Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2024, 11(1):238-247**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

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

Sekoude Jehovah-Nis Pedrie SONON[1]*, Tahirou DJARA[1], Abdou Wahidi BELLO[1], Matine OUSMANE[1]

*Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée / Université d'Abomey-Calavi (LETIA/UAC), Institut d'Innovation Technologique (IITECH SARL), BENIN
*Email: jsonon@iitech-benin.net, jehovahnis@gmail.com

Abstract In this article, we develop a solution for securing IP telephony networks. The solution developed is based on revolutionary blockchain technology and 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 smarts 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

1. 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, eavesdropping on the network, data confidentiality and theft of communication information. Blockchain-based solutions have been developed for digital identity management, and there is a great deal of research into the contribution this technology can make to securing IP telephony networks. But much remains to be done in this area. With this in mind, we have proposed and designed a blockchain-based solution for the enrollment, user connection, communication session and post-communication phases.

2. Materials and Methods

2.1. ToIP threats

As it is mentioned by Sonon *et al.* (2023) [1], ToIP is subject to many 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 major challenge.

2.2. Blockchain: definition and characteristics

Blockchain, in its original definition, is an open source technology for storing and transmitting data, in a decentralized, distributed system. Blockchain literally means "chain of blocks". A block (figure 1) is a set of validated transactions recorded on the blockchain network.

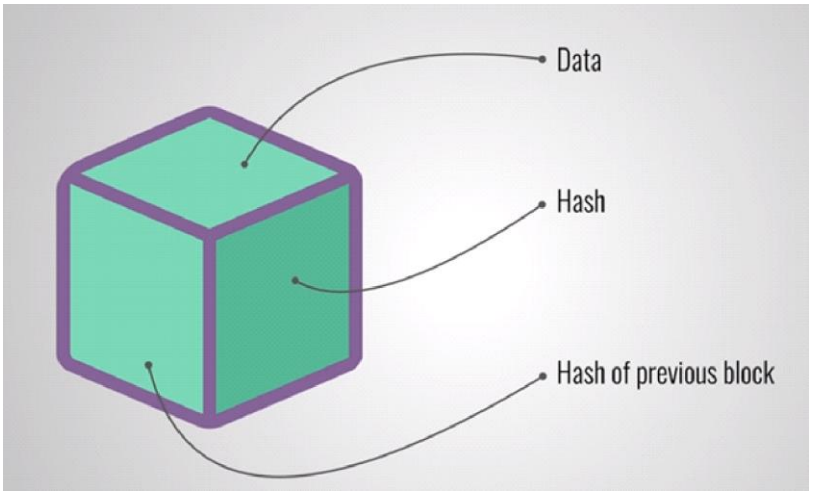


Figure 1: Block constitution [2]

Each $n+1$ block is hashed and cryptographically linked to the previous n block.

$$B_{n+1} = E(Tx)_{n+1} + H(B_n) + H(B_{n+1}) \quad (1)$$

$$H(B_{n+1}) = H(E(Tx)_{n+1} + H(B_n)) \quad (2)$$

(1) : the B_{n+1} block is made up of the set E of Tx transactions, the hash of the previous block and the hash of the current (n+1) block.

(2) : the hash of block $n+1$ $H(B_{n+1})$ is 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.

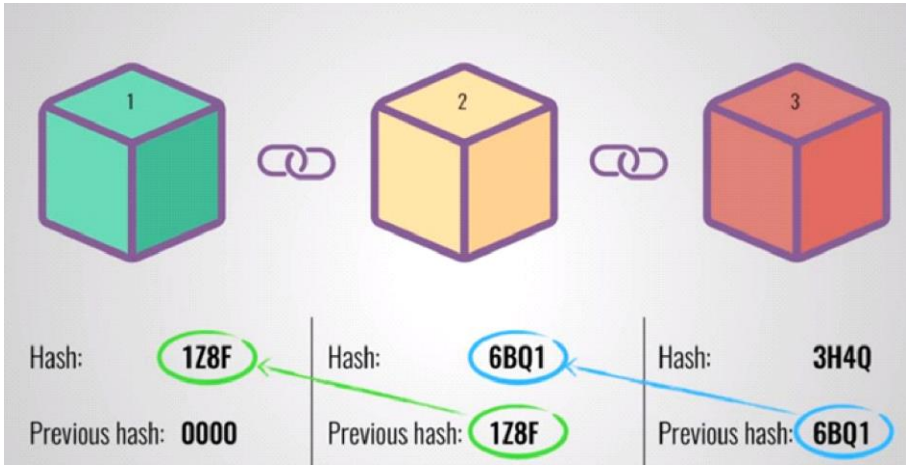


Figure 2: Cryptographic link between blocks [2]

The cryptographic link between blocks ensures data integrity on the network (figure 2). When a block of data is modified, its hash changes. Since this hash is linked to the next block, the hash of the next block changes, and so on (figure 3). This domino effect reveals a modification of the data, and therefore fraud on the network. The fraud is then detected by all network participants, and its effect is cancelled.

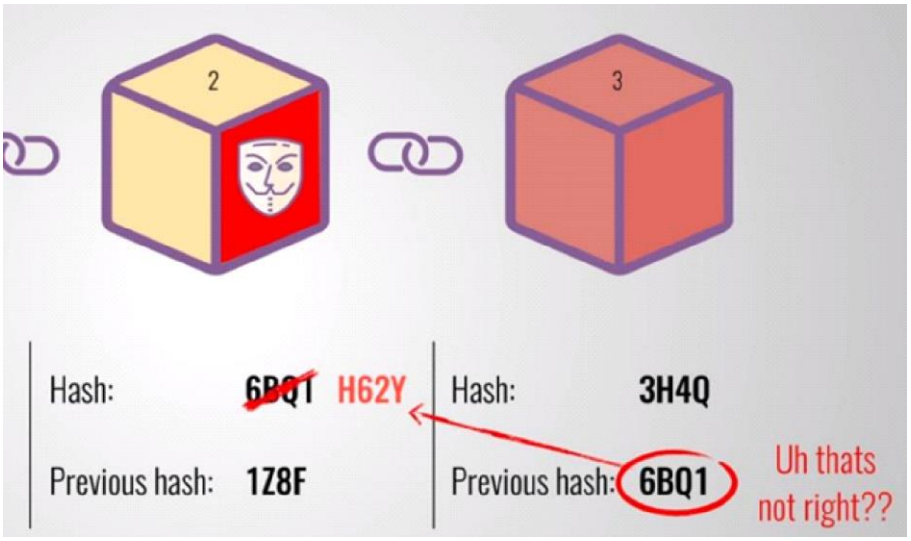


Figure 3: Fraud detection on a blockchain network [2]

In its generic form, blockchain has three major 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 favor of direct communications between a customer and a supplier.

2.3. 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 a number of steps, such as :

- document verification
- biometric verification
- address verification

Once a user has successfully passed all the verification stages in a KYC process, his or her identity is verified and he or she 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 carried out.

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, OTP (One Time Password) can be sent by SMS or to the user's email address, enabling verification of their telephone number or e-mail address. KYC originated in the banking sector, and has since spread to other sectors requiring secure knowledge of the user wishing to access services.

2.4. 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 a number of shortcomings. Indeed, the blockchain technology used in this work is the Ethereum blockchain. Given that Ethereum is a gray area in terms of laws and regulations, not least because of its public nature, there is a problem of data confidentiality. Ethereum also incurs gas charges for every transaction: every transaction is therefore costly. Tests of some of the systems proposed by the researchers listed earlier have raised the issue of system slowness. Finally, issues such as identity theft, identity modification and communication data theft remain unresolved by the above-mentioned work.

3. Results

The proposed solution

To help secure ToIP networks, we intervene in the 4 functional phases of ToIP networks:

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

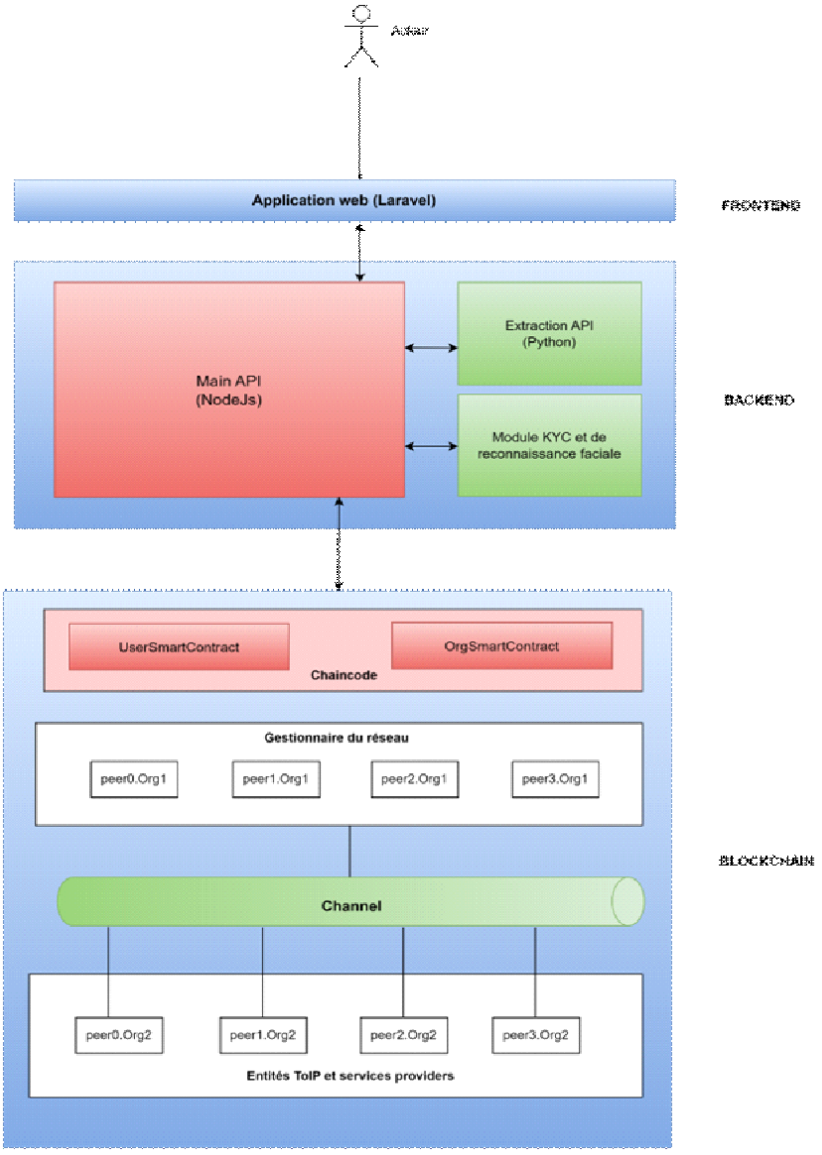


Figure. 4. System Architecture

3.1 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 (figure 4). Once identity has been validated, the user is authorized to use the network's communication services. User identities are stored not in a standard database, but on a private blockchain network.

The solution adopted follows the 3-tier architecture and is composed of :

- the frontend
- the backend
- the blockchain network

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

Laravel implements the MVC model, which consists in separating views (the visible part of the platform) from the logic (figure 5).

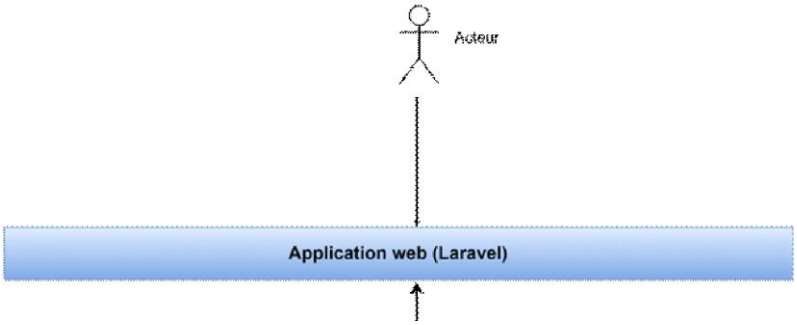


Figure 5: Representation of the solution frontend

```php
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"],
```

Figure 6: Portion of a laravel code integrating the NodeJs api for the creation of a digital identity

Figure 6 presents a portion of a laravel code integrating the NodeJs api for the creation of a digital identity

b) Backend :

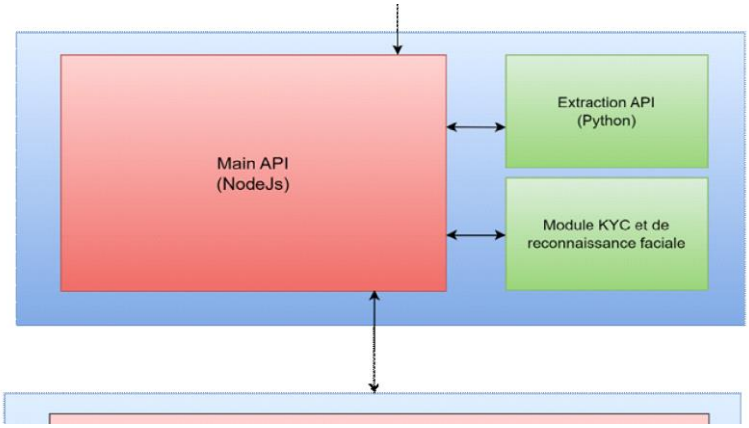


Figure 7: Representation of the backend solution

The backend is the business part of the solution. It comprises as shown in figure 7 :

- 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. Image captures of the user's face are taken, and the user is also asked to present his or her identity document, on which a photo of the user appears. All these images are used for biometric and document verification. 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 and based on the DeepFace library [10], giving us 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. Figure 8 presents a portion of code of the KYC module for identity verification with the DeepFace library.

```
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.resultsF
        print("User is verified with ",score)
        return ['True',score]
    else :
        print("User is not verified with ",score)
        return ['False',score]
```

Figure 8: Code portion of the KYC module for identity verification with the DeepFace library

c) The Blockchain Network: The blockchain network houses user 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 1: Fabric vs Ethereum

Type of blockchain	Public blockchain	Consortium/private blockchain
Privacy	Transparent transactions	Confidential transactions
Goal	Suitable for Business to Customers (B2C) applications	Suitable for Business to Business (B2B) applications
Cryptocurrency	Ether or Ethereum	None
Smart contract programming 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 an organization, and only the latter has the right to write to the data. Also, we don't need a consensus mechanism, since the entities participating in the network don't need to give their approvals before the transaction is validated.

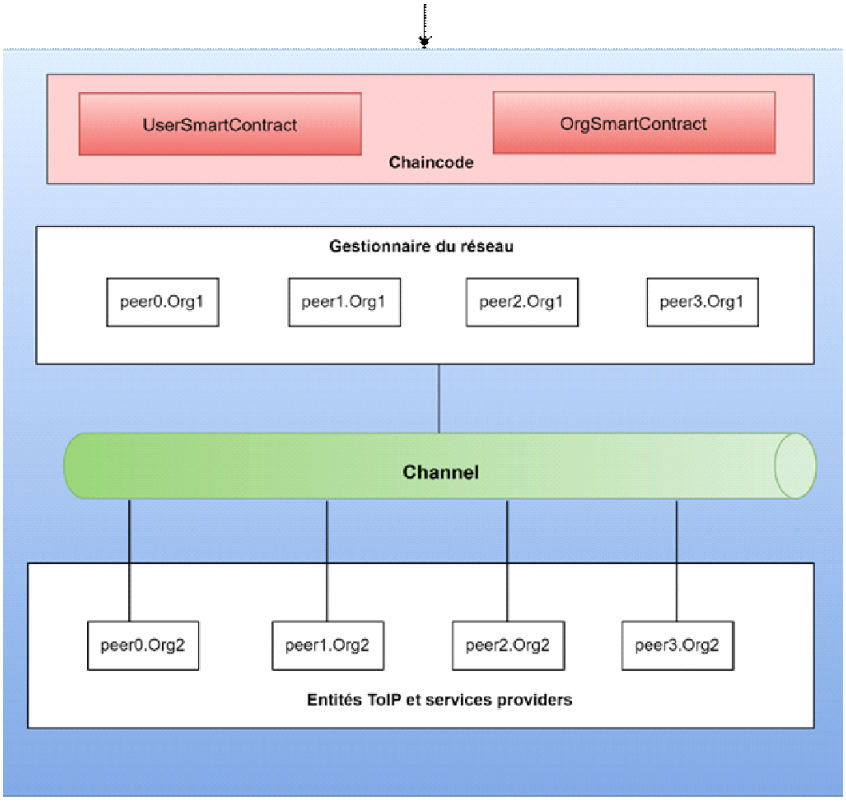


Figure 9: Representation of blockchain network components

In the proposed architecture (figure 9), the blockchain network is made up of smart contracts, constituting the chaincode, which code for identity retrieval from the blockchain network is presented in figure 10. We distinguish between

OrgSmartContract: for managing service providers or telephony networks,

UserSmartContract: for user management.

Data is stored on the channel, and all entities authorized to access the data are linked to 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 the other entities peer1.org2, peer2.org2 are under the aegis of

organization 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,
    });
}
```

Figure 10: Smart contract code for identity retrieval from the blockchain network

3.2 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. It enables the creation of both private and consortium blockchains, unlike Ethereum, which only allows the creation of public blockchains. It is highly suitable for enterprise solutions. The framework employs several hashing algorithms for encrypting data inserted on the network

- 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].

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

- 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 and a receiver R. K_{pu}^{E}, K_{pr}^{E}, K_{pu}^{R} et K_{pr}^{R} are the public and private keys of the sender and receiver. The sender encrypts the message M with a function C using the receiver's public key:

$$V = C(K_{pu}^{R}, \mathrm{M}) \quad (4)$$

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:

$$M = D(K_{pr}^{R}, \mathrm{V}) \quad (5)$$

To verify the authenticity of the message, the sender sends his S signature, and only his public key can be used to decrypt the signature.

$$S = C(K_{pr}^{E}, \mathrm{M}) \quad (6)$$

The receiver decrypts S and obtains m.

$$m = D(K_{pu}^{E}, \mathrm{S}) \quad (7)$$

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 the most widely used SHA algorithm in Hyperledger Fabric, and generates a 256-bit message digest

3.3. 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

$$C=M^e \ (mod\ n) \qquad (8)$$

With RSA-2048, the integer n has a size of 2048. In February 2020, the 23rd smallest RSA cipher (RSA-250) of the 54 numbers listed was factorized. [14]. In addition to RSA encryption, we have implemented other end-to-end encryption mechanisms to secure the communication channel.

3.4. Post-communication

After each communication session, the call recording and call-related information are saved on the blockchain and made available to the session participants.

4. Conclusion and Perspectives

We have proposed a blockchain-based solution that covers the phases of user enrolment, network connection, communication session and post-communication. To ensure that the user wishing to access the service is who he or she claims 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, and communication data such as call duration, speaker names and other data are 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 summed up as the introduction of an emotion detection module to ensure that users are logged in under the right conditions, and the enhancement of the performance of the facial recognition and KYC module.

The use of machine learning algorithms will also enable real-time detection of security threats, notably through the detection of attack patterns and suspicious behavior. Finally, a detection mechanism for denial-of-service (DDoS) and zero-day attacks will enable intelligent filtering of communication traffic, in order to block these types of threats.

Acknowledgment

This research would like to thank Tahirou DJARA, for his contributions to this work and his guidance of our research thesis.

References

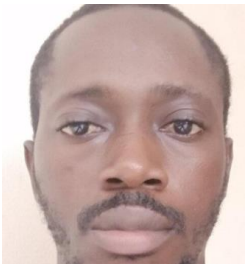
[1]. Sonon et al., Real Impact of the Blockchain in Securing a ToIP Network. DOI: 10.4018/IJSPPC.324165, 2023.
[2]. "How does a blockchain work", Simply Explained, visited on 28/01/2023, URL : https://www.youtube.com/watch?v=SSo%5C_EIwHSd4.
[3]. M. Kara, H. R. J. Merzeh, M. A. Aydın, and H. H. Balık, VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain. Comput. Commun., vol. 198, p. 247-261, jan. 2023.
[4]. Alizadeh et al, DHT and blockchain-based smart identification for video conferencing. 2021.
[5]. Kara et al, Blockchain-based mutual authentication for VoIP applications with biometric signatures. 2021.
[6]. Abubakar et al, Blockchain-based authentication and registration mechanism for SIP-based VoIP systems. 2021.
[7]. Liu et al, A blockchain-based scheme for an authentic phone identity. 2020.
[8]. Ntantogian et al, Some solutions for voice and communication protection against eavesdropping. 2019.
[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-Coperneec.pdf (canopee-group.com), April 2020.
[13]. KERNOUF Yamina et al., Simulation de quelques attaques sur le cryptosystème RSA. 2020.
[14]. https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

Sekoude Jehovah-nis Pedrie SONON is a PhD student at the University of Abomey-Calavi, Benin. His research interests include IP telephony, blockchain, Internet of Things, industrial applications and symbolic programming. He graduated as a design engineer, Master degree, from the Polytechnic School of Abomey Calavi (EPAC) of 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 in the University of Abomey-Calavi, Bénin. His research interests include: biometrics, signal and image processing, computational intelligence, industrial applications and symbolical programming. He received the 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 consultant in the field of science and engineering technology.

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



Matine OUSMANE holds PhD from the University of Abomey-Calavi, Benin. His research focuses on: biometrics, signal processing and images, computer intelligence, industrial applications and symbolic programming. He graduated with a research master 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, web and mobile developer.

Authors: