Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 7 No. 4 (2023) 797 - 808 ISSN Media Electronic: 2580-0760

Utilization of Mobile Network Infrastructure to Prevent Financial Mobile Application Account Takeover

Aldiansah Prayogi[1], Rizal Fathoni Aji[2]
[1, 2]Magister Teknologi Informasi, Universitas Indonesia
[1]aldiansah.prayogi11@ui.ac.id, [2]rizal@cs.ui.ac.id

Abstract

The Covid-19 pandemic has kept almost everyone at home and forced them to do activity online using their mobile gadgets. Penetration of internet and mobile use are increased as lockdowns or restrictions on meeting face to face are getting used to. This has become a new market for cyber criminals to carry out their actions, such as spreading Social Engineering, sending Phishing, doing Account Take Over, and ending in theft of money in Financial Mobile Applications. Application protection with OTP SMS and Magic Link SMS still has vulnerabilities with several examples of cases that have occurred. For this reason, this problem was raised to find a solution by utilizing the Mobile Network Infrastructure. The research methodology used is a quantitative experiment and literature review of previous studies to compare the uniqueness of this study. The experiment was carried out by comparing the compatibility between the phone numbers registered in the application and the phone numbers used on smartphones. Every time a user signs in or signs up, the Financial Mobile Application will perform Mobile Network Verification to cellular operators via API. Verification is carried out by utilizing the header enrichment in the background of the application process that installed on the user's smartphone or tablet to the Mobile Network Verification Server. Then the Financial Mobile Applications can find out, the user is using a valid or invalid phone number. Thus, the target account cannot be taken over, because the cyber criminal's mobile gadget does not have the phone number which is attached in the victim's mobile gadget. This proof was carried out with four test case scenarios with 10 trials each with the sign-up and sign-in processes on the same phone number and differed between devices and applications. The results obtained from the four test case scenarios and each of the 10 trials were 100% successful as expected results. It is hoped that this kind of protection model can reduce losses experienced by Financial Mobile Application users due to Account Take Over.

Keywords: SMS OTP vulnerability; mobile network verification; header enrichment; account takeover prevention

1. Introduction

Mobile technology use has increased rapidly since the beginning of the Covid 19 pandemic. The imposition of restrictions on community activities and lockdowns has forced people to do many things online through applications on their gadgets. The impact of the Covid 19 pandemic has been felt in the penetration of internet access via mobile, one of which is in Indonesia. Based on a survey conducted by the Association of Indonesian Internet Service Providers, internet penetration in Indonesia increased by 73.7% from 2019-2020 and increased by 77.02% from 2021-2022 [1]. In addition, 89.03% are mobile/tablet users, 0.73% are computer/laptop users, and 10.24% are users of both [1]. Then of all these users, 77.64% use data access from cellular operators [1]. This shows how massive the use of cellular applications using cellular operator mobile data is for the people of Indonesia.

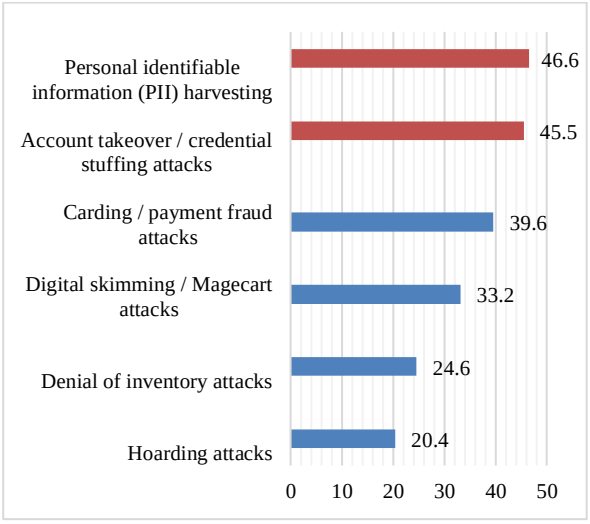

Figure 1. Most organizational concerning on mobile application attacks [2].

Accepted: 03-04-2023 | Received in revised: 18-06-2023 | Published: 12-08-2023

The widespread use of internet access via mobile, in addition to providing opportunities for application business players, is also under the spotlight of cybercriminals to take advantage of it. As an example of the latest case in Indonesia in January 2023, 13 cybercriminals were caught and succeeded in exploiting 493 victims with a loss of 12 billion rupiahs [3]. These cybercriminals use social engineering which is a method of tricking victims into obtaining confidential information, such as passwords, secret questions, and anything that is useful for exploiting accounts [4]. Convincing false information is sent via social media containing phishing links and fake apps APK. Most of their targets are bank customers and e-wallet users. Then they use the phishing method with the impersonation of the official website to get sign-in information from the victim [5] and use mobile malware to exploit smartphones [6] in the form of a fake app APK which is capable of accessing SMS inboxes then forwarding OTP or Magic Link.

Cybercriminals use phishing to get the victim's user sign-in and use installed fake app APK on the victim devices to access SMS inbox, then get the One Time Password (OTP) or forward Magic Link. Even though the security of the application has used Two Factor Authentication (2FA) which integrated with telco infrastructure to send SMS OTP/Magic Link, Account Take Over (ATO) still occurs and still become challenges [7]. This ATO scam apart from committing identity theft to gain access to victims' accounts, also allows them to make unauthorized transactions [8]. Most victims did not receive compensation from Financial Mobile Application providers because customers were deemed negligent, so that the cybercrimes that have occurred recently are quite troubling to the people of Indonesia.

The urgency regarding this attack can also be seen from the Cyberthreat Defense Report in 2022 conducted by the Cyber Edge Group in Figure 1. Respondents consisting of 1200 IT security decision makers and practitioners from organizations with a minimum of 500 employees were asked to choose 3 of the most concern attacks on the mobile application. The two attacks that have become the most concerning are PII harvesting which increased from 39.7% (2021) to 46.6% (2022) and ATO/credential stuffing attacks which increased from 43.7% (2021) to 45.5% (2022) [2]. 90.3% of surveyed organizations indicated that they were concerned with one or more of the mobile attacks on the list [2].

Literature review is carried out in this paper to obtain previous studies that are close to the topic of Financial Mobile Application Account Take Over Prevention. Research on authentication on mobile money using USSD has been carried out, but it still has many vulnerabilities, so additional multi-factor authentication protection is needed [9] - [11]. Two and three factor authentication have also been proposed using passwords, smart cards, and biometrics [12], [13], but vulnerabilities still exist, namely used stolen certificates and fake biometrics by adversary [14]. Propose authentication models using password less and FIDO [15] adoption have also been carried out, but radical transformation needs to be run by financial institutions that are still using password-based authentication [16]. Writing from the results of a literature review regarding security in the online banking system has been discussed, such as the proposal to make a SIM card for verification, authentication, PKI, digital watermarking, and personal digital identity, but this concept has not been tested yet[17], [18]. Then another proposed model of multi-factor authentication using the MAC address, mobile number, IMEI, and SIM serial number (SSN) which need to integrated with cellular provider, has been discussed, but it is only a concept and has not been tested yet [19]. This research takes a distinguishing position from previous studies on the use of cellular infrastructure as an additional authentication factor and conducts real trials.

Based on literature review and the problems shown in Indonesia's cases where there are still exploited victims even though there are utilization of OTP/Magic Link and organization survey results that showing high concern for ATO, the research question of this journal is how to deal with ATO attacks by utilizing cellular network infrastructure. This study aims to provide solutions to Financial Mobile Application providers to protect their customers from ATO attacks. This solution will also very helpful to the public people who use mobile finance apps to circumvent ATO that perpetrated by cybercriminals.

2. Research Methods

In this work there are 3 processes, namely the design of cellular network topology verification, API flow design, and the assessment process. Verification by utilizing cellular network infrastructure will be illustrated by the two designs. Then this system will be evaluated whether it is in accordance with the objectives of this study. Following are the sub-sections of each process in more detail.

2.1 Mobile Network Verification Topology Design

Figure 2 illustrates the high-level topology which is used to perform Mobile Network Verification (MNV). In terms of flow, Financial Mobile Application users when they want to sign-in or sign-up, access will be directed to use the cellular network. The smartphone or tablet will be connected to the Base Transceiver Station (BTS), which is one of the main components that functions to connect user devices to the cellular network [20]. Then the BTS device will be connected to the core network which consists of 3 main components, namely

DOI: https://doi.org/10.29207/resti.v7i4.5025

Mobility Management Entity (MME), Serving Gateway (SGW), Gateway GPRS Support Node/Packet Gateway (GGSN/PGW).

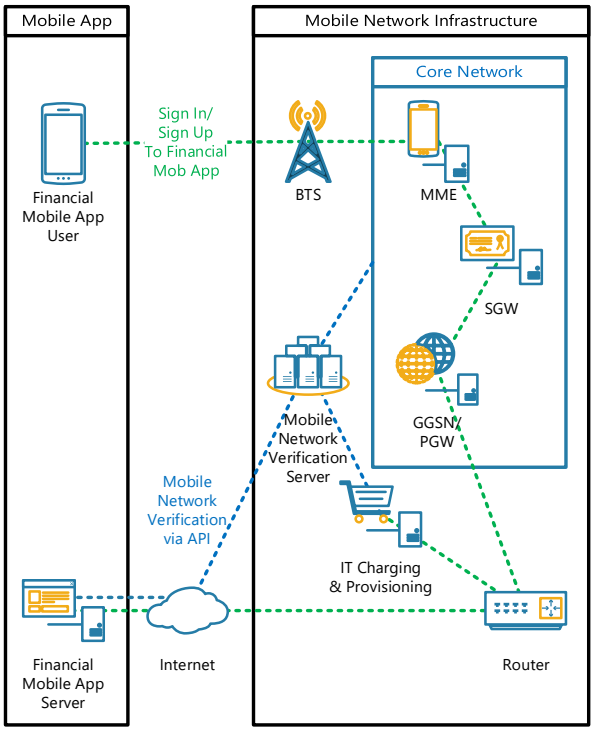

Figure 2. High level MNV topology design.

MME has functions to perform tracking, paging, and signal control procedures that match individual User Equipment (UE) with serving cells that are useful for exchanging data packets [21]. MME will forward the packet to the SGW whose function is to regulate, forward the direction of the data path, and as an inter-handover from the UE to other controllers [22]. Then SGW will work with GGSN/PGW which has the function to ensure and regulate or serve as a termination point for data packet connections to the Internet [23]. From the Internet it will be connected to the Financial Mobile App Server and that is how the high-level flow of the EU can be connected using mobile applications and cellular networks.

To verify and validate whether the user who is signing in or signing up matches the phone number between the one registered and the one being used, the Financial Mobile App Server will ask the MNV Server via API. MNV Server performs a header enrichment method which can identify subscriber profiles in core network [24], two of parameters are the mobile number and the IP source used by UE. Each verification transaction to MNV will be recorded, then this transaction will be charged at IT Charging and Provisioning. A more detailed description will be explained in the Flow Design API.

2.2 API Flow Design

The API flow between the Financial Mobile App Server and the MNV Server in the Figure 3, begins with the access from a smartphone or tablet to the application. When signing in or signing up, 2FA which is useful as a defense guard for user accounts against phishing and easily guessed passwords [25], was changed from SMS OTP/Magic Link to MNV. The SIM card has a unique Phone number so that it can be used as a parameter for verifying the authenticity of the user [9]. The first process in Figure 3 is the phone number which is entered by the user to do sign-in, or sign-up will be forwarded by the Financial Mobile App Server as a parameter to be asked to the MNV Server. Then the MNV Server will return a URL response containing a unique state to the Financial Mobile App Server and forwarded to the smartphone or tablet to do header enrichment. This first process is termed the Add Phone Number process.

The second process in Figure 3 is the header enrichment which is creating a process for adding data fields to the HTTP/HTTPS header in the mobile network.

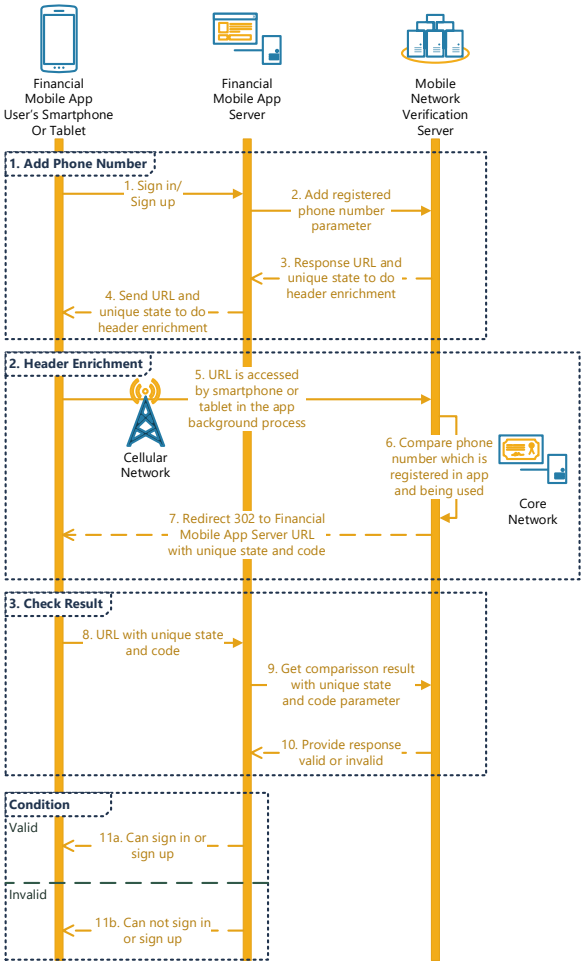

Figure 3. MNV process and API flow design.

DOI: https://doi.org/10.29207/resti.v7i4.5025

It is done to obtain user or device identification such as the Mobile Subscriber Integrated Services Digital Network Number (MSISDN) or the phone number used by the MNV Server [26]. In the background process, the URL containing the unique state will be accessed by the Financial Mobile App on the smartphone or tablet, where the URL leads to the MNV Server. Smartphone or tablet access traffic to these URLs via cellular networks will be inspected by adopting the header enrichment feature in core network to view MSISDN or phone number information [27]. After the Phone Number parameter which is used on the smartphone or tablet to access the URL has been obtained from core network, the MNV Server will perform a comparison with the phone number registered by the application. The MNV Server will direct to a 302 redirect which means a temporary redirect for users to wait the background process by the application on the same page [28] to check the comparative results using a unique state and code.

The third process of MNV in Figure 3 is Check Result. The Financial Mobile App Server will retrieve unique state and code information from the URL sent by the MNV server in the header enrichment process. This unique state and code will be asked again to the MNV Server to find out the status of the phone number verification on the unique transaction whether it is valid or not. The MNV Server will provide a valid or invalid response as a form of 2FA parameter to protect against Account Take Over attacks other than OTP/Magic Link which still can be forwarded to the attacker [29]. If valid, the user will successfully sign-in or sign-up to the next page, otherwise invalid, the user will fail to sign-in or sign-up.

2.3 Assessment Process

The assessment is carried out by conducting tests with the scenarios that can be seen in Table 1. A sample of the Android Financial Application is made to carry out the sign-up and sign-in processes. For the sign-in process, this sample application will use the Firebase feature which makes it easy to authenticate user data such as username/password on the internet cloud and there is an SDK which also makes it easy for the mobile app integration process [30]. Then this sample application will be connected to the MNV server belonging to one of the cellular operators in Indonesia via API. The smartphone which is installed Android Financial App sample will be forced to use cellular network to verify mobile number in cellular infrastructure when header enrichment (step number 2) is run based on Figure 3. Four test cases will be executed, starting from signing up and signing up using the same and different phone number between devices and applications. Each test case is executed ten times. This test case is run to see whether Account Take Over can still occur or not if unknown persons try to sign-in to someone account, but don't have his or her phone number on their device.

Table 1. Testing Scenario

No	Test Case
1	Sign-up using same phone number between device and app
2	Sign-up using different phone number between device and app
3	Sign-in using same phone number between device and app
4	Sign-in using different phone number between device and app

3. Results and Discussions

The results of this study that want to be discussed will be divided into three parts. The first part will discuss about the factors that need to be considered. The second part will discuss prototype of API MNV and integration with Financial Mobile App. The third part will discuss the assessment or evaluation process. Both will be explained in detail in the following subsections.

3.1 Implementation factors that need to be considered

The implementation of authentication and verification technology that utilizes cellular infrastructure in the Financial Mobile App certainly has five factors that support its success. These factors were obtained based on the results of discussions with the product owner from one of the cellular operators that provide the MNV service.

The first factor is that there must be a mobile operator company that provides infrastructure utilization services for additional authentication on mobile applications. This is important because if there are no mobile operators in the country that provide and sell this service, this technology is not applicable.

The second factor is that there must be cooperation between application providers and cellular operators. This relates to the credentials provided by mobile operators for use by application providers in implementing MNV, such as API Key, IP address/domain, price, etc.

The third factor is being adaptable to changes in business processes at application providers. Some application providers are slow in their implementation because they pay too much attention to application size, cost bearer, architectural monolithic, etc.

The fourth factor is the need for policies from government so that all operators in the country provide MNV services. This is important, because in Indonesia alone there are four cellular operators and application users must use one of four different cellular operators.

The fifth factor, apart from MNV, mobile operators and application providers also need to implement SIM Swap detection technology. This is to avoid account takeover

DOI: https://doi.org/10.29207/resti.v7i4.5025

that can occur if cybercriminals exchange SIMs belonging to users who become victims.

3.2 API MNV and Financial Mobile App Prototype

Before integrating the Financial Mobile App, the MNV API test was carried out using the API tester application on a smartphone. The test follows the flow described in Figure 3 where there are three steps, the first is add phone number, the second is header enrichment, and the third is check result. The first scenario of testing this API uses a mobile connection with the same phone number which is attached in the smartphone with the phone number parameter which wants to be checked. This scenario describes the real user who sign-in using the connection with the same phone number which is attached in the smartphone with the phone number which is registered in app.

From the test results, valid credential results are obtained as shown in Figure 4. The second scenario of the API test uses a mobile connection with a different phone number which is attached in the smartphone with the phone number parameter which wants to be checked. This scenario also seems to be someone else or a cybercriminal trying to sign-in using a different phone number between the number which is installed on the smartphone and the number which is registered in the application. The results of this scenario test show invalid credentials as shown in Figure 5. In other words, the people or cybercriminals who use a different installed phone number in their device with app registered phone number, cannot sign-in because of invalid credentials.

In Figure 4, the smartphone uses a cellular data connection with the phone number 081xxxxxx577. This system is equipped with an API key which is always included in the process of adding phone numbers and check results as validation of endpoints that hit the MNV server.

The first process begins by adding the parameter phone number or "MSISDN" 081xxxxxx577 which wants to be checked to MNV URL with the POST JSON method. The response is obtained in the form of an URL with the "state" parameter. This URL is used for the smartphone to access and perform header enrichment using the GET method as the second step. When the smartphone accesses the URL, the MNV server will check whether the connection uses the cellular core network or not. The response is assigned to the callback URL with the "state" and "code" parameters. This parameter will be used to carry out the third step which is the check result process. Because the cellular core network detects the connection and the MNV server record the phone number used by the smartphone the same as the parameters in the first step, 081xxxxxx577, the response obtained is a valid credential result.

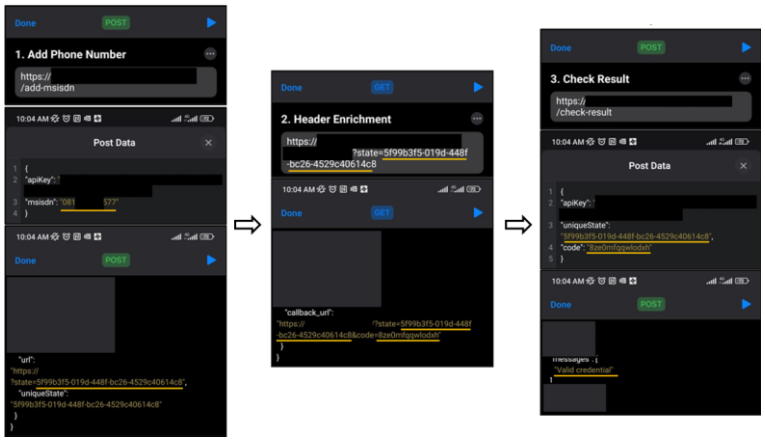

Figure 4. MNV API test with the same phone number.

Likewise in Figure 5, the smartphone still uses a cellular data connection with phone number 081xxxxxx577 as person “A”. However, in the first step, the "MSISDN" parameter being asked is 081xxxxxx999 as person “B”. Here describes the scenario of person “A” trying to take over account of person “B”. Then in the second step, header enrichment occurs where person “A” accesses the URL with the "state" parameter. The cellular core network detects the connection, the MNV server records the phone number used, and stores it in the "state" and "code" parameters. Because person “A” uses a different phone number than the one asked for in the first step, the results of the third step, the check results, show invalid credentials.

After testing the MNV API, a prototype of the Financial Mobile App that has been integrated with MNV was developed. In Figure 6, can be seen that the device uses a mobile connection with phone number 081xxxxxx577 and performs the sign-up process with the same input parameter phone number 081xxxxxx577. In the sign-up process, there are two checking processes, namely checking the similarity of the mobile number and checking whether there is already a user using the email. If the registered mobile number is the same as the

DOI: https://doi.org/10.29207/resti.v7i4.5025

mobile number installed on the smartphone and if no email has been registered, then the sign-up process will be successful. The result obtained is that the user who does the sign-up process using the same phone number between the device and the app was successful. In other words, only users who use the actual phone number on the device can do the registration process.

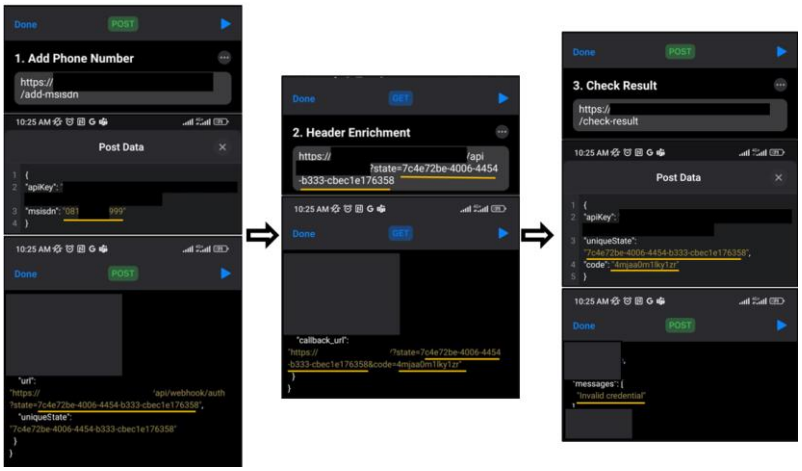

Figure 5. MNV API test with the different phone number.

After the sign-up process in Figure 6 using email testname@gmail.com and phone number 081xxxxxx577 has been successfully created on Firebase, sign-in process using that user are tested in Figure 7. It shows the sign-in process using a mobile connection with the same phone number between attached on the device and registered on that user account, namely 081xxxxxx577. The result obtained is that the sign-in process was successfully carried out, meaning that only users who use the actual phone number connection on their device can sign-in to the application.

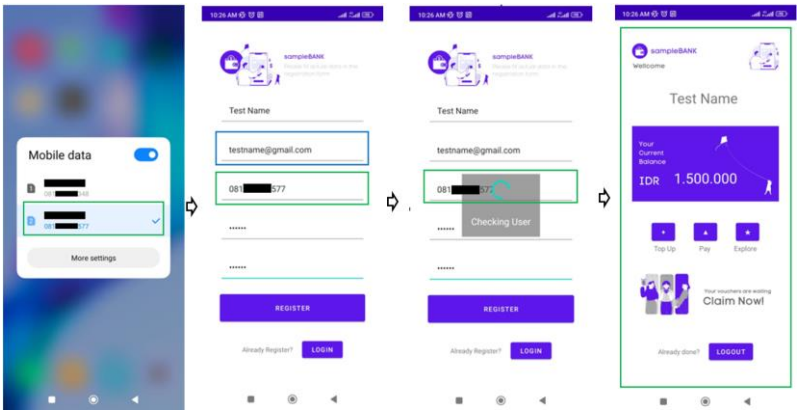

Figure 6. Financial mobile app prototype with sign up process using same phone number between device and app.

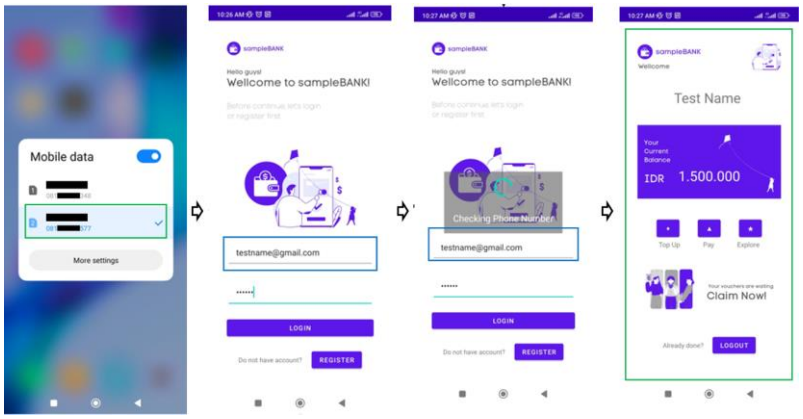

Figure 7. Financial mobile app prototype with sign in process using same phone number between device and app.

DOI: https://doi.org/10.29207/resti.v7i4.5025

Unlike the case with Figure 8, a sign-in experiment using the user account testname@gmail.com and a mobile connection with a different phone number was carried out. The user account is registered using the phone number parameter 081xxxxxx577, while the mobile connection on the device uses the phone number 081xxxxxx348. The result obtained is that the sign-in process using a different phone number between devices and apps was fails, this scenario is also as expected. In other words, if the cybercriminal manages to get the victim's account user to sign-in, they still cannot sign-in, because the cybercriminal does not have a phone number installed on the device.

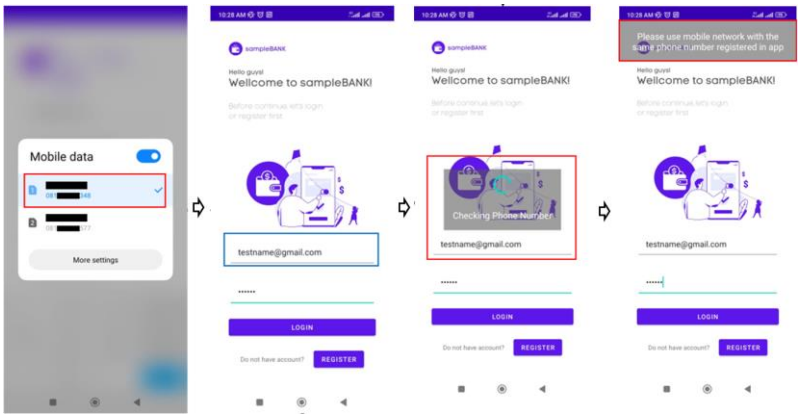

Figure 8. Financial mobile app prototype with sign in process using different phone number between device and app

Like Figure 9, the sign-up process is carried out using a different phone number parameter between the one used as the mobile connection on the device and the one entered in the form. The result obtained is that the sign-up process using a different phone number parameter fails and this scenario is in line with expectations. In other words, the application needs to ensure that the user who registers an account in the application is a real user using the same phone number which is used in mobile device connection. So that the validation when doing sign-in is straight between the user account tied to the phone number parameter to be checked at MNV.

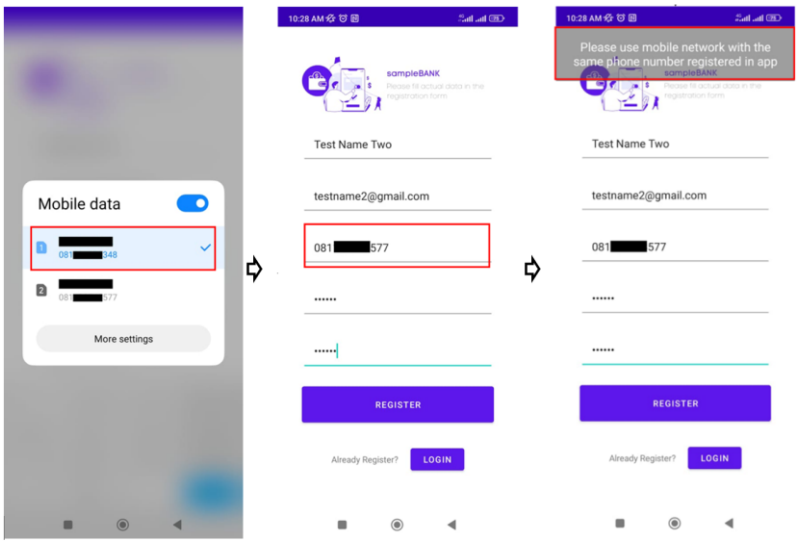

Figure 9. Financial mobile app prototype with sign up process using different phone number between device and app.

3.3 Assessment and evaluation result

Table 2 is a summary of the four test cases that were carried out. Each test case was carried out ten times, where the first and second test cases carried out the sign-up process, then the third and fourth test cases carried out the sign-in process. The first test case performs sign-up using the same phone number between the device and the application, while the second test case uses a different phone number. From the first test case with 10 trials, the expected result was that sign-up could be carried out, and the results were successful as expected. Then for the second test case, 10 trials were also carried out, the expected result was that registration could not be carried out and the results were successful as expected.

Sign-in attempts that are often carried out by cybercriminals need to be secured, for that the third and fourth test cases are carried out. The third test case was

DOI: https://doi.org/10.29207/resti.v7i4.5025

carried out 10 times to sign-in using the same phone number between device and app, while the fourth test case was also tried 10 times using a different phone number. The third test case has successful results according to expectations where sign-in is successful when using the same phone number between the device and the app. Then the fourth test case also has successful results according to expectations where signing in fails when the phone number is different between the device and the app.

Table 2. Testing Result

No	Test Case	Expected Result	Number of Tries	Result
1	Sign-up using same phone number between device and app	Can sign-up	10 times	Success
2	Sign-up using different phone number between device and app	Cannot sign-up	10 times	Success
3	Sign-in using same phone number between device and app	Can sign-in	10 times	Success
4	Sign-in using different phone number between device and app	Cannot sign-in	10 times	Success

In more detail, the first test case can be seen in Figure 10, the second test case in Figure 11, the third test case in Figure 12, and the fourth test case in Figure 13. The first test case in Figure 10 can be seen that the selected connectivity uses phone number 081xxxxxx577. Then the sign-up process is carried out ten times in succession using an email with the name from testcase1trial1@gmail.com until testcase1trial10@gmail.com by entering the phone number 081xxxxxx577 to register. This means that the phone number used in this first test case for device connection and the phone number used for registration are the same. From the MNV transaction log, it can be seen that the ten trials produced a valid credential response. Then from the Firebase console you can also see that the sign-up process of the ten email users has been successfully created. The ten trials in this first test case had successful results that matched expectations where successful sign-up using the same phone number between the device and the app.

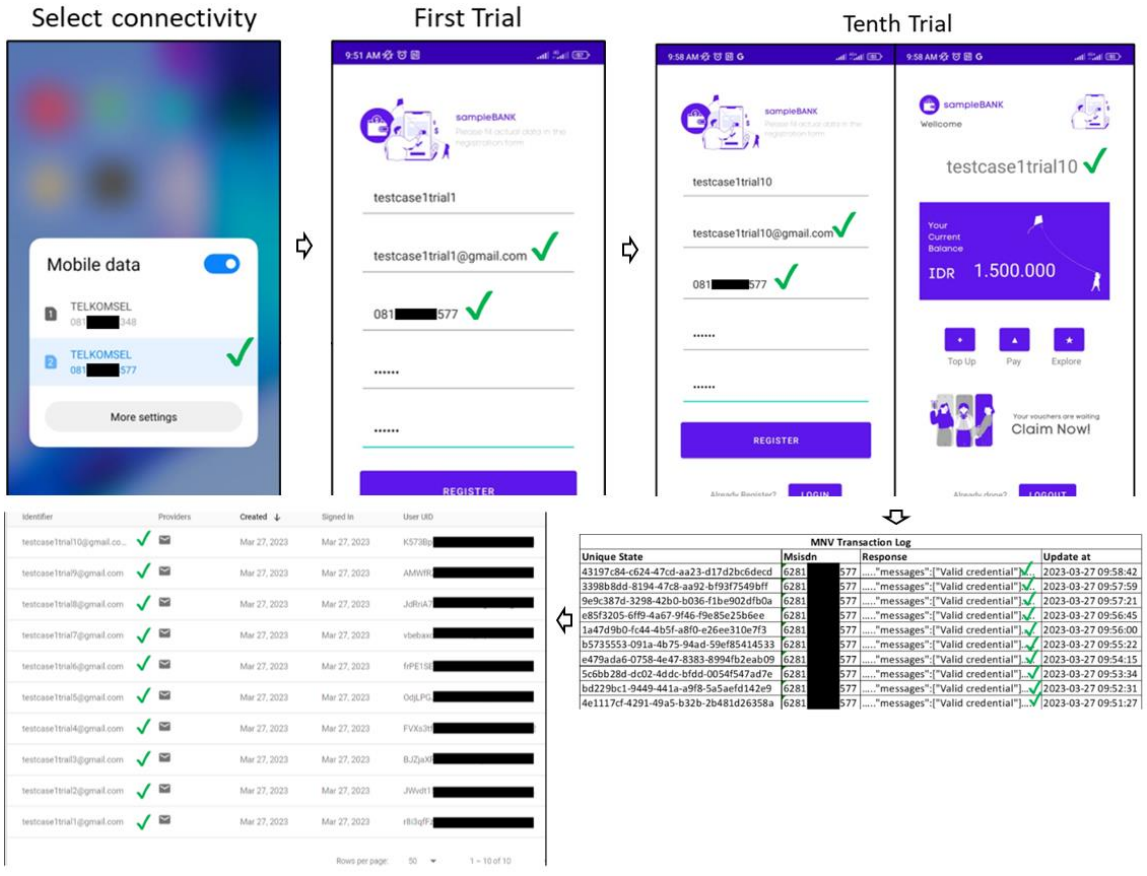

Figure 10. Result of test case 1

The second test case in Figure 11 can be seen that the selected connectivity uses the phone number 081xxxxxx577 and then tries to register using a different phone number, namely 081xxxxxx348. The sign-up process for the second test case is carried out ten times in succession using an email with the name

DOI: https://doi.org/10.29207/resti.v7i4.5025

from testcase2trial1@gmail.com until testcase2trial10@gmail.com by entering the phone number 081xxxxxx348 to register. From the MNV transaction log can be seen that the ten attempts result are invalid credential responses. Then from the Firebase console it can also be seen that the sign-up process for the ten email users failed to be created. The ten trials in this second test case had successful results that matched expectations where they failed to sign-up using a different phone number between the device and app.

Then for the third and fourth test cases, before conducting an experiment to sign-in, two users were registered in the Firebase by email testcase3@gmail.com with phone number 081xxxxxx577 and testcase4@gmail.com with phone number 081xxxxxx348. This user was created to separate users from the first test case that was successfully created on Firebase using the email testcase1trial1@gmail.com to testcase1trial10@gmail.com.

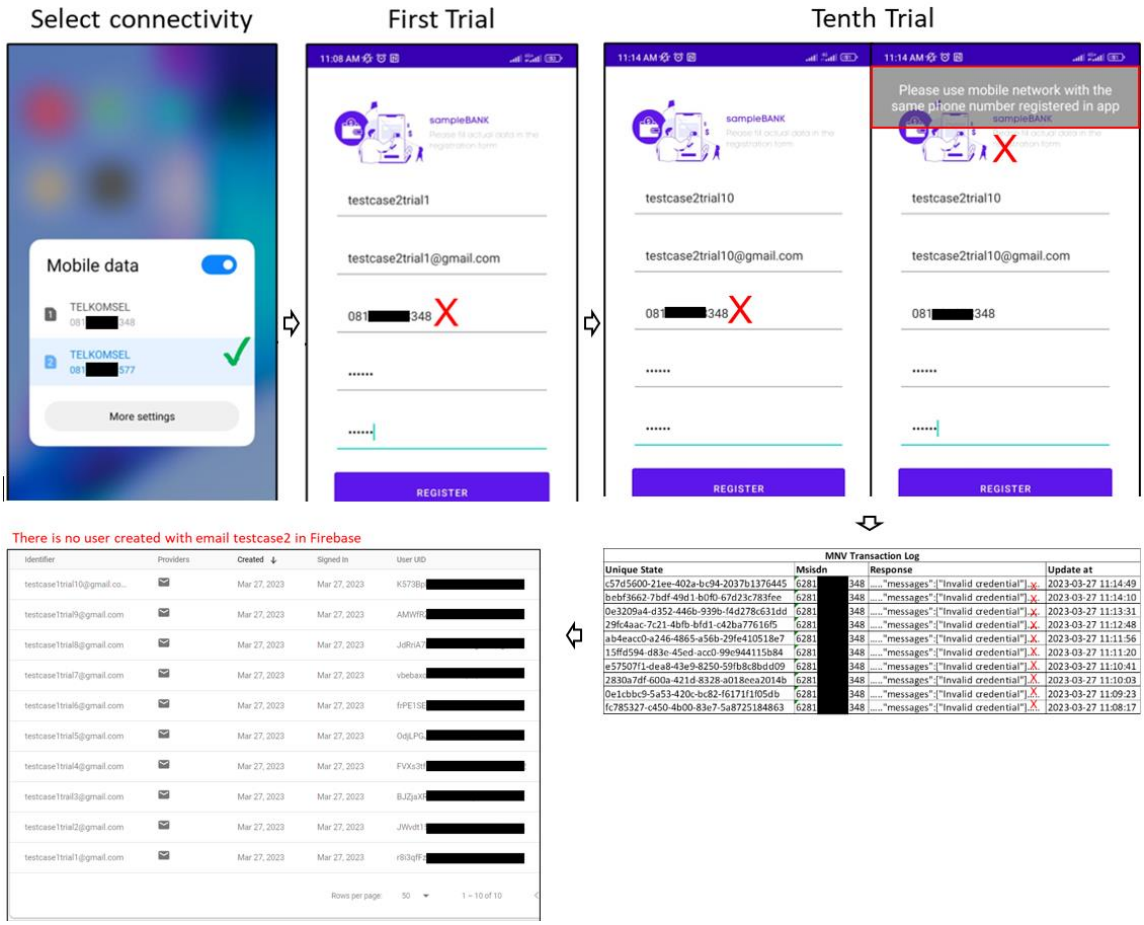

Figure 11. Result of test case 2

The third test case can be seen in Figure 12, where the sign-in process using the same phone number between device and app is carried out. Users registered with the email testcase3@gmail.com with phone number 081xxxxxx577 on Firebase will be tried to sign-in on the device with the same connection selection as phone number 081xxxxxx577 as well. The experiment was carried out 10 times and it can be seen in the MNV transaction log that the ten sign-in processes have valid credential responses. In other words, this third test case has been successful as expected, where sign-in will succeed if using the same phone number between device and app.

The fourth test case can be seen in Figure 13, where the sign-in process using a different phone number between device and app is also done ten times. This experiment was carried out using a registered user using the email testcase4@gmail.com with the phone number 081xxxxxx348 on Firebase. The selected connection on the device uses the phone number 081xxxxxx577 which means it is different from the phone number registered on Firebase. The results obtained are successful as expected, where sign-in fails when the phone number is different between the device and the app. This can be seen in the MNV transaction log which shows ten invalid credential responses. From the results of the overall testing of the four scenarios, it can be seen what the differences in each test case are, what are the benefits that can be adopted based on these test scenarios and can be summarized as in Table 3.

DOI: https://doi.org/10.29207/resti.v7i4.5025

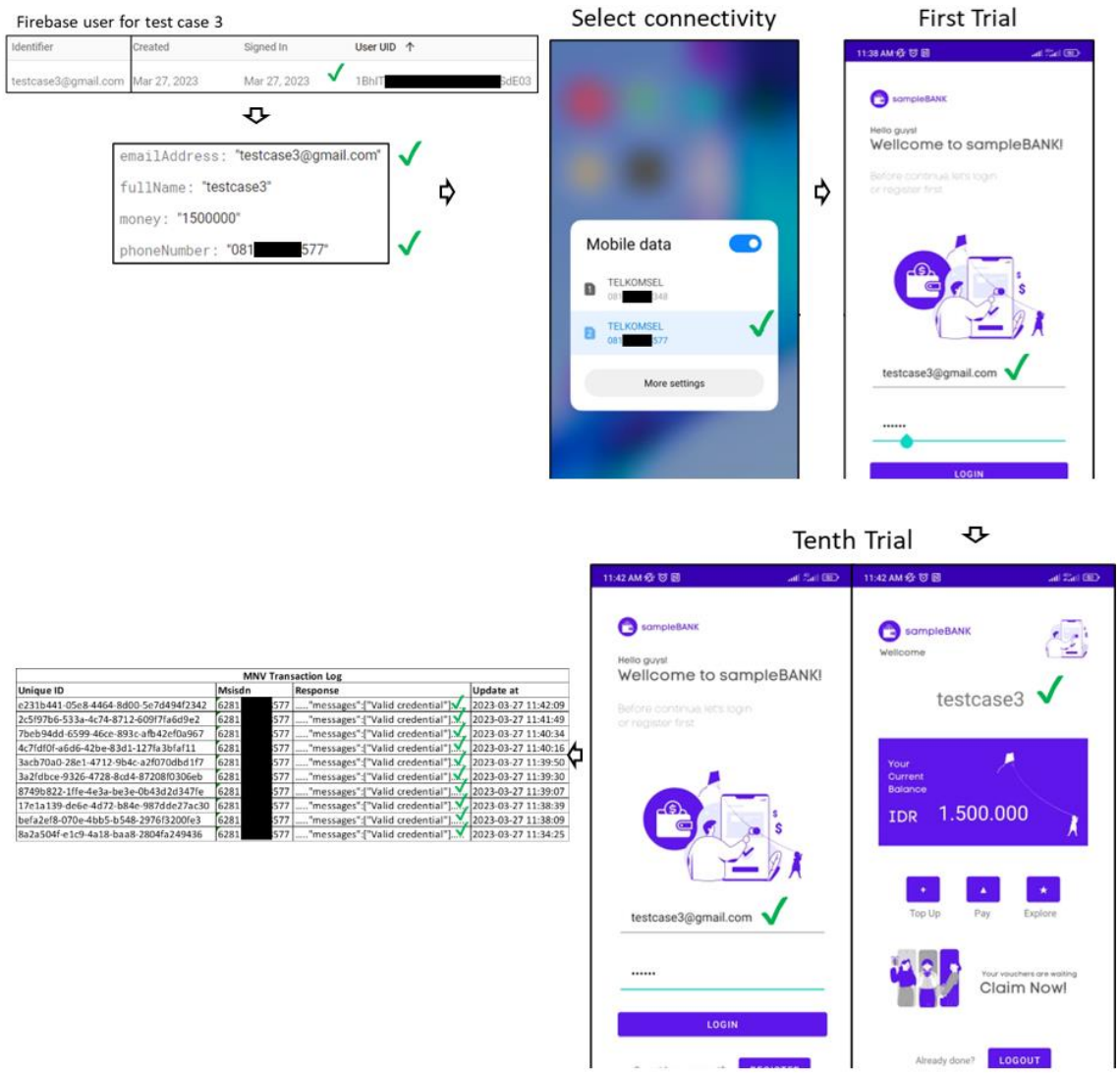

Figure 12. Result of test case 3

Table 3. Differences and advantages of testing scenarios

Test Case	Differences	Advantages
Test Case 1	This test case illustrates the process of **registering** an account by a **real user**.	Financial institutions can ensure the legitimacy and authenticity of users who register with the application because they use their phone number.
Test Case 3	This test case describes the process of **logging** into a financial mobile app by a **real user**.	Users will be secured because only real users who have the same phone number registered in the application as installed on their smartphone.
Test Case 2	This test case illustrates the process of **registering** a financial mobile app account by **cybercriminals** using the victim's identity, of course the victim's phone number is not installed on the cyber criminal's smartphone.	Cybercriminals will not be able to register an account on behalf of the victim because they do not have the victim's phone number installed on their smartphone, so the user will be secured.
Test Case 4	This test case illustrates the process of **logging** into the financial mobile app by **cybercriminals** using the victim's credentials, of course the victim's phone number is not installed on the cybercriminal's smartphone.	Cybercriminals will not be able to log into the application and will not be able to steal money from the victim's account even if they have the username and password because they do not have the victim's phone number installed on their smartphone, so users will be secured.

DOI: https://doi.org/10.29207/resti.v7i4.5025

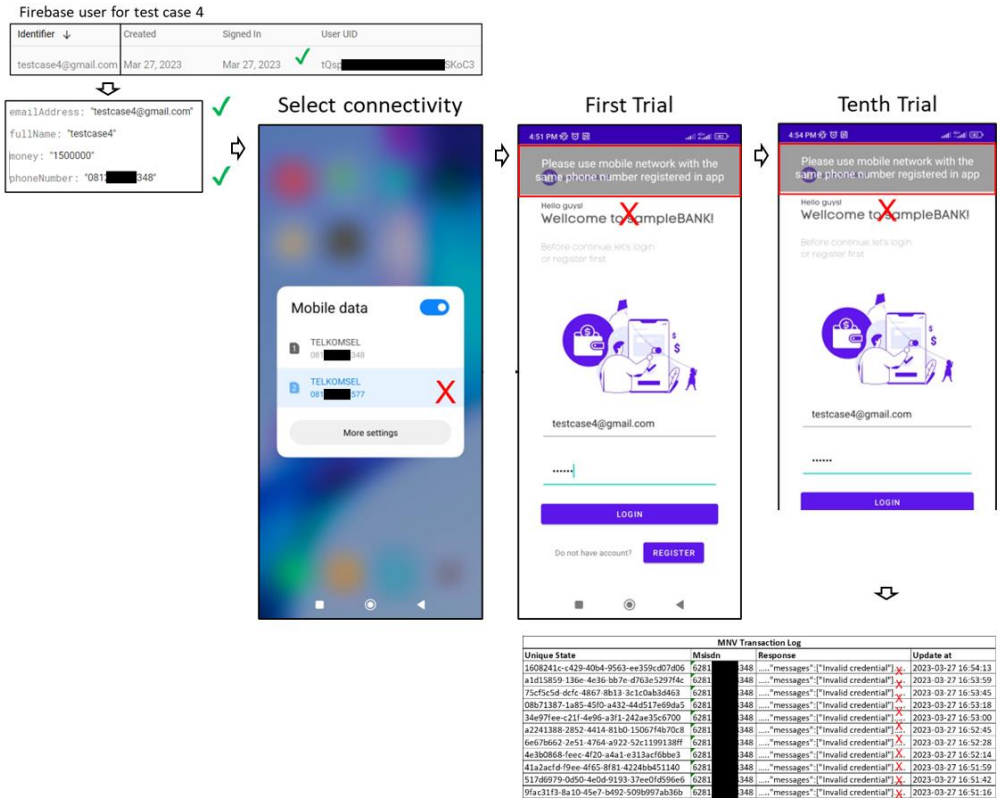

Figure 13. Result of test case 4

4. Conclusions

The problems and cases of ATO attacks on the Financial Mobile App that lead to theft of customer money in Indonesia have been described in this study. The existing OTP SMS or SMS Magic Link has been used, but from the cases described it has become a vulnerability to be forwarded to cyber criminals who have succeeded in taking credential sign-in through social engineering, phishing, and fake APK. As previously explained, this study aims to provide solutions to Financial Mobile Application providers to protect their customers from ATO attacks. So, in this study it can be shown that there is also a part of the cellular network infrastructure can be utilized to prevent the ATO attacks, namely by carrying out Mobile Network Verification, which looks at the similarities between the phone numbers used on the device and those registered in the application whether they are the same or not. Thus, cybercriminals who have the victim's user credential sign-in will not be able to sign-in to take over the victim's Financial Mobile App account, because the cybercriminal's device does not have the victim's phone number attached. For testing scenarios that describe the sign-up and sign-in processes carried out by actual users in test case 1 for 10 trials and test case 3 for 10 trials also obtained 100% successful results according to expected results, where the real user is successful to sign-in and sign-up. Likewise, testing scenarios that describe the sign-up and sign-in processes carried out by cybercriminals who has victim's credentials but certainly do not have the victim's phone number installed on their smartphone in test case 2 for 10 attempts and test case 4 for 10 trials, the result is 100% success, according to the expected results too, where cyber criminals fail to take over the victim's account. The conclusion is that MNV has succeeded in protecting users from account take over attacks, where only those who have the same phone number installed on the device and who are registered in the application can sign-in or sign-up. It is hoped that this kind of protection model can reduce losses experienced by Financial Mobile Application users due to Account Take Over.

Our next work and research for multifactor authentication by utilizing this mobile network infrastructure is to add another parameter which can be obtained from it. Other additional parameters besides the phone number that can be utilized are IMEI (International Mobile Equipment Identity), IMSI (International mobile Subscriber Identity), and detection of SIM Card replacement to deal with SIM Swap attacks. This parameter collaboration will strengthen the protection of financial mobile app users against account take over attacks. Follow-up research can also be made into a case study that is implemented in an actual financial company, how this technology is adopted, how big the business potential is from the

DOI: https://doi.org/10.29207/resti.v7i4.5025

operator's side, how well risks can be reduced from the financial institution's side, and how satisfied users are with this kind of information security technology.

References

[1] Asosiasi Penyelenggara Jasa Internet Indonesia, "Profil Internet Indonesia 2022," *Apji.or.Od*, no. June, p. 10, 2022, [Online]. Available: apji.or.id.

[2] CyberEdge Group, "2022 Cyberthreat Defense Report," *CyberEdge Gr.*, p. 66, 2022.

[3] Medcom.id, "Penipuan Modifikasi APK Jaring 493 Korban dengan Kerugian Rp12 Miliar," *Medcom.id*, 2023. https://www.medcom.id/nasional/hukum/Rkje4Q6b-penipuan-modifikasi-apk-jaring-493-korban-dengan-kerugian-rp12-miliar.

[4] K. Chetioui, B. Bah, A. O. Alami, and A. Bahnasse, "Overview of Social Engineering Attacks on Social Networks," *Procedia Comput. Sci.*, vol. 198, no. 2021, pp. 656–661, 2021, doi: 10.1016/j.procs.2021.12.302.

[5] M. P. Bach, T. Kamenjarska, and B. Žmuk, "Targets of phishing attacks: The bigger fish to fry," *Procedia Comput. Sci.*, vol. 204, pp. 448–455, 2022, doi: 10.1016/j.procs.2022.08.055.

[6] M. A. Husainiamer, M. Mohd Saudi, and M. Yusof, "Securing Mobile Applications Against Mobile Malware Attacks: A Case Study," *19th IEEE Student Conf. Res. Dev. Sustain. Eng. Technol. Towar. Ind. Revolution, SCOReD 2021*, pp. 433–438, 2021, doi: 10.1109/SCOReD53546.2021.9652685.

[7] P. Doerfler *et al.*, "Evaluating login challenges as a defense against account takeover," *Web Conf. 2019 - Proc. World Wide Web Conf. WWW 2019*, pp. 372–382, 2019, doi: 10.1145/3308558.3313481.

[8] J. Bento, P. Saleiro, A. F. Cruz, M. A. T. Figueiredo, and P. Bizarro, "TimeSHAP: Explaining Recurrent Models through Sequence Perturbations," *Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, pp. 2565–2573, 2021, doi: 10.1145/3447548.3467166.

[9] G. Ali, M. A. Dida, and A. E. Sam, "Two-factor authentication scheme for mobile money: A review of threat models and countermeasures," *Futur. Internet*, vol. 12, no. 10, pp. 1–27, 2020, doi: 10.3390/fi12100160.

[10] A. P. Binitie, "Design of a Resilient System against Shoulder Surfing Attack : Adaptable to USSD Channel," pp. 1–19, 2023.

[11] A. Patience, N. Christiana, and P. Oguguo, "Security against Shoulder Surfing Attack Adaptable to Feature Phones using USSD Technology," *Int. J. Innov. Sci. Res. Technol.*, vol. 7, no. 12, pp. 560–568, 2022, [Online]. Available: www.ijisrt.com560.

[12] M. Wazid, S. Zeadally, and A. K. Das, "Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 56–60, 2019, doi: 10.1109/MCE.2018.2881291.

[13] J. M. Chigada, "A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions," *SA J. Inf. Manag.*, vol. 22, no. 1, pp. 1–9, 2020, doi: 10.4102/sajim.v22i1.1194.

[14] B. Chaimaa, E. Najib, and H. Rachid, "E-banking Overview: Concepts, Challenges and Solutions," *Wirel. Pers. Commun.*, vol. 117, no. 2, pp. 1059–1078, 2021, doi: 10.1007/s11277-020-07911-0.

[15] Z. P. Zwane, T. E. Mathonsi, and S. P. Maswikaneng, "An intelligent security model for online banking authentication," *2021 IST-Africa Conf. IST-Africa 2021*, pp. 1–6, 2021.

[16] R. Laborde *et al.*, "A User-Centric Identity Management Framework based on the W3C Verifiable Credentials and the FIDO Universal Authentication Framework," *2020 IEEE 17th Annu. Consum. Commun. Netw. Conf. CCNC 2020*, 2020, doi: 10.1109/CCNC46108.2020.9045440.

[17] W. A. Hammood, R. Abdullah, O. A. Hammood, S. Mohamad Asmara, M. A. Al-Sharafi, and A. Muttaleb Hasan, "A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 769, no. 1, 2020, doi: 10.1088/1757-899X/769/1/012061.

[18] K. K. Kamal, S. Gupta, P. Joshi, and M. Kapoor, "An efficient mCK signing and mobile based identity solution for authentication," *Int. J. Inf. Technol.*, vol. 15, no. 3, pp. 1637–1646, 2023, doi: 10.1007/s41870-023-01189-8.

[19] 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," *Proc. - 2021 Int. Conf. Softw. Eng. Comput. Syst. 4th Int. Conf. Comput. Sci. Inf. Manag. ICSECS-ICOCSIM 2021*, vol. 0, pp. 411–416, 2021, doi: 10.1109/ICSECS52883.2021.00081.

[20] Y. Y. Tefera, T. Kibatu, B. S. Shawel, and D. H. Woldegebreal, "Recurrent Neural Network-based Base Transceiver Station Power Supply System Failure Prediction," *Proc. Int. Jt. Conf. Neural Networks*, 2020, doi: 10.1109/IJCNN48605.2020.9206978.

[21] A. A. R. Alsaeedy and E. K. P. Chong, "A review of mobility management entity in LTE networks: Power consumption and signaling overhead," *Int. J. Netw. Manag.*, vol. 30, no. 1, p. e2088, 2020, doi: https://doi.org/10.1002/nem.2088.

[22] D. Basu, A. Jain, R. Datta, and U. Ghosh, "Optimized Controller Placement for Soft Handover in Virtualized 5G Network," *2020 IEEE Wirel. Commun. Netw. Conf. Work. WCNCW 2020 - Proc.*, 2020, doi: 10.1109/WCNCW48565.2020.9124902.

[23] W. D. S. Coelho, A. Benhamiche, N. Perrot, and S. Secci, "Network Function Mapping: From 3G Entities to 5G Service-Based Functions Decomposition," *IEEE Commun. Stand. Mag.*, vol. 4, no. 3, pp. 46–52, 2020, doi: 10.1109/MCOMSTD.001.1900040.

[24] W. Liang, L. Cui, and F. P. Tso, "Low-latency service function chain migration in edge-core networks based on open Jackson networks," *J. Syst. Archit.*, vol. 124, p. 102405, 2022, doi: https://doi.org/10.1016/j.sysarc.2022.102405.

[25] M. Golla, G. Ho, M. Lohmus, M. Pulluri, and E. M. Redmiles, "Driving 2FA adoption at scale: Optimizing two-factor authentication notification design patterns," *Proc. 30th USENIX Secur. Symp.*, pp. 109–126, 2021.

[26] M. Pattaranantakul, C. Vorakulpipat, and T. Takahashi, "Service Function Chaining security survey: Addressing security challenges and threats," *Comput. Networks*, vol. 221, p. 109484, 2023, doi: https://doi.org/10.1016/j.comnet.2022.109484.

[27] Y. Xu, C. Dai, and A. Li, "Admission Control for Quality of Services of Mobile Cellular Network," *MobiArch 2020 - Proc. 2020 ACM MobiArch 2020 15th Work. Mobil. Evol. Internet Archit. Part Mobicom 2020*, pp. 54–59, 2020, doi: 10.1145/3411043.3412508.

[28] J. A. Overton, M. Cuffaro, and C. J. Mungall, "String of PURLs – frugal migration and maintenance of persistent identifiers," *Data Sci.*, vol. 3, no. 1, pp. 3–13, 2019, doi: 10.3233/ds-190022.

[29] K. Reese, T. Smith, J. Dutson, J. Armknecht, J. Cameron, and K. Seamons, "A usability study of five two-factor authentication methods," *Proc. 15th Symp. Usable Priv. Secur. SOUPS 2019*, pp. 357–370, 2019.

[30] M. D. Pop and A. R. Stoia, "Improving the Tourists Experiences: Application of Firebase and Flutter Technologies in Mobile Applications Development Process," *Proc. - 2021 Int. Conf. Eng. Technol. Comput. Sci. EnT 2021*, pp. 146–151, 2021, doi: 10.1109/EnT52731.2021.00033.

DOI: https://doi.org/10.29207/resti.v7i4.5025