

DESIGN OF SECURE MOBILE PAYMENT SYSTEM WITH BIOMETRIC AUTHENTICATION BASED ON CONNECTED OBJECTS

Abdou Khadre Dieylani FALL*, Ahmed Dooguy KORA*, Hamidou DATHE**

*Ecole Supérieure Multinationale des Télécommunications. Roudé Fann Bel Air Dakar Liberté SENEGAL

**Cheikh Anta Diop University. Dakar-Fann SENEGAL

kocc26@yahoo.fr, ahmed.kora@esmt.sn, hamidou.dathe@yahoo.fr

Abstract— Mobile technologies have grown rapidly and operators have made huge investments in the deployment of mobile networks (3G, 4G, and 5G). Mobile payment systems are also developing rapidly and several players are involved in the ecosystem (mobile operators, banks and financial institutions, payment service providers, manufacturers, merchant, end users, etc.). However, for a broad adoption of mobile payment systems, security must be ensured. Several solutions have been proposed. The aim of this study is to propose a secure payment system using connected objects as payment terminals and which is based on a biometric authentication and on use of tokens (for the payment). The security analysis has shown that our solution has a good level of security and can prevent fraudulent transactions. In addition, using customer's fingerprint in the multi-step payment validation process ensures maximum security. This mechanism, combined with geolocation and the use of tokens (basic tokens, payment tokens), increases the security provided. Additionally, we compute the complexity of our algorithm using the Landau asymptotic notation and the grand O notation. We have seen that our algorithm have a complexity of $O(n^2)$ where n is the length of the square matrix of tokens used to choose one validation code for the payment. Our solution presents a good level of performance compared to other algorithms previously studied mainly because it does not use cryptographic operation and the computational load occurs only on the platform.

Keywords— security, biometrics, fingerprint, mobile technologies, algorithm complexity, mobile payment.

I. INTRODUCTION AND OVERVIEW ON MOBILE PAYMENT SYSTEMS AND BIOMETRICS

In a simple way, mobile payment refers to any transaction of goods and services that uses mobile equipment (mobile phone, bank card, connected objects ...). Sensitive data (personal identity, account number, bank card, passwords ...) are often transmitted in a mobile payment process. As a result, they are subject to many threats and security challenges are numerous. This first part of the document presents an overview on mobile payment and biometrics. We will also talk about the security of mobile payments. In the second part, we will focus on the different security solutions proposed for mobile payment systems. The third part of the document presents the design of our solution. The fourth and final part provides a security analysis of the proposed solution as well as an analysis of the complexity of the proposed algorithm.

The mobile phone is today a terminal that can be used in many transactions. In the field of payment, several use cases can be envisaged: **in a basic GSM authentication process, as**

digital signature, in a payment application. A mobile payment system involves several technologies aimed at addressing the various technical, operational and security requirements. Mobile payment systems are often classified into 5 categories: **mobile payments where the customer pays at the point of sale terminal with his mobile phone** (example: Google wallet, Apple pay); **mobile payments where the merchant uses his mobile phone as a point-of-sale terminal to process transactions** (example: Square Register); **mobile payment platforms that provide payment services on mobile device where you have to download and install an application** (example: PayPal, Alipay); **independent mobile payment systems** where a company (e.g. Amazon, Starbucks) decides to develop its own online payment service and provide the same services as mobile payment platforms, and these systems can quickly be opened if they are widely adopted by merchants and retailers; **direct billing systems by the operator** where the customer does not need to have a credit / debit card and the amount of the transaction is added to the subscriber's bill.

Biometrics was mainly developed to address the problem of weakness and loss of passwords. It is an identification / authentication method based on human, physical or behavioral data. The biometric means are often classified in 2 categories and differ as much on the level of security offered as on the ease of implementation: **the physical (physiological) means** such as the iris, the fingerprint and the **behavioral means** such as voice, signature or keystroke dynamics. A biometric process often follows 3 steps: **registration/enrollment, verification and identification.** All biometric systems have not the same performance and these criteria below are used to measure the performance of a biometric system: **False Recognition Rate (F.R.R), False Acceptance Rate (F.A.R), and Equal Error Rate (E.E.R).** Biometric authentication systems are increasingly used in mobile payment systems. Biometric devices (fingerprint reader for example) are embedded in mobile phones (Apple, Samsung ...) and other accessories such as biometric scanners are accessible at low cost. The use of biometrics in mobile payment systems offers many advantages. The customer no longer needs to use a token or store a password to trade, and that improves convenience. The difficulty of identity theft, and even sharing an individual's biometric traits strengthens the security of biometric payment systems. There is a close link between the user and his identifiers.

A secure mobile payment system must have the following properties: confidentiality, authentication, integrity,

availability, non-repudiation and authorization. Several security threats and attacks with serious impacts have been identified in mobile payment systems. In 2014, Symantec identified more than one million applications considered as malware able of carrying out fraudulent activities (call recording, sending instant messages, tracking via GPS, password spoofing ...). Mobile payment systems rely on SSL / TLS to protect data transiting over the internet. This protocol is known to be vulnerable to the attack of the "man in the middle". The security challenges are therefore numerous and affect several aspects: the security of mobile equipment (data storage, OS security, etc.), the security of the various network technologies (access, transport, etc.) and the security of the services provided to the various entities. Several security mechanisms have been proposed to address these threats.

II. LITERATURE REVIEW ON MOBILE PAYMENT SYSTEMS SECURITY

We present a review of literature on mobile payment systems security.

In [1] Shemin and Vipinkumar offer an electronic payment system based on quantum cryptography, visual cryptography and image steganography. The visual cryptography used in this system protects the customer's data by masking the details of the client authentication by generating 2 elements called "share" for the bank and the client respectively. Quantum cryptography secures the transmission of a one-time password (OTP One Time Password). Image steganography helps secure the transmission of the customer's share to the bank by combining it with the one-time password. These two proceedings (quantum cryptography and steganography) prevent security threats such as phishing and identity theft.

If a spy succeeds to recover the "share" of the client sealed in a one-time password during transmission to the bank, he will not be able to reuse this "share" and pretend to be the client because at each transmission, a new password is generated. So if the hacker sends this pirated "share" to the bank, the validation of the one-time password fails and the transaction is rejected. The use of quantum cryptography enables to securely carry the one-time password. The spy is not able to obtain the authentication details of the client from the "share" of the client because to get it he must mix the 2 "share" (share of the client and share of the bank).

In [2] Wei Feifei designs a mobile payment security model based on a trusted third party. This model ensures data integrity, confidentiality, non-repudiation and authentication. The 4 main elements of the model proposed by Feifei are:

- Mobile equipment that communicates with the application server, trusted third party server and other devices via wireless internet.
- The application server that is the ecommerce platform and provides the service according to the demand of the mobile terminal.
- The PKI that provides the security services.
- The trusted third party that provides mobile devices with a way to access the platform. It completes the services related to the PKI by allowing the merchant

to authenticate to the mobile terminal. It also provides undeniable evidence in case of conflict around a transaction.

Feifei proposes a 2-step authentication model: a first authentication between the mobile terminal and the trusted third party, and a second authentication between the mobile terminal and the application server.

In [3] Sheyful offers a 3-layer security model to secure electronic transactions: **layer 1: traditional security (login, PIN); layer 2: biometric security using fingerprints or iris recognition; layer 3: mobile security (GPS or mobile SMS).**

The authors in [4] propose a security analysis of electronic payment protocols based on quantum cryptography. The authors introduce a formal analysis method to analyze the security properties of an electronic payment system based on quantum cryptography. They relied on previous work published by other authors on the same subject. Their work has shown that these protocols do not comply with all the requirements and security properties including accountability and fairness. Accountability can provide sufficient evidence to resolve potential future disputes after protocol execution. A communication protocol having the property of fairness is such that it assures an honest party, having emitted the information that is expected from him, to receive the information that he even discounts. Then they propose an improved version of the protocol and check through a formal method analysis that this protocol meets the properties of accountability and fairness.

Rajendran, Kumar and Bindhumadhava propose in [5] a secure digital payment system that ensures privacy. The authors propose digital tokens. These are an abstraction of the classic currencies and have an equivalent value. An intermediary entity will mediate the transaction between a payer and a payee. The system is based on existing payment systems and ensures confidentiality and privacy of the actors. It also protects against potential fraud and provides interoperability between different banks, equipment and service providers.

In [6], the authors propose a mobile payment infrastructure based on biometrics. To ensure the security of mobile payment systems, they offer a secure infrastructure that combines multimodal biometric cryptography (fingerprint and vein biometrics) with time-based encryption based on a single password.

Yang uses the concepts of identity-based cryptography to design a mobile payment system in [7]. An identity-based signature is added to the transaction data and a unique key is used to encrypt that data. Customer side cryptographic operations are implemented in a smart card in which several algorithmic functions are designed. This mechanism provides better security compared to other solutions like SET and 3-D Secure.

In [8] Ahang and Xeng propose, a mobile payment protocol based on a dynamic token. The protocol includes 4 steps: **system initialization, user registration and authentication, transaction request and payment.** The security of the mobile terminal is ensured using a password and by fingerprint

identification. The use of the SSL protocol ensures the security of the communications. Authentication and payment security are ensured using dynamic token and using certificateless public key cryptography techniques. The protocol allows to authenticate the user through his personal information and through the mobile phone. The user logs in to the system through a password or fingerprint. During the payment process, the dynamic token generated by the mobile phone contains the phone's IMEI number and the smart card's ICCID code, thus ensuring the safety and reliability of the mobile phone. Once the authentication is successful, the server will be able to execute the payment requests and handle user's funds to complete the payment.

IV. DESIGN AND ARCHITECTURE

We propose to set up a secure payment system based on:

- **Biometric fingerprint authentication.**
- The creation of **initialization (or basic) tokens** (at the activation of the customer's account) and **payment tokens** (for the validation of a transaction).
- **Geolocation** of entities from the HLR of the mobile network.

We propose to simulate payment terminals from connected objects. We suggest using Arduino or Raspberry PI. The connected object as payment/validation terminal is equipped with GSM module to communicate with the mobile phone network and WIFI module to communicate with the payment platform via the Internet. A fingerprint reader is also connected to the microcontroller, as well as an LCD for displaying the data. **Figure 1** shows the architectural design of our secure mobile payment solution.

The payment platform consists of a set of servers connected to the Internet for enrolling customers and validating payments.

The payment platform also communicates with various partners (banks, mobile operators, financial institutions) in a secure way to obtain some customer information, mainly the customer balance. This part (secure communication between the platform and the partners) is not concerned in our paper. We will just point out that the platform has all the information regarding the payment capacity of the customer (balance).

Note that this device is only intended to validate the payment of a customer who makes a transaction with a merchant.

We will also assume that the device allows the secure transmission of the fingerprint to the enrollment platform and its secure storage.

In this paper, we will design the different algorithms that will allow the customer to make an electronic transaction securely via the platform.

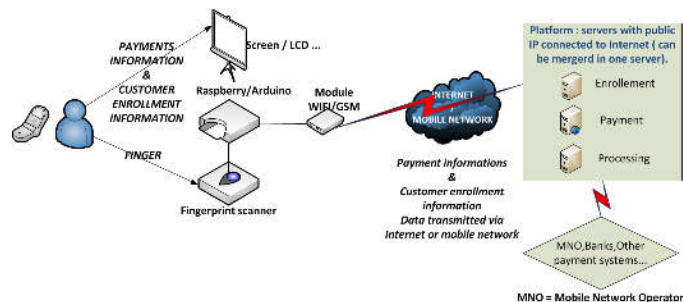


Figure 1. Architectural design of the secure payment solution

V. SECURITY ANALYSIS, COMPLEXITY AND PERFORMANCE ANALYSIS OF THE ALGORITHM

A. Security analysis

The different security properties to be insured are mainly: authentication, integrity, confidentiality and non-repudiation.

In our paper, the various entities that communicate mainly are: the customer, the merchant, the payment platform. We have seen that other players are included in the payment process (banks, financial institutions, mobile operators ...).

We are mainly interested in this work by the security of the communication between the customer, the merchant and the platform of payment. At each stage of the algorithm, we will check how the security properties are handled.

1) Step 1: Account initialization

The client logs in via a web interface to initialize his account. Traditional security mechanisms will be applied for secure connection to the web interface and data transmission.

The data transmitted during this step (last name, first name, address, national identification number, telephone number) are sent to the payment platform via the Internet. The security mechanisms for the transmission of data on the Internet will therefore be required during this phase (encryption).

2) Step 2: Account validation

To activate his account, the customer must provide his fingerprint. Security at this level is ensured by 3 mechanisms:

- **Geolocation:** Any customer who wishes to activate his account must have the same geolocation than the activation / payment terminal.
- The **use of an activation code** with an activation delay. Before validating the activation of an account, the platform sends the customer an activation code on his mobile. If the client returns the correct code within the specified time, his account is activated. At this moment, the fingerprint he has transmitted is considered attached to his account.
- The **length of the activation code.**

This process makes it possible to authenticate the customer when he validates his account. The customer is authenticated if he returns the correct validation code. The customer, in order to authenticate the platform, returns a number that represents the length of the validation code that he wishes to receive. If the platform returns a validation code of equal

length to that requested by the customer, the latter will have authenticated the platform.

But even if the fingerprint was modified by a spy before being transmitted, its storage in the platform would be impossible because the validation operation of the account is finalized only if the customer returns the correct validation code. And even if the spy directly alters the fingerprint in the platform (extreme case) this modification would have no impact on the customer's transactions (balance, volume and value of the transactions) because as we will see later in transaction validation, in addition to provide its fingerprint, a transaction validation code is used. The main risk in this scenario is that the customer will not be able to make a payment (because his fingerprint is different than the one known by the platform). To avoid this scenario, we will assume that security mechanisms for the transmission and storage of information (fingerprint, customer info) will be implemented in the platform (encryption, steganography ...). The fingerprint is transmitted by the terminal via the Internet and is stored in the payment platform. The security of the transmission of the fingerprint must therefore be ensured as well as the security of its storage. But this is not the object of this paper.

3) Step 3: Payment and transaction validation

The security of this step is based on the following mechanisms:

- **Geolocation:** the customer and the payment terminal must have the same geolocation.
- The use of a **payment validation code** based on the use of tokens (**basic token or initial token, payment token**) derived from a matrix of tokens payment.
- The **customer's fingerprint**.

In the payment process, all the steps to check customer information are done from the customer's fingerprint. So the fingerprint transmitted by the client must correspond to the one stored in the platform. If in this payment process, the transmission of the fingerprint is corrupted, the transaction will fail because the fingerprint communicated will be different from that known by the platform. Similarly, if the fingerprint stored in the platform is corrupted, the transaction will fail because the transmitted fingerprint will be different from the stored fingerprint.

In the extreme case where fingerprint, in its transmission is corrupted so that it corresponds to a stored fingerprint that itself is corrupted, a second layer of security where the client must return a validation code can prevent fraudulent transactions. The security in this case is based on the robustness of the validation code sent to the client (because we can think that in the scenario described above, access to a valid validation code to validate a transaction). This validation code (which is a token) will be derived from a token matrix whose elements are computed from the following elements:

- The **basic token (or initial token)** of the customer that is initialized at the validation of the customer's account. This token is created from the customer's fingerprint, his phone number, and a time variable (current time). This basic token is an element that is

periodically renewed. The periodicity is computed from a decreasing function of the following parameters: the volume and the value of the transactions, the customer's balance. The idea is the more the customer makes transactions (volume / value) and the higher is the customer's balance, the more the token needs to be renewed (e.g. the shorter the renewal period has to be).

- The **number of tokens in the tokens matrix**. This number is computed from an increasing function of the following parameters: the volume / value of the transactions and the customer's balance. So the more the customer does transactions (volume / values) and the higher the balance is, the more it will have tokens in the matrix. It is important to remember that only one token will be chosen from this matrix as a validation code.
- The **token used during the last transaction** made by the customer.
- **Customer's fingerprint**.

The difficulty of finding the correct validation code of the transaction comes from the fact that to find it, you need at time t:

- To have the customer's fingerprint.
- To have the correct basic token (difficult to find because it is renewed periodically).
- To know the number of token in the matrix (it is also updated after each transaction).
- To know the token used during the last transaction (which itself depends on the elements mentioned above).

No customer will be able to deny having made a transaction; since it is the validation code that he returns that will validate the payment. Also, the customer will be authenticated by the platform if it returns the correct validation code. The client is also sure to communicate with the right platform since he has already authenticated it during the step of validation of his account.

The platform also cannot deny the existence of a transaction, because the final payment code is the combination of the validation code sent to the customer and a random code generated by the platform. This random code is only known by the platform and a transaction cannot be validated without this code being generated beforehand.

B. Complexity and performance analysis of the algorithm

1) Reminder on the computing of algorithm complexity

The complexity of an algorithm is the number of elementary operations or memory positions that the algorithm needs to solve a problem of a certain size. Formally, the expression of a complexity takes the form of a mathematical function of the size of the data. There are two types of complexities: **time and spatial**.

Time complexity is the total number of elementary operations to execute the algorithm and spatial complexity is

the maximum number of memory locations used during algorithm execution.

We will only be interested in this study in the analysis of the worst-case time complexity that allows us to obtain an upper limit of the execution time.

We will be interested in the behavior of the algorithm when the size of the data tends to infinity. So, we will look at the order of magnitude of its complexity. We will use the **Landau asymptotic notation** and the **grand O** notation.

2) Notation O (grand O) definition

Given a function $f(n)$, $O(f(n))$ is the set of functions $g(n)$ such that there exists a real positive constant c and a non-negative integer N such that for all $n > N$, $g(n) < c \times f(n)$.

The notation $O(f)$ describes the asymptotic behavior of a function, e.g. for large values. In other words, g is $O(f)$ when, for sufficiently large values of n ($n > N$), the ratio $g(n) / f(n)$ is always bounded by c .

We distinguish different families of algorithms according to their upper bound: constant complexity $O(1)$, logarithmic complexity $O(\log n)$, log-linear complexity $O(n \log n)$, linear complexity $O(n)$, quadratic complexity $O(n^2)$, cubic $O(n^3)$ or more generally polynomial $O(n^k)$, exponential complexity $O(k^x)$.

The following properties will be used for complexity computation:

- $O(f)+O(g)=O(f+g)=O(\max(f,g))$ (addition distributivity).
- $O(f) \cdot O(g)=O(fg)$ (multiplication distributivity).

The following computation rules will be used for computing the worst-case time complexity.

- Elementary operation (we consider an instruction): constant time $O(1)$.
- Call of a function: If f is the worst complexity of the function, then the complexity of the call is in $O(f)$.
- Conditional test (IF): If f is the complexity of the condition and g_i the complexities of the different blocks (ELSE ...), then the worst-case complexity is in $O(f + \max(g_i))$.
- Loop (for, while, repeat): If f is the complexity of the block and the condition, and g the upper bound of the number of iterations at worst, then the worst-case complexity is in $O(f \cdot g)$.
- Sequence of instructions: if f_i is the complexity of the i^{th} instruction; then the worst-case complexity of the sequence is in $O(\sum f_i)$.
- In a database, you will find several kinds of file organization (sequential, indexed, random (hash code) with different complexities. With a sequential organization, the search from a field value requires to browse all the table, so with a complexity $O(n)$, indexing allows to have a complexity of $O(\log n)$ and the hashing, complexity of $O(1)$, so the search functions will have the following complexities: $O(1)$, $O(n)$ and $O(\log n)$ depending on the type of file organization in the database.
- The random () function is considered to be of constant complexity.

- The time () function is considered to be of constant complexity.
- The execution time of variable declarations is considered insignificant and is not taken into account in the calculation of costs.
- The following operations are considered elementary and of constant complexity $O(1)$: multiplication, addition, comparison, assignment, returns statement, logic, and concatenation.

Our solution has 3 main steps: **registration**, **validation of registration** and **payment**. Each step uses a set of functions. We will therefore compute the time complexity of each function by applying the rules outlined above.

3) Results

The computing of the complexities of the different functions is summarized in the following in Table 1.

Functions	Complexity
Function Initialize_Account (a, b, c, d, e)	$O(1), O(n), O(\log n)$
Function Search_Location(a, b)	$O(1)$
Function Gen_Customer_Validation_Code(a, b, c, d)	$O(1)$
Function Set_Validation_Account_Param(i)	$O(1)$
Function Create_Payment-Token(a, b, c, d, e)	$O(n^2)$
Function Create_Basic-Token(a, b, c)	$O(1)$
Function update_basic_token(a, b, c, d, e)	$O(1)$
Function search_customer_for_account_validation(a)	$O(1), O(n), O(\log n)$
Function search_id_for_account_creation(a)	$O(1), O(n), O(\log n)$
Function Validate_Account(a, b, Tel _{old})	$O(n)$
Function search_customer(a)	$O(1), O(n), O(\log n)$
Function check_balance(a)	$O(1), O(n), O(\log n)$
Function check_account_status(a)	$O(1), O(n), O(\log n)$
Function update_volume_trans(a)	$O(1), O(n), O(\log n)$
Function update_basic_token_after_payment(a, b, c, d)	$O(1), O(n), O(\log n)$
Function update_trans_value(a, b)	$O(1), O(n), O(\log n)$
Function search_trans_value(a)	$O(1), O(n), O(\log n)$
Function search_trans_volume(a)	$O(1), O(n), O(\log n)$
Function search_basic_token(a)	$O(1), O(n), O(\log n)$
Function search_token_last_trans(a)	$O(1), O(n), O(\log n)$
Function search_nb_token_payment(a)	$O(1), O(n), O(\log n)$
Function update_periodicity_renew_basic_token(a, b, c, d)	$O(1), O(n), O(\log n)$
Function update_nb_token_for_payment(a, b, c, d)	$O(1), O(n), O(\log n)$
Function update_balance(a, b)	$O(1), O(n), O(\log n)$
Function update_token_last_trans(a, b)	$O(1), O(n), O(\log n)$
Function validate_payment_transaction(E ₂)	$O(n^2)$

Table 1 . Complexity of the different functions of the algorithm

Following this results, we can conclude that our **overall algorithm complexity is $O(n^2)$** .

To assess the **performance of our algorithm**, we refer to [9] where authors perform the evaluation of five mobile payment protocols with different characteristics using their computational cost and their transmission time. The five payment protocols named in [9] as **Virtual PoS**, **Real PoS**, **Anonymous Payment**, **KSL** and **M-Cash** are studied in more details respectively in [10], [10],[11],[12] and [13].

In our paper, we have not taken into consideration the transmission time. We have mentioned that the interaction between entities occur via Internet (for the transmission of fingerprint and other data related to the transaction) and via GSM (for the transmission of different validation code and token to the customer). So to assess the performance of our algorithm, we will only compare the computational cost with authentication (only will be concerned Virtual PoS, Real PoS and M-Cash) of the different mobile payment protocol assessed in [9] to the order of magnitude related to the complexity of our algorithm.

We have seen that our algorithm have a complexity of $O(n^2)$ where n is the length of the square matrix of tokens used to choose one validation code for the payment. So according to Table 2, we can see while n is less or equal than 10000,

our algorithm has a better computational cost than all the other mobile payment protocols presented in [9].

Complexity	Time for n =							
	5	10	20	50	250	1 000	10 000	1 000 000
Constant complexity $O(1)$	10 ns	10 ns	10 ns	10 ns	10 ns	10 ns	10 ns	10 ns
Logarithmic complexity $O(\log n)$	10 ns	10 ns	10 ns	20 ns	30 ns	30 ns	40 ns	60 ns
Linear complexity $O(n)$	50 ns	100 ns	200 ns	500 ns	2.5 μ s	10 μ s	100 μ s	10 ms
Log-linear complexity $O(n \log n)$	40 ns	100 ns	250 ns	850 ns	6 μ s	30 μ s	400 μ s	60 ms
Quadratic complexity (polynomial) $O(n^2)$	250 ns	1 μ s	4 μ s	25 μ s	625 μ s	10 ms	1 s	2.8 hours
Cubic complexity (polynomial) $O(n^3)$	1.25 μ s	10 μ s	80 μ s	1.25 ms	156 ms	10 s	2.7 hours	316 years

Table 2. Magnitude order of time execution of an algorithm following his complexity

Table 3 sums up the different computational cost of the different algorithms and we see that our algorithm has better performance than the other. This is especially because in our algorithm, we do not use cryptographic operations and also all the computational cost is only supported by the platform. And for the other mobile payment protocols in [9], all the entities (customer, merchant and trust third party) perform cryptographic operations which can be heavy.

	Virtual PoS	Real PoS	M-Cash	Our solution for $n \leq 10000$
Total Computational cost(s)	7,893	11,734	4,003	1

Table 3. Computational cost of the different payment systems solution

VI. CONCLUSIONS

In the work presented in this document, we have proposed and designed a mobile payment solution with connected objects as payment terminals and which rely on a biometric authentication and use of token payment. The solution ensures that transactions (especially payment) are safe. So the other aspects that may be involved in a transaction are not taken into account but we can consider interconnecting the platform to other applications (inventory management application, billing application ...).

The security analysis has shown that our solution has a good level of security and can prevent fraudulent transactions. In addition, the use of the customer's fingerprint in the multi-step payment validation process ensures maximum security. This, combined with geolocation and the use of tokens (basic tokens, payment tokens), increases the security provided. Moreover our algorithm presents a good level of performance compared to other algorithms previously studied mainly because no cryptographic operation is used.

However, to retrieve the customer's balance information, our platform needs to be interconnected to other platforms (banks, financial institutions, mobile operator) that will provide this information. And it will be necessary to ensure a good level of security for the exchange of information between the different platforms. That is one of the challenges. The other major challenge also concerns the security of the biometric template and the secure storage of information in the platform (encryption and steganography techniques). Another challenge is the platform scalability test. Our platform must be able to process a number of transactions simultaneously. These different points will probably be studied in our next works.

REFERENCES

- [1] P.A.Shemina, K.S.Vipinkumar. "E-Payment System Using Visual and Quantum Cryptography". International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST - 2015).
- [2] Wei Feifei. "Research on Security of Mobile Payment Model Based on Trusted Third Party". 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing
- [3] Md. Syeful Islam. "An Algorithm for Electronic Money Transaction Security (Three Layer Security): A New Approach". International Journal of Information and Computer Security · February 2015.
- [4] Yi Liu, Xingtong Liu, Jian Wang, Lei Zhang and Chaojing Tang. "Security analysis of electronic payment protocols based on quantum cryptography." 2017 4th International Conference on Information Science and Control Engineering.
- [5] Balaji Rajendran, Anoop Kumar Pandey, B S Bindhumadhava. "Secure and privacy preserving digital payment." Centre for Development of Advanced Computing Bangalore, India. 2017.
- [6] Wencheng Yang, Jiankun Hu, Song Wang, Jucheng Yang, Lei Shu. "Biometrics for securing mobile payments: Benefits, challenges and solutions." 2013 6th International Congress on Image and Signal Processing (CISP 2013).
- [7] Yang Rui-Xia. "Design of Secure Mobile Payment System Based on IBC". 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications.
- [8] Xuewang Zhang, Hao Zeng, Xuewang Zhang. "Mobile payment protocol based on dynamic mobile phone token." 2017 9th IEEE International Conference on Communication Software and Networks.
- [9] Rafael Martinez-Pelaez, Francisco Rico-Novella. "Study of mobile payment protocols and its performance evaluation on mobile devices". Article in International Journal of Information Technology and Management · January 2010
- [10] Marko Hassinen, Konstantin Hyppönen, and Keijo Haataja, "An Open, PKI-Based Mobile Payment System". University of Kuopio, Department of Computer Science POB 1627, FIN-70211, Kuopio, Finland. 2006
- [11] Jesus Téllez Isaac, José Sierra Camara, Antonio Izquierdo Manzanares, Joaquín Torrez Marquez. "Anonymous Payment in a Kiosk Centric Model using digital schemes with message recovery and low computational power Devices". 2006
- [12] Supakorn Kungpisdan, Bala Srinivasan, and Phu Dung Le. "Lightweight Mobile Credit-Card Payment Protocol". School of Network Computing, Monash University McMahon Road, Frankston, Victoria 3199 Australia. 2003.
- [13] Rafael Martinez-Pelaez, Francisco Rico-Novella. "New ash Electronic Model: A script anonym". Technical University of Catalonia, Department of Telematics Engineering. C/Jordi Girona 1 i 3, C3, D-214, 08034, Barcelona, Spain. 2006.
- [14] Dhvani Shaha, Vinayak Bharadib. "IoT based Biometrics Implementation on Raspberry Pi." 7th International Conference on Communication, Computing and Virtualization 2016.
- [15] C.Sunil, Prof. K. Prahlada Rao. "Embedded Linux based smart security system using IoT and raspberry pi processor." International Journal of Technical Innovation in Modern Engineering & Science. Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585. Volume 3, Issue 11, November-2017.
- [16] Jordi Sapes, Francesc Solsona. "FingerScanner: Embedding a Fingerprint Scanner in a Raspberry Pi". Department of Computer Science and INSPIRES, University of Lleida, Jaume II 69, Lleida 25001, Spain; Academic Editor: Vittorio M.N. Passaro. Received: 14 October 2015; Accepted: 30 January 2016; Published: 6 February 2016.
- [17] N ChitraKiran, Bhuvan Teja, Suchira Suresh, B Krishna, S M Akarsh, Jerrin Yomas. "A biometric based payment system by using payee and payer module." 2017 2nd IEEE International Conference On Recent Trends in Electronics Information & Communication Technology (RTEICT), May 19-20, 2017, India.
- [18] Ram Kumar Garg -- N K Garg. "Developing secured biometric payments model using Tokenization." 2015 International Conference on Soft Computing Techniques and Implementations- (ICSCTI) Department of ECE, FET, MRIU, Faridabad, India, Oct 8-10, 2015
- [19] Dastgir Pojee, Sajjad Zulphekar, Fahim Harh, Varsha Shah. "Secure and quick NFC payment with data mining and intelligent fraud detection." Proceedings of the 2nd International Conference on

Communication and Electronics Systems (ICCES 2017).IEEE Xplore
Compliant - Part Number: CFP17AWO-ART, ISBN: 978-1-5090-5013-0
[20] Ariana Tulus Purnomo, Yudi Satria Gondokaryono, Chang-Soo
Kim. "Mutual authentication in securing mobile payment system using
encrypted QR code based on Public Key Infrastructure." 2016 IEEE 6th
International Conference on System Engineering and Technology(ICSET) .
Oktober 3-4, 2016 Bandung – Indonesia



Abdou Khadre Dieylani FALL was born in Dakar (Senegal) on August 26, 1986. In 2006, he received a degree in Telecommunications and Networking at Ecole Supérieure Polytechnique de Dakar. He also received a Bachelor's degree in Computer Science at Université Cheikh Anta Diop in 2009. In 2011, he received a Master 2 in Cryptology, Software Science and Database at Université Cheikh Anta Diop. He finally received a Master 2 in Systems and Networking at Université Gaston Berger de Saint Louis.

He is actually a PhD Student in Telecommunications at Ecole Supérieure Multinationale des Telecommunications and Ecole Supérieure Polytechnique de DAKAR. He also has 11 years of experience in telecommunication services, network security and mobile financial services at SONATEL (Société Nationale de Télécommunications du Sénégal).

His research area covers networking and communications architectures and security, SDN/NFV, Cyber security, IoT, Mobile Technologies, Machine learning in cyber security and finance.



Ahmed D. KORA was born in Parakou (Benin Republic) on May 17, 1971. He is graduated in Physics Sciences in 1998 from "Faculté des Sciences Techniques" at "Université d'Abomey-Calavi", Bénin, where he got his Diplôme d'Etude Approfondie (DEA) in Material Sciences in 2000. In 2003, he received a Master "Réseaux Télécoms" degree from "Ecole Supérieure Multinationale de Telecommunications" (ESMT) and the Ph.D. degree in telecommunication from the University of Limoges, France, in 2007. He is

currently with the ESMT and Director of Research and Innovation. His research area covers communications, radio and optical networks system architecture, universal access, mobile network quality of service and quality of experience, low cost IT systems for development, etc. Prof. KORA is IEEE member and also member of Fiber Optic Association



Hamidou DATHE is working in Cheikh Anta Diop University as Full Professor. He is the Head of Doctoral School of Mathematics and Informatics at Cheikh Anta Diop University. His area of research is mathematics and differential geometry and applications.