International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 41 No. 3 Jan. 2024, pp. 785-794
© 2024 Innovative Space of Scientific Research Journals
http://www.ijias.issr-journals.org/

Multi-factor authentication system for securing mobile money transactions using mobile money services in Ivory Coast

Nogbou Georges Anoh[1], Tiémoman Kone[1], Gokou Hervé Fabrice Diedie[2], and Michel Babri[3]

[1]UFR Informatique et science du numérique, Université Virtuelle de Côte d'Ivoire, Abidjan, Côte d'Ivoire

[2]Université Peleforo Gon Coulibaly, BP 1328, Korhogo, Côte d'Ivoire

[3]Laboratoire de recherche en informatique, Institut National Polytechnique Felix Houphouet Boigny, Yamoussoukro, Côte d'Ivoire

ABSTRACT: Mobile money is a financial service available on mobile phones. The evolution of mobile telephony in Africa, and particularly in Côte d'Ivoire, has led to the growing evolution of mobile money services. These services have revolutionized the lives of citizens who do not have access to or do not have a bank account. Thanks to the mobile money service, any citizen can now transfer, withdraw or save money and even make payments. However, with the digitalization of systems, users of these mobile money services suffer from cyberattacks thanks to the scale of social engineering. To slow down and fight against this evolution of cyberattacks. In this article, we propose a new multi-factor authentication system in the context of mobile money transactions unlike the two-factor authentication system. We have developed an authentication algorithm for transfers using a password, fingerprint or secret word and a secret code. For direct deposit, we have proposed a system that provides a withdrawal code to the issuer that the recipient must provide upon withdrawal. We also proposed an authentication algorithm for password changes based on the current password and a secret code to provide. These contributions will help curb deposits made by mistake, scams and theft of mobile phones with password theft.

KEYWORDS: mobile money service, authentication, transfer, deposit, password, fingerprint, secret word, secret code.

1 INTRODUCTION

The evolution of communication technologies and the adoption of mobile phones in Africa and particularly in Côte d'Ivoire, has favored the creation of mobile money services by banking and telecommunications operators. According to statistics provided by the Telecommunications Regulatory Authority in Côte d'Ivoire (ARTCI) for the first quarter of 2023 [1], the number of subscribers linked to mobile telephony is 50,130,099 including 23,203,174 mobile money subscribers with a national population estimated at 29,389,150 inhabitants, according to the final overall results of the General Population and Housing Census (RGPH 2021) [2]. However, the mobile internet market totals 26,789,366 mobile internet subscribers, which shows that the number of subscribers who have access to mobile applications for mobile money services is considerable and even significant. This proliferation of the mobile Internet has no consequences for Internet users of mobile financial services, although it has improved the level of populations without access to the banking financial system. Indeed, in a statement on December 21, 2021, the Director of IT and Technological Traces (DITT) in Côte d'Ivoire indicated that on average 4,500 to 5,000 complaints are recorded per year compared to 150 in 2011 [3]. Today, Ivory Coast is one of the countries most affected by cybercrime in West Africa. Cybercrimes are largely carried out by attacks linked to social engineering, namely the theft of personal information, phishing, Shoulder Surfing, Pretexting. To fight against cybercriminals with the numerous attacks, authentication solutions have been proposed in the literature. In Ivory Coast, in the context of online purchases, the authentication system used is the two (2) factor authentication system which is experiencing an increase in attacks. Two (2) factor authentication system threat models are classified into five categories [4] namely: (i) attacks against authentication, such as spoofing attacks, replay attacks, spoofing attacks, phishing attacks and Trojan horse attacks; social engineering attacks, identity theft attacks, (ii) attacks on privacy; (iii) privacy attacks, such as eavesdropping attacks, brute force attacks, guessing attacks, and shoulder surfing attacks; (iv) attacks on integrity; (v) availability attacks, such as DoS and DDoS attacks, and cell phone theft.

In addition, to secure mobile money services, two categories of security system are proposed namely cryptographic functions (such as asymmetric encryption function, symmetric encryption function and hash function) and personal identification that we can subdivide into two categories: (i) authentication systems based on password, PIN code, OTP code, and QR code; (ii) countermeasures based on physiological biometrics through fingerprint recognition, face recognition, iris recognition and retina recognition, and behavioral biometrics through voice recognition. Authors in [5], through a statistical study showed that the use of better access controls such as multi-factor authentication (i.e. PIN, one-time password and biometric fingerprint), customer awareness campaigns and training of mobile money service agents are recommended by mobile money service users. Authors in [6] propose a multi-factor authentication algorithm for mobile money applications. The proposed authentication system uses a novel approach combining PIN, one-time password (OTP) and biometric fingerprint to enhance security during mobile money authentication. It also uses a biometric fingerprint and quick response (QR) code to confirm mobile money withdrawal. Given that in our developing countries, the large part of the population that has adopted mobile money services is predominantly illiterate, then with this approach a portion of mobile money users who do not have a mobile phone will not be able to access the mobile money service, which is not advantageous for mobile money service operators. In [7], the authors studied the different factors of authentication systems making it possible to authenticate a user and prove their identity to a service. The main goal of this work is to allow a network administrator to get an idea of all the different multi-factor authentication systems that can be leveraged to create an adequate user authentication strategy for their department. In this work [8], the authors proposed a new authentication method for online banking services. The proposed method does not take into account a user name or password. However, it uses a PIN code instead of the password. Before connecting, the information (MAC Address, SIM card number, International Mobile Identifier) concerning the mobile phone must be verified to authorize the transaction. With this method, if an attacker knows the PIN code and has the user’s phone in their possession, they can conduct transactions as if they were the legitimate user. In [9], the authors propose a money transfer system between two employees of an SME. For this to be possible, users of the SME money transfer system must be registered using a number of parameters including a photo of the iris if this information is correct. The authentication factors that are taken into account to be able to transfer money to another user are the PIN of the sender, The recipient account and the iris of the sender. In this work [10], the authors implemented a two-factor authentication system: (i) PIN code verification. (ii) Generation of OTP on registered mobile number, in connection with transfer of funds from one bank account to another through ATM and ATM card. The problem this approach raises is what to do if an attacker knows the PIN and has the user’s phone? In this study [11], the authors proposed a security model that allows tracking of mobile money account creation using the Transport Layer security (TLS) protocol to protect transactions between banks and mobile network operators and financial regulators. In this work [12], the authors present a fingerprint-based authentication system for transactions related to online banking service. The proposed system includes an enrollment phase which consists of recording the encrypted identifier of the mobile as well as the user’s fingerprint at the server level. Then, a client verification phase is executed to enable a secure transaction. The question that arises is what happens if the user does not have an Android phone or loses their phone? For online banking services, the authors of [13] offer an authentication system based on PIN code, facial recognition and an OTP code to guarantee the security of transactions carried out by customers against phone theft and identity theft. A quantitative study was carried out based on an online questionnaire [14] in order to assess the acceptance of the use of fingerprint in the authentication system of Bahrain online banking services by users of these services and to identify them. In this work [15], the authors proposed a hybrid authentication model (HAM), using a combination of PIN and fingerprints for authentication for the use of mobile banking applications. In the implementation of the system, the customer, to carry out a transaction must provide his PIN and fingerprint in order to be able to carry out a transaction if necessary. In this work, five factors were defined in order to minimize the risks of identity theft: (i) access rights, (ii) securing the enrollment phase, (iii) encryption of transmitted data, (iv) certification of the cloud provider if applicable, (v) Effective control from registration to the storage or retrieval process. According to [16], biometric systems for online banking have several advantages because they provide increased security and reliability, they are simple and convenient, they save time, and they make identity fraud impossible. According to [17], new modes and types of fraud can be grouped according to users of mobile money services. The main frauds perpetrated against customers of mobile money services include: (i) identity theft, (ii) false promotions, (iii) agents who ask the customer for their personal identification number (PIN), (iv) theft of the identity of the service provider by fraudsters, (v) losses attributable to transfers made in error to the benefit of involuntary beneficiaries who refuse to remit the money received. In Ivory Coast, to transfer money via a mobile money application, you must first deposit money into your Mobile Money account through approved providers, then follow the following steps [18]: (i) Dial the operator’s USSD code, (ii) Choose the code for the operation to be carried out, (iii) Enter the recipient’s telephone number, (iv) Enter the amount you wish to transfer, (v) Choose the type of transfer, (vi) Enter your Mobile Money transaction PIN, (vii) Confirm the transfer, (viii)

Sender receives confirmation SMS. This transfer system does not protect the user against transfers made in error, against identity theft and mobile phone theft.

In Ivory Coast, mobile money transfer applications use a two-factor authentication system (PIN code and OTP). However, in the face of social engineering and the numerous attacks mentioned in the literature, a multi-factor authentication system must be proposed and implemented. Several authentication systems have been proposed in the literature (table 1), however, they are not adapted to the context of Côte d'Ivoire where the vast majority of users of mobile money services are illiterate. In addition to this, the fingerprint used in the authentication systems proposed in the literature is one of the best solutions, however, the fingerprint of a user may experience a modification linked to a bodily problem and therefore no longer be available. Under these conditions, it is more than necessary to propose a new authentication system for mobile money services in Ivory Coast.

Table 1. Comparison of systems from the literature

Authors	Year	Authentication factors
G. Ali et al.	2021	PIN code, one-time password (OTP), biometric fingerprint, quick response code (QR)
WA Hammood et al.	2021	PIN code, MAC address, SIM card number, International Mobile Identifier,
K. Sudharsan et al.	2019	PIN code, iris recognition
S. Rwiz et al.	2020	PIN code, one-time password (OTP)
S.Ali et al.	2022	Cryptographic protocol
MJ Zadeh et al.	2019	Fingerprint and cryptographic protocol
Z.Mirza et al.	2020	PIN code, facial recognition and an OTP code

2 PROPOSAL FOR A MULTI-FACTOR AUTHENTICATION SYSTEM

The Mobile Money service is a system that provides a mobile wallet that allows people who do not have a bank account to save, send, receive money and pay for expenses from a mobile phone. Mobile money services have many advantages because they allow populations who do not have access to bank accounts to have access to financial services, thus revolutionizing the daily lives of populations in developing countries.

2.1 SYSTEM FOR IDENTIFYING A MOBILE MONEY CUSTOMER

Identification involves recording personal information relating to a customer of a mobile telephone operator. In the identification system proposed in addition to information linked to the identity of customers (First and last name, photo), we have added a PIN code and a secret word of six (6) characters each, then the recording of the fingerprint as illustrated in Figure 1.

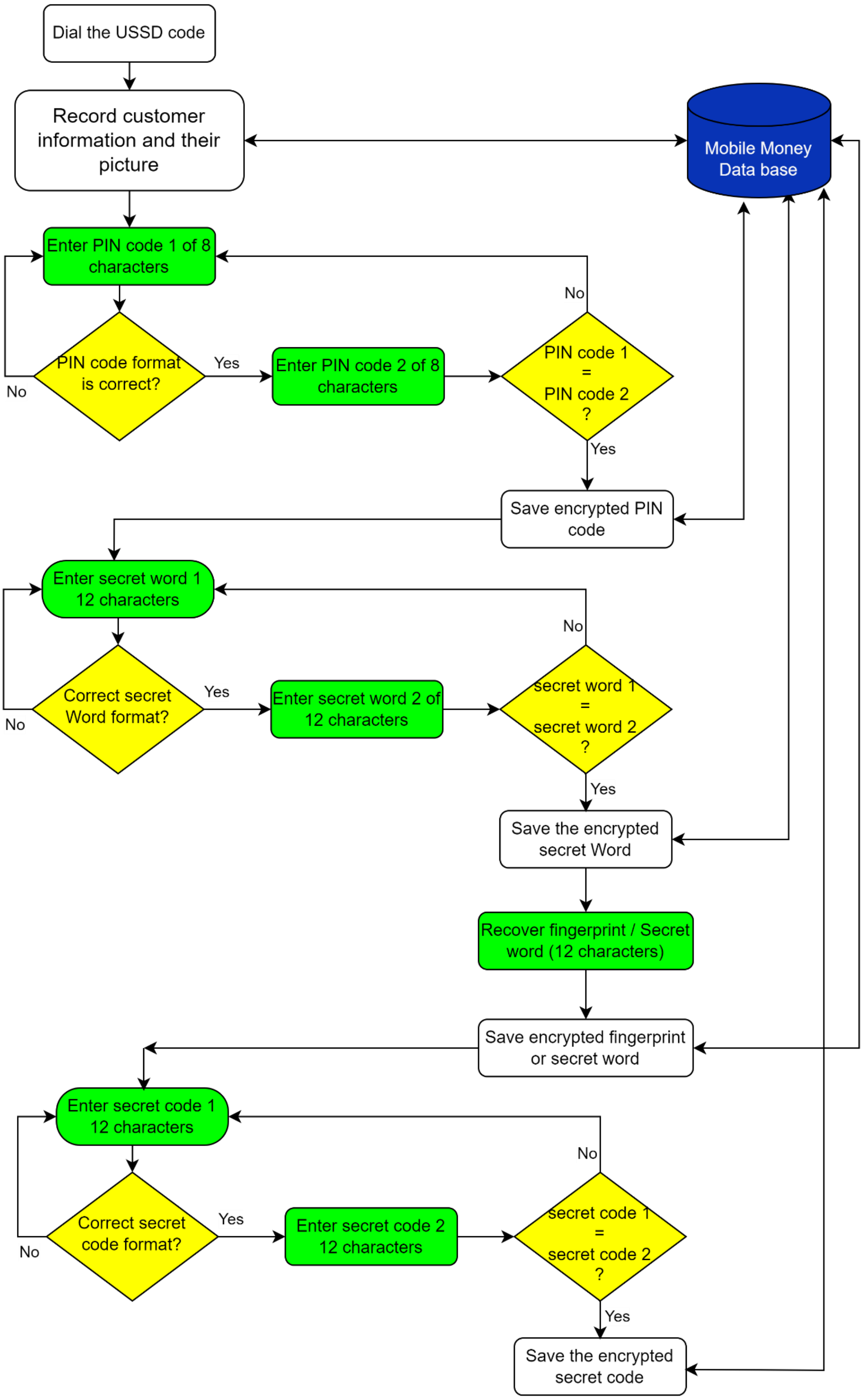
Dial the USSD code
Record customer information and their picture
Mobile Money Data base
Enter PIN code 1 of 8 characters
PIN code format is correct?
Yes
No
Enter PIN code 2 of 8 characters
PIN code 1 = PIN code 2 ?
No
Yes
Save encrypted PIN code
Enter secret word 1 12 characters
Correct secret Word format?
Yes
No
Enter secret word 2 of 12 characters
secret word 1 = secret word 2 ?
No
Yes
Save the encrypted secret Word
Recover fingerprint / Secret word (12 characters)
Save encrypted fingerprint or secret word
Enter secret code 1 12 characters
Correct secret code format?
Yes
No
Enter secret code 2 12 characters
secret code 1 = secret code 2 ?
No
Yes
Save the encrypted secret code

Fig. 1. Customer identification

When identifying a mobile money customer, the customer provides an identity document allowing all information about them to be recorded. After this step, the customer's photo is captured and all this information is recorded in the mobile money operator's database. Then, the customer enters his six (6) character password which is also recorded in the operator's database. Finally, the client enters a secret recovery word. All this information is encrypted and saved at the database level.

2.2 MONEY DEPOSIT SYSTEM

In the money deposit system offered via mobile money services, the sender receives a money withdrawal code which he must transfer to the recipient as illustrated in Figure 2.

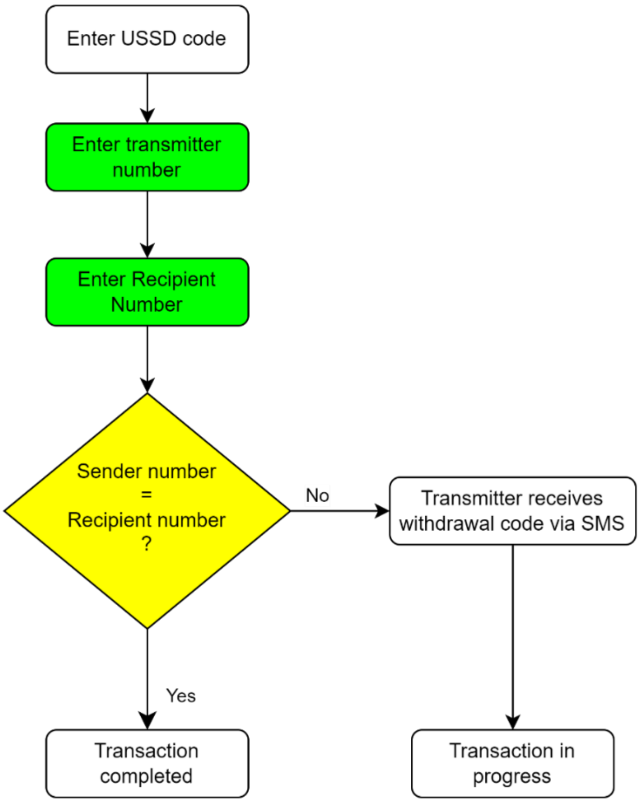

Fig. 2. Money deposit

Indeed, this system will make it possible to curb the actions of ill-intentioned people who pose as victims in order to defraud honest citizens. With this system, if the recipient has not received the withdrawal code, they cannot access the money. Suppose I made a deposit to a bad person and just after depositing I realize that I am facing an anarchy, I can block the process by confiscating the withdrawal code so that the process fails after a certain period.

2.3 MONEY WITHDRAWAL SYSTEM

In the process of withdrawing money, we verify the identity of the person who came to make the withdrawal in order to curb those who steal mobile phones and who have knowledge of the PIN code of official holder of the phone. In this action, the customer identity verification is verified by the service provider and the withdrawal transaction is authorized if the customer identity is the same with that of the number on which the money will be withdrawn as shown in the figure 3.

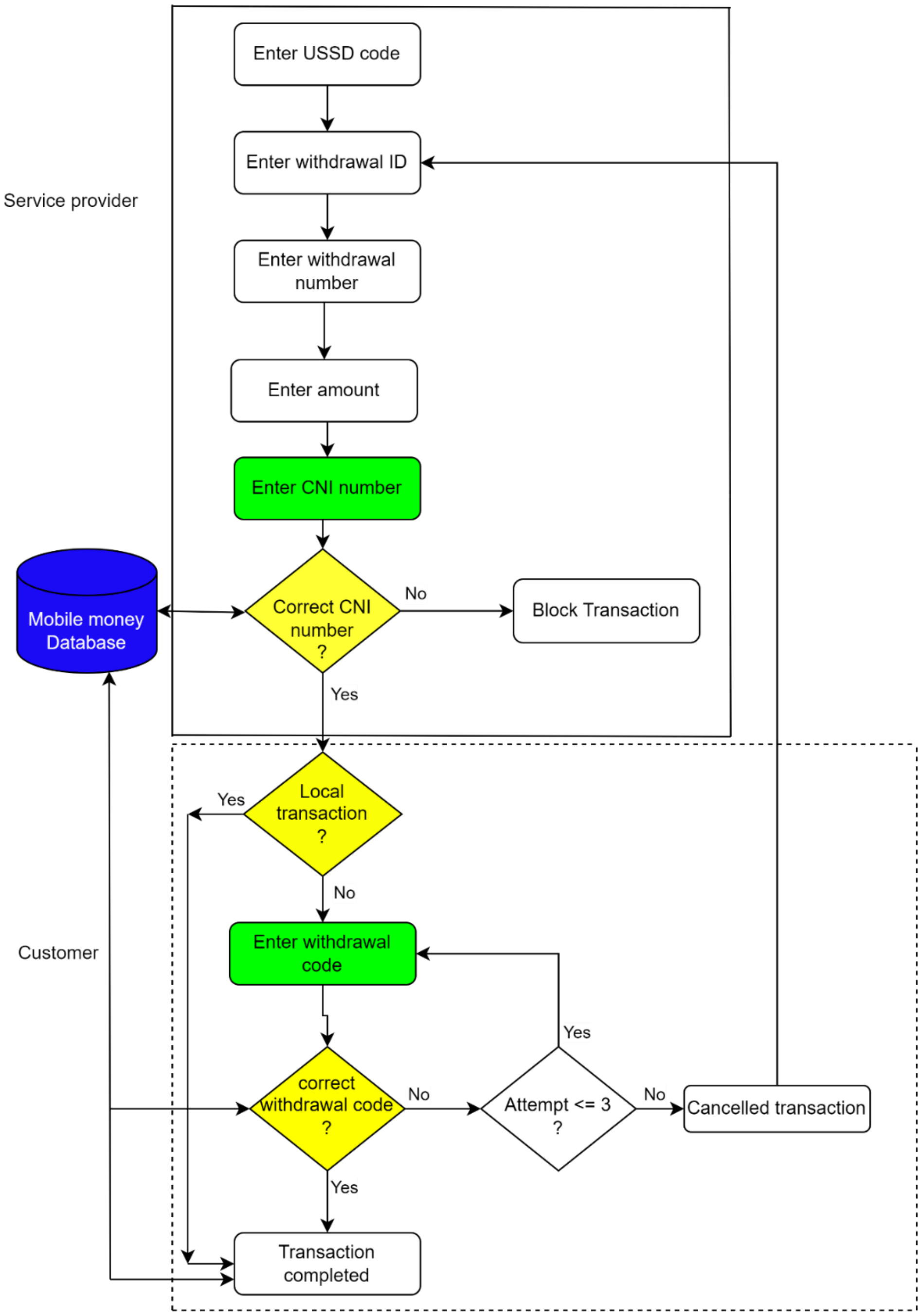

Fig. 3. Withdrawal

2.4 CHANGE PASSWORD

In the current system, a malicious person can change the password or PIN code of a mobile money account if he or she has possession of the user's mobile phone and its PIN code. To avoid these situations, we proposed a new password modification system which takes into account another authentication parameter authorizing password change as presented in Figure 4.

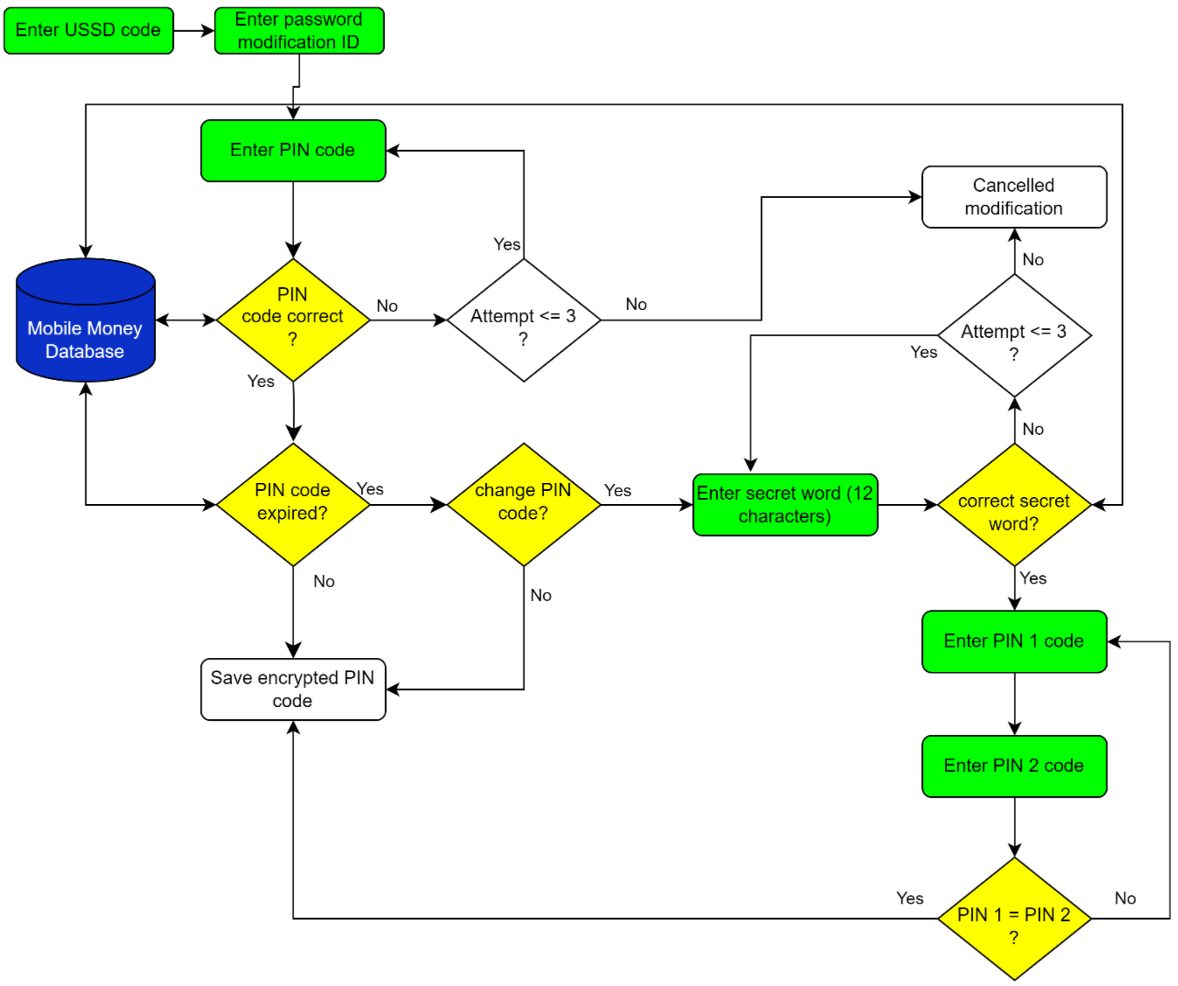

Fig. 4. Password modification

2.5 Money transfer system via mobile money services

The money transfer operation via mobile money services is a service that allows you to send and receive money. In Ivory Coast, the system in place uses a password authentication system. With this system, all it takes is for a malicious person to have the mobile phone and knowing its PIN code, they can transfer money to another account. To curb these types of transactions, we proposed a new multi-factor authentication system that takes into account the PIN code, the fingerprint and a secret code as illustrated in Figure 5.

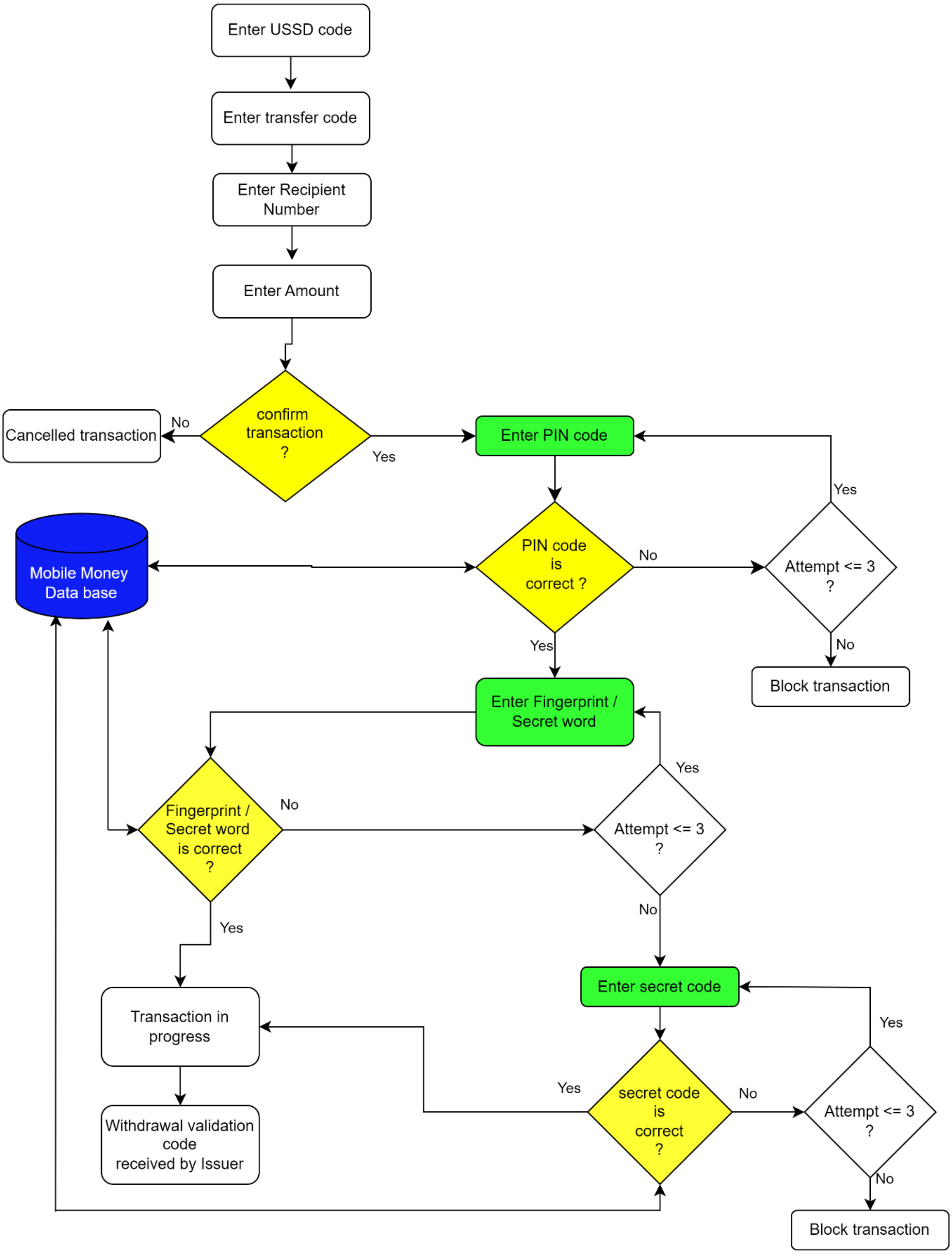

Fig. 5. Money transfer authentication system

3 ANALYSIS OF PROPOSALS

In Ivory Coast, the current identification system is limited to information linked to the identity of the customer with a password or secret code composed of four (4) digits without fingerprints. In our contribution, we propose to integrate the consideration of the fingerprint, a secret word of twelve (12) characters with a secret code of at least twelve (12) characters.

Concerning the deposit system, we proposed a solution which makes it possible to slow down deposits made in error by integrating a withdrawal code that the issuer must transmit to the recipient before the latter receives the amount deposited. This deposit system will also help curb anarchists because an issuer can refuse to transfer the withdrawal code to the recipient if he realizes that the latter is a scammer after he has made the deposit.

Our current mobile money system allows the customer to change their password. However, an attacker, if he manages to steal the client's password, has the possibility of modifying the password of the legitimate client. In our proposal, to slow down this, the client is asked for a secret code in addition to the password in order to be able to change the password.

As part of the money transfer, in addition to the password which is requested during the transaction, we have offered to provide the fingerprint or the secret word of twelve (12) characters depending on the type of mobile of the customer and allow the sender to receive a withdrawal code to provide to the recipient. This contribution makes it possible to slow down illegitimate transactions carried out by attackers who know the password of the customer's password and have possession of their mobile phone.

4 CONCLUSION

In this study, we reviewed the authentication systems proposed in the literature in the context of mobile money services. We analyzed the different authentication factors adopted in relation to what is done in Côte d'Ivoire and we proposed a new authentication system for mobile money services. Our contributions take into account the customer's mobile phone type (Android or not) and several authentication factors. We have developed an authentication algorithm for transfers using a password, fingerprint or secret word and a secret code. For direct deposit, we have proposed a system that provides a withdrawal code to the issuer that the recipient must provide upon withdrawal. We also proposed an authentication algorithm for password changes based on the current password and a secret code to provide. In our future work, we will propose a mobile money application based on this authentication system in order to propose it to the authorities in order to help them make better decisions in the context of mobile money services.

REFERENCES

[1] Telecommunications/ICT Regulatory Authority of Côte d'Ivoire, «SUMMARY OF KEY INDICATORS OF THE IVORIAN TELECOMMUNICATIONS MARKET IN THE 1st QUARTER 2023», *Key market indicators*. https://www.artci.ci/index.php/marches-regules/observatoire-telecoms/statistiques-du-marche-telecoms/entreprises-cles.html (accessed August 26, 2023).

[2] Minister of Planning and Development, «FINITIVE OVERALL RESULTS OF RGPH 2021: THE POPULATION USUALLY LIVING IN THE IVORY TERRITORY IS 29,389,150 INHABITANTS», *CI GOVERNMENT*. https://www.gouv.ci/_actualite-article.php?recordID=13769 (accessed August 26, 2023).

[3] CICG, «CYBERCRIME: THE PLATFORM TO FIGHT AGAINST CYBERCRIME HANDLES AN AVERAGE OF 4,500 TO 5,000 COMPLAINTS PER YEAR», *CI GOVERNMENT*. http://www.gouv.ci/_actualite-article.php?recordID=12960 (accessed August 26, 2023).

[4] G. Ali, M. Ally Dida, and A. Elikana Sam, «Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures,»*Future Internet,* flight. 12, no. 10, p. 160, Sep. 2020, doi: 10.3390/fi12100160.

[5] G. Ali, M. Ally Dida, and A. Elikana Sam, «Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda,»*Information,* flight. 11, no. 6, p. 309, June 2020, doi: 10.3390/info11060309.

[6] G. Ali, MA Dida, and A. Elikana Sam, «A Secure and Efficient Multi-Factor Authentication Algorithm for Mobile Money Applications,»*Future Internet,* flight. 13, no. 12, p. 299, Nov. 2021, doi: 10.3390/fi13120299.

[7] AAS AlQahtani, Z. El-Awadi, and M. Min, «A survey on user authentication factors,» in*2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON),* IEEE, 2021, p. 0323-0328.

[8] WA Hammood, RA Arshah, SM Asmara, and OA Hammood, «User Authentication Model based on Mobile Phone IMEI Number: A Proposed Method Application for Online Banking System,» in*2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM),* IEEE, 2021, p. 411-416.

[9] I. Islam, KM Munim, MN Islam, and MM Karim, «A proposed secure mobile money transfer system for SME in Bangladesh: An industry 4.0 perspective,» in*2019 International Conference on Sustainable Technologies for Industry 4.0 (STI),* IEEE, 2019, p. 1-6.

[10] K. Sudharsan, VA Kumar, R. Venkatesan, V. Sathyapreiya, and G. Saranya, «Two three step authentication in ATM machine to transfer money and for voting application,»*Procedia Computer Science,* flight. 165, p. 300-306, 2019.

[11] S. Rwiza, M. Kissaka, and K. Kapis, «Security Model for Tracking Creation of Mobile Money Using Transport Layer Security Protocol,»*Tanzania Journal of Science,* flight. 46, no. 3, p. 791-806, 2020.

[12] S. Ali, «Analyzing Mobile Banking Security using Biometric Authentication.» Rochester, NY, April 28, 2022. doi: 10.2139/ssrn.4096398.

[13] MJ Zadeh and H. Barati, «Security Improvement in Mobile Banking Using Hybrid Authentication», in*Proceedings of the 2019 3rd International Conference on Advances in Artificial Intelligence,* Istanbul Turkey: ACM, Oct. 2019, p. 198-201. doi: 10.1145/3369114.3369151.

[14] Z. Mirza, E. Alsalem, F. Mohsin, and WM Elmedany, «Users' Acceptance of Using Biometric Authentication System for Bahrain Mobile Banking,»*KnE Engineering,* p. 102-121, Oct. 2018, doi: 10.18502/keg.v3i7.3075.

[15] A. Adeniyi, «Factors to Consider to Minimize Identity Theft in Mobile Banking,»*ISACA JOURNAL,* flight. 5, p. 1-5, 2017.

[16] K. NAZAR, «Role of biometric authentication in the security of mobile banking applications | Inoxoft», *Inoxoft Blog,* March 28, 2023. https://inoxoft.com/blog/role-of-biometric-authentication-in-mobile-banking-app-security-benefits-features-risks/ (accessed August 28, 2023).

[17] WB Mercy and R. Mazer, «Mobile Financial Services: Protecting Customers, Providers, and the System from Fraud,» *www.cgap.org,* 2017.
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/
https://www.cgap.org/sites/default/files/Brief-Fraud-in-Mobile-Financial-Services-April-2017-French.pdf

[18] «Open a Moov Money account», *MOOV AFRICA IVORY COAST*.
https://www.moov-africa.ci/moov-money/ouvert-un-compte-moov-money/ (accessed September 1, 2023).