International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-12 Issue-4, March 2023

Securing the User Registration Process in an IP Telephony System using Blockchain and KYC Technologies

Sekoude Jehovah-Nis Pedrie SONON, Tahirou DJARA, Abdou Wahidi BELLO, Matine OUSMANE

Abstract: ***In this article, we develop a solution for securing IP telephony networks. The solution developed is based on revolutionary blockchain technology. It uses KYC, facial recognition and OTP techniques to secure the various levels of user interaction with the ToIP network (enrolment, authentication, communication session, post-communication session). A comparative study, based on the Ethereum and Hyperledger Fabric blockchains, enabled us to select Hyperledger Fabric as the development framework for our blockchain. The criteria justifying our choice are essentially: the modularity of the architecture, the variety of programming languages for smart contracts, the possibility of creating private channels between network members, high access control and data confidentiality, as well as a flexible consensus model. These criteria are crucial, as they guarantee both the robustness and flexibility of the network in a shared communication data context. To guarantee data confidentiality, access rights management and transaction speed, we opted for a private blockchain developed under the Hyperledger Fabric framework.***

Keywords: Blockchain, Hyperledger fabric, IP telephony, KYC Security Voice over IP

I. INTRODUCTION

Telephony over Internet Protocol (ToIP) is a public or private communications service that uses Internet Protocol (IP) to transmit voice (VoIP) and provide other telephony services (messaging, call transfer, voicemail, etc.). Despite their advantages, telephony networks face threats, including identity theft, denial-of-service attacks, eavesdropping on the network, data confidentiality breaches, and theft of communication information.

Manuscript received on 26 February 2023 | Revised Manuscript received on 05 March 2023 | Manuscript Accepted on 15 March 2023 | Manuscript published on 30 March 2023.
*Correspondence Author(s)
Sekoude Jehovah-Nis Pedrie SONON*, Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée, Université d'Abomey-Calavi (LETIA/UAC), Institut d'Innovation Technologique (IITECH SARL), BENIN, Email ID: jehovahnis@gmail.com, ORCID ID 0000-0003-2271-1631
Tahirou DJARA, Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée / Université d'Abomey-Calavi (LETIA/UAC), Institut d'Innovation Technologique (IITECH SARL), BENIN, Email ID: csm.djara@gmail.com
Abdou Wahidi BELLO, Université d'Abomey-Calavi (UAC), Institut d'Innovation Technologique (IITECH SARL), BENIN, Email ID: solfath@yahoo.fr
Matine OUSMANE, Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée / Université d'Abomey-Calavi (LETIA/UAC), Institut d'Innovation Technologique (IITECH SARL), BENIN, Email ID: amatine.ousmane@gmail.com

Blockchain-based solutions have been developed for digital identity. management, and there is a great deal of Each n + 1 block is hashed and research into the contribution this technology can make to securing IP cryptographically linked to the previous n block. telephony networks. But much remains to $B = E(Tx) + H(B) + H(B)$ (1) Be done in this area. With this in mind, we have proposed and designed a n+1 n+1 $H(B) = H(E(Tx)\, n\, n$+1 + $H(B))$ (2) Blockchain-based solution for enrollment and user connection.

n+1: the Bn+1n+1 n

Block is made up of the set E Communication session and post-communication phases.

A. ToIP Threats

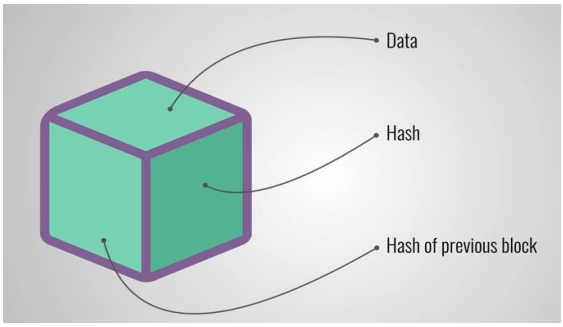
As mentioned by Sonon et al. (2023) [1], ToIP is subject to numerous threats. These include :

- identity theft
- identity modification
- denial of service
- network eavesdropping
- traffic detour
- theft of communication information
- etc.

These are just some of the threats to IP telephony networks. Securing these networks is therefore a significant challenge.

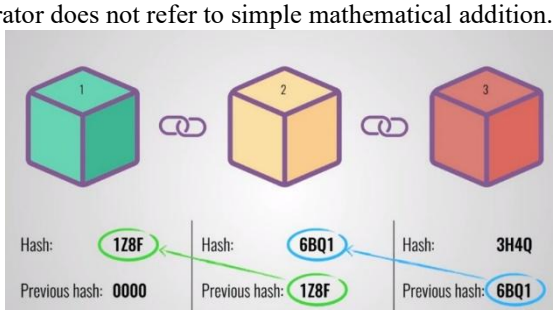
II. BLOCKCHAIN: DEFINITION AND CHARACTERISTICS

Blockchain, in its original definition, is an open-source technology for storing and transmitting data in a decentralised, distributed system. Blockchain means "chain of blocks". A block is a set of validated transactions recorded on the blockchain network.



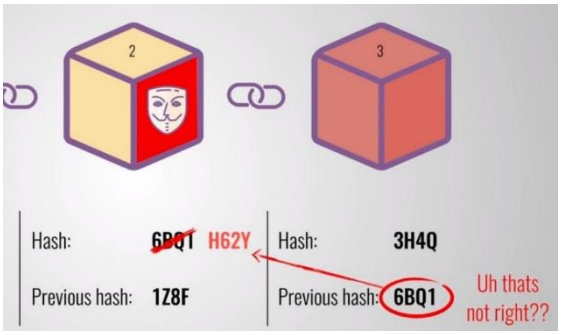
[Fig.1: Block Constitution [2]]

of Tx transactions, the hash of the previous block and the hash of the current (n+1) block.: the hash of block n + 1 $H(B)$ is n+1 formed from the transactions of this current block and the hash of the previous block. Note: The (+) operator does not refer to simple mathematical addition.



[Fig.2: Cryptographic Link Between Blocks [2]]

The cryptographic link between blocks ensures data integrity on the network. When a block of data is modified, its hash changes. Since this hash is linked to the next block, the hash of the following block changes, and so on. This domino effect reveals a modification of the data, indicating potential fraud on the network. All network participants then detect the scam, and its impact is cancelled.



[Fig.3: Fraud Detection on a Blockchain Network [2]]

In its generic form, blockchain has three significant properties, namely :

- **transparency:** all users can consult all exchanges recorded since the blockchain was created.
- **security:** this is achieved in two ways, firstly through the creation of new blocks, and secondly through replication across all network nodes.
- **disintermediation:** since blockchain is based on peer-to-peer relationships, the role of intermediaries is eliminated in favour of direct communications between a customer and a supplier.

III. KYC TECHNIQUES

KYC stands for Know Your Customer. It describes the process of verifying the identity of (new) customers. The KYC process is implemented to prevent illegal activities such as identity theft, money laundering or fraud. Identity verification as part of the KYC process may involve several steps, such as :

- document verification
- biometric verification
- address verification

Once a user has completed all the verification stages in a KYC process, their identity is verified, and they can access the desired services. In the event of failure, the request must be repeated; otherwise, the KYC will not be validated, and transactions will not be processed.

The introduction of artificial intelligence (AI) and video (KYC Liveness) speeds up the process of validating an individual's KYC, and also reinforces control over the validity of documents. Finally, an OTP (One-Time Password) can be sent via SMS or to the user's email address, enabling verification of their telephone number or email address. KYC originated in the banking sector and has since spread to other industries that require secure knowledge of the user wishing to access services.

IV. SOME EXISTING WORKS

Kara et al. in 2023 [3] worked on a decentralized identity authentication system for Voice over IP called VoIPChain.

The work of Alizadeh et al. in 2021 [4] focused on DHT and blockchain-based intelligent identification for videoconferencing.

Also with Kara et al. in 2021 [5], a study was carried out on blockchain-based mutual authentication for VoIP applications with biometric signatures.

Abubakar et al. in 2021 [6] worked on a blockchain-based authentication and registration mechanism for SIP-based VoIP systems.

Liu et al. in 2020 [7] conducted their studies on a blockchain-based scheme for authentic telephone identity.

In 2019, Ntantogian et al [8] proposed some solutions for protecting voice and communications against eavesdropping.

In 2023, SONON et al. [1] worked on the real impact of Blockchain in securing a ToIP network.

Analysis of these resources has revealed several shortcomings. Indeed, the blockchain technology used in this work is the Ethereum blockchain. Given that Ethereum is a grey area in terms of laws and regulations, particularly due to its public nature, concerns exist regarding data confidentiality. Ethereum also incurs gas charges for every transaction; therefore, every transaction is costly. Tests of some of the systems proposed by the researchers listed earlier have raised concerns about system slowness. Finally, issues such as identity theft, identity modification and communication data theft remain unresolved by the work mentioned above.

V. THE PROPOSED SOLUTION

To help secure ToIP networks, we intervene in the four functional phases of ToIP networks:

- user enrolment
- network connections
- the communication session
- post-communication

A. User Registration and Login

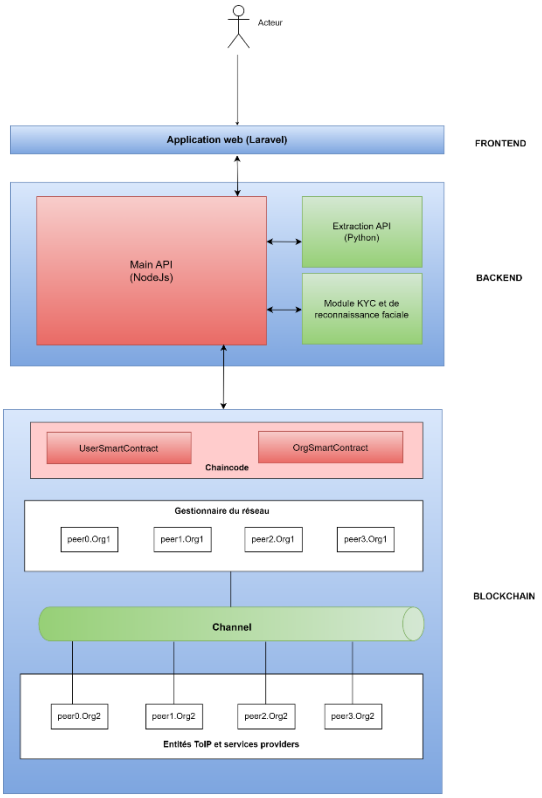
Ensuring the identity of users accessing a ToIP network is crucial. That's why we've implemented an identification and authentication system that includes KYC techniques for verifying user identity. Once identity has been validated, the user is authorized to use the network's communication services. User identities are stored not in a standard

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

database, but on a private blockchain network.

Frontend The frontend is an IT term used to designate all the graphical interfaces of a solution. Several languages and frameworks are used to design graphical interfaces. In this case, we used the Laravel framework [9] to create the solution's graphical interfaces.

Laravel implements the MVC model, which consists of separating views (the visible part of the platform) from the logic.



[Fig.4: Representation of the Solution Frontend]

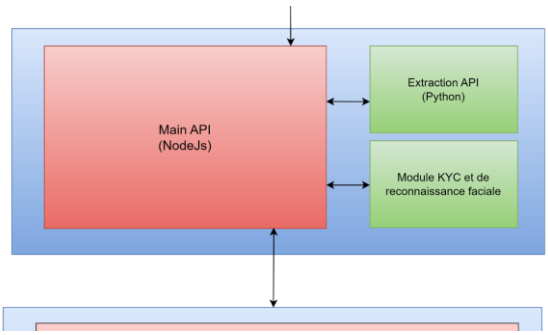
```
public function store(Request $request)
{
    //send qr code scanner email to user
    $data = $request->all();
    $additionnalData = [];
    $userExists = false;
    // ----- check if user already exists
    $user = Http::withHeaders([
        'username' => 'admin',
        'orgId' => 'org1',
        'email' => $data["email"],
    ])->get(config('app.blockchain_api_url') . '/users/check

    $userExists = $user["success"];
    if ($userExists) {
        return response([
            "success" => false,
            "message" => "L'utilisateur existe déjà"
        ], 200);
    }
    // -----
    try {
        $additionnalData = [
            "username" => $data["username"],
            "phone" => $data["phone"],
            "email" => $data["email"],
            "profession" => $data["profession"],
            "nationality" => $data["nationality"],
```

[Fig.5: Portion of a Laravel Code Integrating the NodeJs api for the Creation of a Digital Identity]

Fig. 4. System Architecture. The solution adopted follows the 3-tier architecture and is composed of :

- the frontend
- the backend
- the blockchain network

B. Backend :



[Fig.6: Representation of the Backend Solution]

The backend is the business part of the solution. It comprises :

- main API developed in NodeJS, enabling communication with the blockchain network.
- Flask API housing the KYC and facial recognition module,
- API for extracting identity attributes from the document provided.

Identity verification with our solution involves the user standing in front of our live image-taking module. Images of the user's face are captured, and the user is also asked to present their identity document, on which a photo of the user appears. These images are used for biometric and document verification purposes. The first step is to ensure that the facial images taken correspond to a single individual, and that this individual is indeed the one on the ID card presented. This entire process is automated using an artificial intelligence module developed based on the DeepFace library [10], yielding a performance rate of 75%. The face detection modules used are mainly Facenet512 and SFace. Manual verification may be used in cases where the module requires a human decision.

```
def makeVerification(self,img1,img2,img3) :
    for step in range(0,2) :
        if (step == 0) :
            self.results = []
        else :
            self.resultsForIdCard = []
            img2 = img3
        for i in range(0,4) :
            print('--- Test ',i, ' ---')
            if i <=2 :
                model = self.models[2] #facenet512
                metric = self.metrics[i] #cos,euclide
            else :
                model = self.models[8] #sface
                metric = self.metrics[1] #euclidean
            result = DeepFace.verify(img1_path = img1,
            if(step == 0) :
                self.results.append(result["verified"]
                print(self.results)
            else :
                self.resultsForIdCard.append(result["
                print(self.resultsForIdCard)
        print("---------------END TEST--------------")

    score = str(self.results.count(True) + self.result
    if(self.results.count(True) >= 3 and self.results
        print("User is verified with ",score)
        return ['True',score]
    else :
        print("User is not verified with ",score)
        return ['False',score]
```

Fig. 7. Code portion of the KYC module for identity verification with the DeepFace library. *The Blockchain Network:* The blockchain network houses user

Retrieval Number: 100.1/ijitee.C980813030224
DOI: 10.35940/ijitee.C9808.12040323
Journal Website: www.ijitee.org

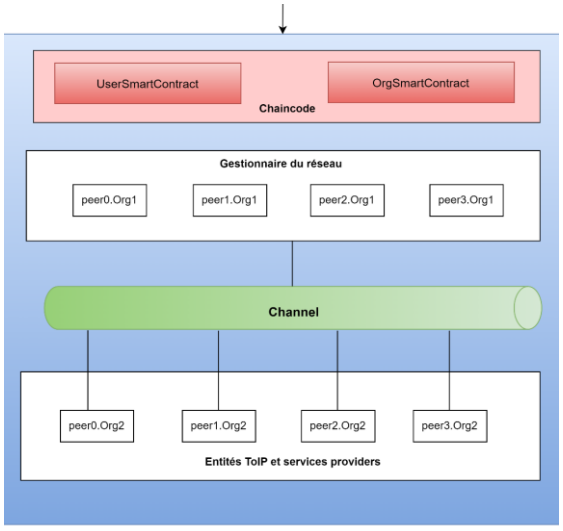
Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

identities. It has been developed using the Hyperledger Fabric framework. Existing research into securing telephony networks using blockchain employs the Ethereum blockchain. However, Hyperledger Fabric is better suited to this type of application. Table 1 compares the Ethereum and Fabric blockchains.

Table-I : Fabric vs Ethereum

	Ethereum	Hyperledge r Fabric
Type of blockchain	Public blockchain	Consortium/ private blockchain
Privacy	Transparent transactions	Confidential transactions
Goal	Suitable for	Suitable for
	Business to Customers (B2C) applications	Business to Business (B2B) applications
Cryptocurr ency	Ether or Ethereum	None
Smart contract programmi ng languages	Solidity	Golang, Javascript, Java
Consensus mechanism	Proof of Work	Flexible mechanism
Speed	Low	Fast

For its advantages in terms of data confidentiality, access rights management, absence of gas charges and transaction speed, we opted for a private blockchain based on the Hyperledger Fabric framework. Unlike a consortium blockchain, the data stored on a private blockchain is dependent on a single organisation, and only that organisation has the right to write to the data. Additionally, we don't require a consensus mechanism, as the entities participating in the network don't need to provide their approval before the transaction is validated.



[Fig.8. Representation of Blockchain Network Components]

In the proposed architecture, the blockchain network comprises smart contracts that constitute the chaincode. We distinguish between :

- OrgSmartContract: for managing service providers or telephony networks.
- UserSmartContract: for user management.

Data is stored on the channel, and all entities authorised to access the data are associated with it. Each entity in our architecture represents a peer. Every peer belongs to an organization (a term specific to Hyperledger Fabric). We declare org1 to be the network manager and peer1 as the other entity.org2 and peer2.org2 are under the auspices of Organisation 2 (org2). Access to data stored on the channel is possible through the smart contracts of the chaincode, which itself is the only communication interface between the network and the backend.

```
async getUserIdentity(ctx, userKey) {
    let oldUser = await ctx.stub.getState(userKey);
    oldUser = JSON.parse(oldUser);
    if (!oldUser || oldUser.length === 0) {
        return JSON.stringify({
            success: false,
            message: "User doesn't exist",
        });
    }
    let identity = oldUser.identity;
    return JSON.stringify({
        success: true,
        message: "Identity retrieved successfully",
        identity: identity,
    });
}
```

[Fig.9. Smart Contract Code for Identity Retrieval from the Blockchain Network]

C. The Hyperledger fabric framework

Hyperledger Fabric [11] is a flagship framework from the Hyperledger project. It is an open-source, permission-based solution launched in 2015. Unlike Ethereum, which only allows the creation of public blockchains, it enables the creation of both private and consortium blockchains. It is highly suitable for enterprises. solutions. The framework employs several hashing algorithms for encrypting data inserted on the network:

D. Elliptic curve cryptography (ECC)

This is a public-key cryptographic algorithm based on the mathematics of elliptic curves, providing a more efficient alternative to traditional public-key cryptographic algorithms such as RSA [11].

$$y = x + ax + b \quad (3)$$

- *Asymmetric cryptography:* This ensures the confidentiality of the message exchanged between two pairs. Otherwise, only the sender and receiver of the message must be able to read the data. Let's assume a message M, a sender E widely used SHA algorithm in Hyperledger Fabric, and generates a 256-bit message digest.

E. The communication session

When a user logs on for the first time, a public and private key pair is generated using the RSA-2048 algorithm. Messages exchanged during a communication session are encrypted using the users' public keys. RSA encryption is an asymmetric cryptographic algorithm used to exchange confidential data over the Internet [13]. If M is a natural number strictly less than n (product of 2 random primes), representing a message, then the encrypted message will be represented by :

$C=M^e \pmod n$ (8)

and a receiver R.

R

E

K

pu

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

E
K ,
pr
K et
pu
With RSA-2048, the integer n has a size of 2048. In February 2020, the 23rd smallest
K
pr
Are the public and private keys
RSA cypher (RSA-250) of the 54 numbers
of the sender and receiver. The sender encrypts the message M with a function C using the receiver's public key:
R
Listed was factorized. [14]. In addition to RSA encryption, we have implemented other end-to-end encryption mechanisms to secure the communication channel.
$V = C(K\,pu, \mathrm{M})$ (4)

F. Post-Communication

When the receiver receives the value V, it is the only one able to decrypt it thanks to a function D using its private key :
R
After each communication session, the call recording and call-related information are
$M = D\,(K\,pr, \mathrm{V})$ (5)
Saved on the blockchain and made To verify the authenticity of the message, the sender sends their signature, and only their public key can be used to decrypt the signature. available to the session participants.

VI.CONCLUSION AND PERSPECTIVES

$E\,S = C(K\,pr, \mathrm{M})$ (6)
We have proposed a blockchain-based solution that covers the phases of user The receiver decrypts S and obtains m. E enrolment, network connection, communication session and $m = D\,(K\,pu, \mathrm{S})$ (7) post-communication. To ensure that the If m = M, then the authenticity of the message is assured [12].

Secure Hash Algorithm (SHA): SHA is a family of cryptographic hash functions used to guarantee data integrity. SHA-256 is used to ensure

that users wishing to access the service are who he or she claim to be. We employ KYC techniques through document verification, biometric verification and the sending of OTPs. A facial recognition module reinforces security during the user login phase. The communication session is

Secured by end-to-end encryption, communication data, such as call duration, speaker names, and other information, is stored on the blockchain. User identities stored on the blockchain network are reliable, secure and reusable. Prospects for improvement in the proposed solution can be summarised as the introduction of an emotion detection module to ensure that users are logged in under the correct conditions, and the enhancement of the facial recognition and KYC module's performance.

The use of machine learning algorithms will also enable the real-time detection of security threats, particularly through the identification of attack patterns and suspicious behaviour. Finally, a detection mechanism for denial-of-service (DoS) and zero-day attacks will enable intelligent filtering of communication traffic, allowing for the blocking of these types of threats.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Sonon *et al.*, *Real Impact of the Blockchain in Securing a ToIP Network.* DOI: http://doi.org/10.4018/IJSPPC.324165,2023
2. "*How does a blockchain work*?" Simply Explained, visited on 28/01/2023, URL: https://www.youtube.com/watch?v=SSo%5C_EIwHSd4.
3. M. Kara, H. R. J. Merzeh, M. A. Aydın, and H. H. Balık, *VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain.* Comput. Commun., vol. 198, p. 247-261, Jan. 2023. http://dx.doi.org/10.1016/j.comcom.2022.11.019
4. Alizadeh et al, *DHT and blockchain-based smart identification for video conferencing.* 2021. https://doi.org/10.1016/j.bcra.2022.100066
5. Kara et al, *Blockchain-based mutual authentication for VoIP applications with biometric signatures.* 2021. http://dx.doi.org/10.1109/UBMK52708.2021.9558972
6. Abubakar et al, *Blockchain-based authentication and registration mechanism for SIP-based VoIP systems.* 2021. http://dx.doi.org/10.1109/CSNet52717.2021.9614646
7. Liu et al, *A blockchain-based scheme for an authentic phone identity.* 2020. http://dx.doi.org/10.3390/s23031264
8. Ntantogian et al, *Some solutions for voice and communication protection against eavesdropping.* 2019. http://dx.doi.org/10.1016/j.compeleceng.2019.05.008
9. https://laravel.com/
10. https://github.com/serengil/deepface
11. https://hyperledger-fabric.readthedocs.io
12. *How to represent a Blockchain through a mathematical model*. COPERNEEC, Available on : Blockchain-Copernеec.pdf (canopee-group.com), April 2020.
13. KERNOUF Yamina et al., *Simulation de quelques attaques sur le cryptosystème RSA.* 2020. https://dspace.ummto.dz/items/96e5528e-acfb-407e-ac5b-e37dc9c97c77
14. https://www.geeksforgeeks.org/rsa-algorith m-cryptography/

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

AUTHOR'S PROFILE

Sekoude Jehovah-nis Pedrie SONON is a PhD student at the University of Abomey-Calavi, Benin. His research interests include IP telephony and blockchain. Internet of Things, industrial applications and symbolic programming. He graduated with a Master's degree in Design Engineering from the Polytechnic School of Abomey-Calavi (EPAC) at the University of Abomey-Calavi in 2019. He is a consultant in the field of IP telephony, computer analysis, graphic design and web and mobile development.

Tahirou Djara is a Senior Lecturer at the Polytechnic School of Abomey-Calavi, located within the University of Abomey-Calavi, Benin. His research interests include: biometrics, signal and image processing, computational intelligence, industrial applications and symbolic programming. He received his PhD degree in signals and image processing from the University of Abomey-Calavi in 2013. He is a consultant in quality assurance in higher education and a consultant in the field of science and engineering technology.

Abdou Wahidi BELLO holds a PhD from the University of Abomey-Calavi, Benin. He is a consultant in the field of computer analysis, as well as a web and mobile developer.

Matine OUSMANE holds a PhD from the University of Abomey-Calavi, Benin. His research focuses on biometrics, signal processing and image analysis, computer intelligence, industrial applications, and symbolic programming. He graduated with a research master's degree from the Institute of Training and Research in Computer Science (IFRI) at the University of Abomey-Calavi in 2012. He is a consultant in the field of computer analysis, as well as a web and mobile developer.