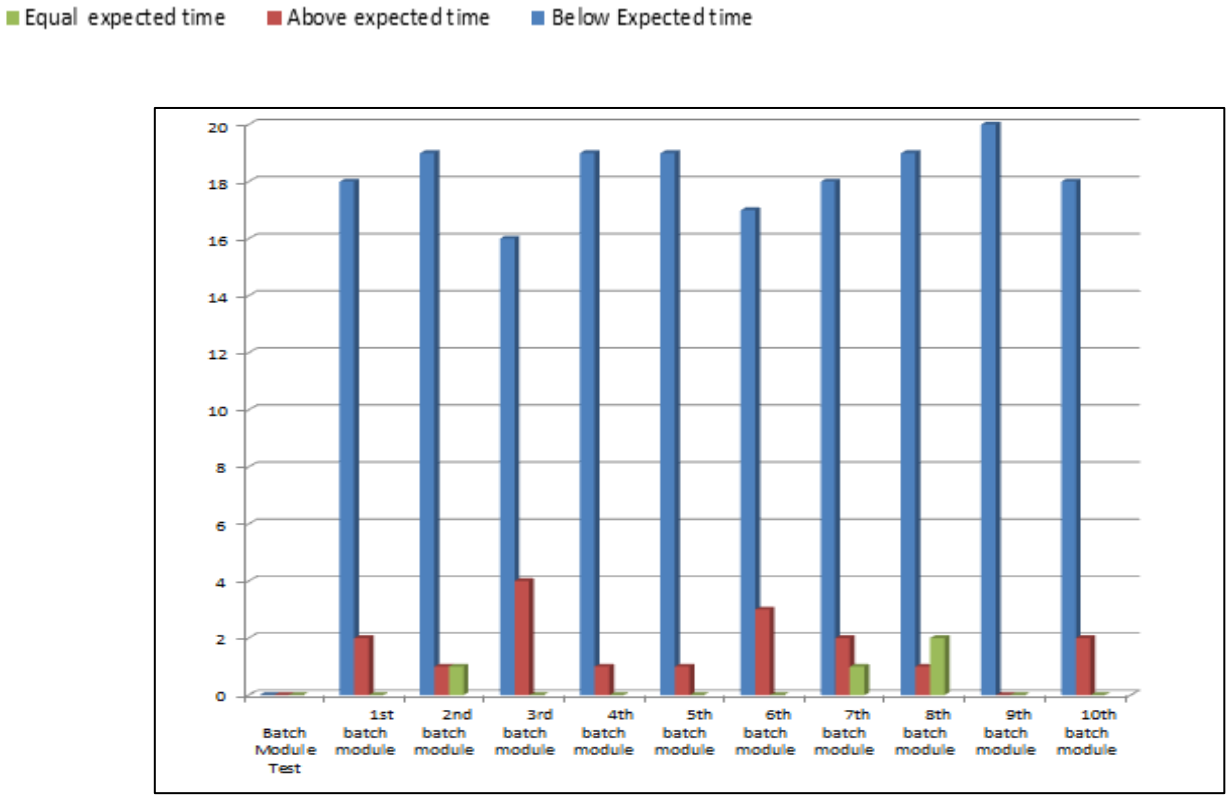


**Figure 5: Graphical representation of unit test summary**

## V. Conclusion

The user authentication at all levels of the authentication processes in this research invariably averts the illegitimate attempts to execute attacks. Obviously, it is practically impossible for the fraudsters to bypass all these authentication processes demonstrated in this research, even with user compromise. Similarly, legitimate users on the other hand, can longer compromise their sensitive information since the 3rd authentication factor involves the user's live facial image for capturing and authentication. Therefore, user compromise, impersonation, eavesdropping, phone theft, among others are totally minimized by the authentication processes of this research. The research recommends a further research on biometric security to avert spoofing attacks on the user's images.

## REFERENCES

[1] Achmad, S., Bambang, B. W., and Burhanuddin, B., (2024). Effects of service quality and customer satisfaction on loyalty of bank customers. Cogent business and management, 8.1, Doi:10.1080/23311975.2021
[2] Alallq, H.A.E., (2024). The impact of quality of banking services on the customer satisfaction in small and medium banks. South Asisn journal of social sciences and humanities. ISSN: 2582-7065 (online) SAJSSH, vol.5, issue 2, pp35-44
[3] Ali, G., Dida, M. A., & Sam, A. E. (2020). Two-factor authentication scheme for mobile money: A review of threat models and countermeasures. *Future Internet*, *12*(10), 1–27. https://doi.org/10.3390/fi12100160
[4] Alioune, D., Jordan, S, Tegawende, B., and Jacques, K.,(2024). Insecurity of mobile apps in developing countries. A systematic literature review. Computer science >Cryptography and security. arXiv:2405.05117v2(CS), 1-18
[5] Akintola, G. B., (2024), Assessing the vulnerabilities of online digital mobile banking applications in Nigeria. International journal of sientific research in multidisciplinary studies. Vol. 10, issue 7, pp 29-45, retrieved online at www.isroset.org.
[6] Amador, P., Martinez-Gonzalex, M. M. and Payo, V.C. (2023). App-based detection of vulnerable implementations of OTP SMS APIs in the banking sector. Wireless network. Retrieved online: https://doi.org/10.1007/s11276-023-03455-w. pps 1-15
[7] Deshpande, S. and Jethani V (2021)Multi-factor authentication on mobile phones using existing brightPass. Turkish journal of computer science and mathematical education. Trabzon vol. 12, ISS 12,pp 948-9531
[8] Dewi, C. S., and Zulkifli Z. (2024). E-banking Technology: A comprehensive study on customer satisfaction and bank services. International journal of business, law and education. Vol. 5, no. 2, pp 1655-1665. Doi:https://doi.org/10.567442/ijblev512.708
[9] Festus-Amaka, E.N, Odii, J.N, Isa,A.I, Okolie, S.A, Ayogu, I.I (2023), Robust Authentication medium for safety of financial

transactions. journal of science and logics in ICT research. University of ibadan, 10(1), 1-7
[10] Hassan, A. O., Ewuga, S. K, Abdul, A.A, Abrahams, T. O, Oladeinde, M., and Dawodu, S. O, (2024). Cubersecurity in banking: A global perspective with a focus on Nigerian practices. Computer science and IT research journal, vol. 5, issue 1, pp 41-59. Doi:10.51594/csitry.v5i.701
[11] Khan et al (2023), Role of authentication factal, vol. 5, issue ors in Fin-Tech mobile transaction security. Journal of big data; 10:138, pgs 1-37
[12] Mayhoffer R. and Sigg, S. (2021). Adversary models for mobile device authentication. *ACM computing surveys*, 54(9), Article 198, 1-22
[13] Muhammad, I. U., Muhammad, M. L., Joshua, A., Timothy, M, and Agushaka, J., (2024). Banks short message service threats notification system on an Android based phone. FUDMA journal of sciences (FJS), vol. 8, No. 2, pp 46-58, Doi:https://doi.org/10.33003/fs-2024-0802-2339
[14] Peeters, C., Patton, C., Munyaka, I. N. S., Olszewski, D., Shrimpton, T., and Traynor, P., (2022): SMS OTP security (SOS) hardening SMS-based two factor Authentication. 2022 ACM Asia conference on computer and communications security (Asia CCS'22), 15 pages.Doi:https://doi.org/10.1145/3488932.3497756
[15] Reyes, A. R. L., Festijo, E. D., & Medina, R. P. (2019). *Enhanced Multi - factor Out - of - Band Authentication En Route to Securing SMS - based OTP*. International journal of engineering and technology innovation 9(2) 145-154
[16] Suneetha, M., Reddy, L. N., Teja, A. S., and Ghrinesh, M. G., (2024). An OTP based secure online transaction using facing recognition. International journal of novel research and development. (IJNRD), IJNRD.org, ISSN:2456-4184, v0l9, issue 3, pp 282-289
[17] Umar, M.I., Liman, M.M., Abah, J., Moses, T. and Agushaka, J. (2024). Banks short message service threats notification system on an Android based phone. FUDMA journal of sciences (FJS), vol. 8, No. 2, pp 46-58, Doi:https://doi.org/10.33003/fs-2024-0802-2339

How to cite this article:
Amaka Eugenia Ngozi et al. Ijsrm.Human, 2026; Vol. 29 (5): 58-66.
Conflict of Interest Statement: All authors have nothing else to disclose.