الجمهورية الجزائرية الديمقراطية الشعبية
République algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة عين تموشنت
Université de Belhadj Bouchaib d'Ain-Temouchent
Faculté des Sciences et de la Technologie
Département d'Electronique et des Télécommunications

Projet de fin d'études

Pour l'obtention du diplôme de Master en :

Domaine : SCIENCE ET TECHNOLOGIE

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Thème

Réalisation d'un système d'authentification à double facteur biométrique

Présenté Par :

Melle. BERKANE ASMAA IKRAM

Mr. CHINYUKU MALVERN

Devant le jury composé de :

Dr. Sekkal Mansouria	**MCA**	**UBBAT**	**Président**
Dr. Meradi Abdelhafid	**MCB**	**UBBAT**	**Examinateur**
Dr. Yagoub Reda	**MCB**	**UBBAT**	**Encadrant**

Année universitaire 2022/2023

Remerciements

Nous louons Allah, tout-puissant, de nous avoir donnée la volonté, l'aide, le courage, la santé et la patience pour finaliser ce travail.

Nous remercions particulièrement notre encadreur ***Mr. YAGOUB Réda****, pour son encadrement de grande qualité scientifique, sa disponibilité, ses conseils et pour la confiance qu'il nous a accordée tout au long du projet.*

Nos sincères remerciements à nos familles pour leurs soutiens et pour leurs sacrifices tout au long de nos carrières d'études.

Nos vifs remerciements aux membres de jurys ***Mme. Sekkal Mansouria et Mr. Meradi Abdelhafid*** *de bien vouloir accepter d'évaluer notre travail.*

Nous ne pouvons pas terminer sans penser à tous ceux qui nous ont aidés, soutenu et encouragé tout au long de la réalisation de ce mémoire surtout nos enseignants du département de génie électrique qui ont participé à notre formation ainsi que le personnel administratif.

Dédicace

Je rends grâce à dieu de m'avoir donné le courage et la volonté. Ainsi que la conscience d'avoir pu terminer mes études.

Je dédie ce travail à :

A ceux qui me sont chers

A ceux qui ont toujours cru en moi

A ceux qui m'ont toujours encouragé

Mes chères parents ***ma mère*** *et* ***mon père*** *pour leur amour, leur soutien et leurs encouragements*

A ma raison de vivre à la prunelle de mes yeux ***maman chérie***

Aucune dédicace ne sauvait être assez éloquente pour exprimer

ce qu'elle mérite pour tous les sacrifices qu'elle m'a cessé de me donner

Depuis ma naissance, durant mon enfance et même à l'âge adulte.

Merci d'être l'épaule sur lequel que je peux toujours compter.

À mes chères tentes merci pour vos encouragements

À toutes mes chères amies et collègues

et à notre encadreur : ***Mr. Yagoub Reda*** *pour son aide et son soutient tout au long de notre mémoire fin d'étude*

À toute la famille ***BERKANE*** *et la famille* ***DOUKALI***

Finalement, à mon binôme ***Malvern*** *et sa famille*

Ikram

Dédicace

Je rends grâce à dieu de m'avoir donné le courage et la volonté. Ainsi que la conscience d'avoir pu terminer mes études.

Je voudrais dédier ce travail à ma mère,

A mon père et mes petits frères, les personnes qui comptent le plus pour moi,

Je la dédie à mes chers amis,

A mon binôme qui a tout donné pour la réalisation de ce projet.

Malvern

Abstract

The proliferation of internet services on the web has meant that almost anything can be done online nowadays. From internet banking, e-commerce, online examinations and even logging onto sensitive databases, high security measures to protect access to these services are paramount. Perhaps the most common method to secure online accounts is the use of passwords, a single factor authentication mechanism. Passwords are however not secure as they are prone to brute force attacks, dictionary attacks, social engineering attacks, phishing and keylogger attacks.

Dual-factor authentication mechanisms have emerged to enhance the security level of web applications. In addition to passwords, OTPs (one-time passwords) have been added as a second layer of authentication. These codes are sent from the OTP server to the user's phone via SMS (short message service). The user then enters the OTP on their web application account to verify the authentication process. However, due to the weaknesses of the SS7 (signaling system 7) protocol, SMS messages can be redirected by hackers therefore exposing the authentication code.

In this thesis, we propose a dual-factor authentication scheme that uses a biometric identifier as the second authentication factor. Biometric recognition offers a natural solution that is immune to the weaknesses of using OTPs and passwords.

Keywords: authentication, web security, two-factor authentication, biometric recognition, biometric system, biometric Identifier, fingerprint recognition, facial recognition, matching.

Résumé

La prolifération des services Internet sur le web signifie que presque tout peut être fait en ligne de nos jours. Qu'il s'agisse de services bancaires en ligne, de E-commerce, d'examens en ligne ou même de l'accès à des bases de données sensibles, il est primordial de mettre en place des mesures de sécurité élevées pour protéger l'accès à ces services. La méthode la plus courante pour sécuriser les comptes en ligne est sans doute l'utilisation de mots de passe, un mécanisme d'authentification à facteur unique. Les mots de passe ne sont toutefois pas sûrs car ils sont sujets à des attaques par force brute, par dictionnaire, par ingénierie sociale, les attaques de type keylogger et par les attaques de type phishing.

Des mécanismes d'authentification à double facteur sont apparus pour améliorer le niveau de sécurité des applications web. Outre les mots de passe, les OTP (mots de passe à usage unique) ont été ajoutés comme deuxième couche d'authentification. Ces codes sont envoyés par le serveur OTP au téléphone de l'utilisateur par SMS (short message service). L'utilisateur saisit ensuite l'OTP sur son compte d'application web pour vérifier le processus d'authentification. Cependant, en raison des faiblesses du protocole SS7 (système de signalisation 7), les messages SMS peuvent être redirigés par des pirates informatiques, exposant ainsi le code d'authentification.

Dans cette thèse, nous proposons un schéma d'authentification à double facteur qui utilise un identifiant biométrique comme deuxième facteur d'authentification. La reconnaissance biométrique offre une solution naturelle qui est immunisée contre les faiblesses de l'utilisation des OTP et des mots de passe.

Mots-clés : authentification, sécurité web, authentification à deux facteurs, reconnaissance biométrique, système biométrique, identificateur biométrique, reconnaissance d'empreintes digitales, reconnaissance faciale, la mise en correspondance.

ملخص

يعني انتشار خدمات الإنترنت على الويب أنه يمكن القيام بأي شيء تقريبا عبر الإنترنت في الوقت الحاضر. من الخدمات المصرفية عبر الإنترنت والتجارة الإلكترونية والامتحانات عبر الإنترنت وحتى تسجيل الدخول إلى قواعد البيانات الحساسة ، تعتبر التدابير الأمنية المشددة لحماية الوصول إلى هذه الخدمات ذات أهمية قصوى. ربما تكون الطريقة الأكثر شيوعا لتأمين الحسابات عبر الإنترنت هي استخدام كلمات المرور ، وهي آلية مصادقة أحادية العامل. ومع ذلك ، فإن كلمات المرور ليست آمنة لأنها عرضة لهجمات القوة الغاشمة وهجمات القاموس وهجمات الهندسة الاجتماعية والتصيد الاحتيالي وهجمات keylogger.

ظهرت آليات المصادقة الثنائية لتعزيز مستوى أمان تطبيقات الويب. بالإضافة إلى كلمات المرور ، تمت إضافة OTPs (كلمات المرور لمرة واحدة) كطبقة ثانية من المصادقة. يتم إرسال هذه الرموز من خادم OTP إلى هاتف المستخدم عبر الرسائل القصيرة (خدمة الرسائل القصيرة). ثم يقوم المستخدم بإدخال كلمة المرور لمرة واحدة على حساب تطبيق الويب الخاص به للتحقق من عملية المصادقة. ومع ذلك ، نظرا لنقاط الضعف في بروتوكول SS7 (نظام الإشارات 7) ، يمكن إعادة توجيه رسائل SMS من قبل المتسللين وبالتالي كشف رمز المصادقة.

في هذه الأطروحة ، نقترح نظام مصادقة ثنائي العامل يستخدم معرفا بيومتري كعامل مصادقة ثان. يوفر التعرف البيومتري حلا طبيعيا محصنا ضد نقاط الضعف في استخدام OTP (كلمة مرور لمرة واحدة) وكلمات المرور.

الكلمات المفتاحية: المصادقة ، أمان الويب ، المصادقة الثنائية ، التعرف على المقاييس الحيوية ، النظام البيومتري ، المعرف البيومتري ، التعرف على بصمات الأصابع ، التعرف على الوجه ، المطابقة.

Sommaire

Liste des Figures

Liste Des Tableaux

Liste des Abréviations

ARPA: Advanced Research Projects Agency

ARPANET: Advanced Research Projects Agency Network

IP : Internet Protocol

IPv4 : Internet Protocol version 4

IPv6 : Internet Protocol version 6

BBN: Bolt, Beranek and Newman

DoD: Department of Defense

MIT: Massachusetts Institute of Technology

ARPA IPT: Advanced Research Projects Agency Network Information Processing Techniques

IMP: Interface Message Protocol

UCLA: University of California, Los Angeles

NWG: Network Working Group

NCP: Network Control Protocol

DNS: Domain Name System

NFSNET: National Science Foundation Network

ISP: Internet Service Provider

IEEE: Institute of Electrical and Electronics Engineers

URL: Uniform Resource Locator/Universal Resource Locator

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

HTML: Hypertext Markup Language

XHTML: Extensible Hypertext Markup Language

XML: Extensible Markup Language

WYSWYG: What You See is What You Get

FTP: File Transfer Protocol

ARP: Address Resolution Protocol

ICMP: Internet Control Message Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

ASCII: American Standard Code for Information Interchange

SSH: Secure Shell

E-mail : Electronic mail

E-commerce : Electronic commerce

CERN : Conseil Européen pour la Recherche Nucléaire

W3C : World Wide Web Consortium

INRIA : Institut National de Recherche en Informatique et Automatique

P2P: peer to peer

SFA: Single Factor Authentication

2FA: Two Factor Authentication/Dual-Factor Authentication

3FA: Three factor Authentication

MFA: Multi-Factor Authentication

PIN: Personal Identification Number

OOB: Out-Of-Band

USB: Universal Serial Bus

OTP: One-Time Password

TAN: Transaction Authentication Number

FIDO: Fast IDentity Online

GPS: Global Positioning System

SMS: Short Message Service

mTAN: Mobile Transaction Authentication Number

SMS TAN: Short Message Service Transaction Authentication Number

NIST: National Institute of Standards and Technology

MOOC: Massive Open Online Course

FAR: False Acceptance Rate

FRR: False Reject Rate

FERET: Facial Recognition Technology

FBI: Federal Bureau of Investigation

CODIS: Combined DNA Index System

ADN: Acide désoxyribonucléique

ISO: International Organisation for Standardisation

ABIS: Automated Biometric Identification System

FM: False Match

FNM: False Non-Match

FTA: Failure-To-Acquire

FTE: Failure-To-Enroll

JSX: JavaScript Extensible Markup Language

NPM: Node Package Manager

JSON: JavaScript Object Notation

CLI: Command Line Interface

VS code: Visual Studio code

SS7: Signaling System 7

Introduction générale

De nos jours, avec la prolifération des services accessibles via l'internet, notre interaction avec plusieurs sites web est inévitable. Qu'il s'agisse de services bancaires en ligne, de E-commerce, d'éducation en ligne, d'accès à des comptes de médias sociaux ou de bien d'autres services internet, un mécanisme d'authentification est primordial pour sécuriser ces comptes. Le mécanisme de sécurité le plus répandu parmi les utilisateurs d'internet est la combinaison d'un nom d'utilisateur et d'un mot de passe. Les mots de passe sont pratiques pour l'utilisateur et constituent le mécanisme d'authentification le plus acceptable puisqu'ils existent depuis des décennies. Il existe une confiance générale et une familiarité avec l'utilisation des mots de passe, mais ils ne constituent plus une méthode d'authentification sûre.

L'utilisation de mots de passe présente de nombreuses vulnérabilités. Tout d'abord, ils sont faciles à oublier, c'est pourquoi de nombreux utilisateurs les recyclent sur différents sites web. Si un pirate parvient à deviner ou à intercepter un mot de passe, il aura ensuite accès à vos autres comptes. Les mauvaises pratiques en matière de mots de passe, comme les mots de passe courts et à faible entropie, ont rendu les utilisateurs vulnérables aux attaques par force brute et aux attaques par dictionnaire. En outre, l'authentification par mot de passe est sujette à des attaques de phishing et d'ingénierie sociale. Dans le passé, nous avons entendu parler de fuites de bases de données de mots de passe où des pirates ont exposé des bases de données entières de mots de passe d'une entreprise.

Les systèmes d'authentification sont conçus sur la base de trois critères principaux appelés facteurs d'authentification. Il s'agit de ce que l'on sait, de ce que l'on a et de ce que l'on est. L'utilisation des mots de passe est classée dans la catégorie « quelque chose que vous connaissez ».

Dans notre projet de fin d’étude, nous ajoutons un deuxième facteur à l'utilisation des mots de passe, à savoir « ce que vous êtes ». En plus d'un mot de passe, l'utilisateur doit présenter une empreinte digitale ou un balayage du visage pour compléter le processus de connexion. Cela ajoute deux exigences au processus de sécurité, ce qui le rend encore plus sûr.

Notre mémoire de fin d’études est divisé en trois chapitres.

Le chapitre 1 présente un bref historique de l'internet et du World Wide Web.

Le chapitre 2 traite des différents mécanismes d'authentification existants, des différents identifiants biométriques utilisés dans l'authentification biométrique et des différents éléments d'un système d'authentification biométrique.

Le chapitre 3 présente notre solution d'authentification biométrique à deux facteurs.

CHAPITRE 1

Généralités sur le Web

1.1 Introduction

Depuis des siècles, les êtres humains ont toujours l'envie de se communiquer. Les premiers modes de communication c'était d'envoyer des lettres en utilisant des pigeons, les signaux de la fumée et d'ailleurs un messager à cheval qui délivrait le message de l'émetteur au récepteur. Après cette époque le domaine de réseaux et télécommunications a subi beaucoup des évolutions, parmi eux c'est l'internet qui est l'une des inventions les plus importants qui a affecté notre vie.

Aujourd'hui l'internet a franchi toutes les barrières et a changé la façon dont nous parlons, de travailler, de faire des achats et même de payer les factures. Elle a facilité notre vie de vrai en la rendant plus confortable. L'époque où nous devions faire la queue pour payer nos factures de téléphone ou bien d'électricité, maintenant nous pouvons les payer en cliquant sur un bouton depuis notre maison. Cette technologie a atteint un tel niveau que nous n'avons même pas besoin d'un ordinateur, nous avons des Smartphones qui permet d'accéder facilement.

Grâce à l'internet nous pouvons rester connectés à nos amis et à notre famille. Aujourd'hui, Internet a permis non seulement de parler mais aussi d'utiliser la vidéoconférence en utilisant des applications populaires comme Skype, Viber etc. A un prix très bas, à tel point qu'une heure de chat vidéo en utilisant internet est moins chère que le coût d'envoi d'une lettre. Dans nos jours l'internet est devenu très indispensable à un point tel que maintenant nous ne pouvons pas penser à notre vie sans lui.

1.2 Définition de l'internet

L'internet est un ensemble des réseaux autonomes reliés entre eux. On s'y comprend un inter-network (entre réseaux).

D'après Larousse l'internet est un « réseau télématique international, issu militaire américain Arpanet (conçu en 1969) et résultant de l'interconnexion d'ordinateur du monde entier utilisant un protocole commun d'échanges de données (IP pour Internet Protocol). [Abréviation : Net.]. Tout utilisateur d'un micro-ordinateur muni d'un modem peut se connecter à internet via un fournisseur d'accès pour la consultation d'information [sites web], la messagerie électronique, des forums, des blogs, le commerce électronique et les réseaux sociaux, etc.] »

1.3 Historique

L'idée de faire un réseau des architectures interconnectées mondiale est prévue dans les pensées de Monsieur J.C. R Licklider (Lukasik, 2011).Il était un psychologue travaillant sur les facteurs des humains dans la deuxième guerre mondiale, il a participé au projet Charles (système de défense aérienne) et il était chercheur à la société BBN avant d'arriver à ARPA.

1.3.1 ARPA

Le projet ARPA était lancé le 07 février 1958 par le DoD, une branche militaire américaine qui emploie la technologie des ordinateurs dans la défonce de leur pays (Lukasik, 2011). ARPA avait plusieurs domaines de recherche dont les réseaux informatiques contrôle et commandes était parmi eux.

Licklider se retrouve à ARPA en 1962 avec sa vision de « réseau galactique ». Il travaille avec Ivan Sutherland, Bob Taylor et un chercheur de MIT L.G. Roberts pour leur expliquer son idée de relier plusieurs ordinateurs entre eux. Son bureau était renommé de command and control à ARPA IPT. L'ARPA commence à se focaliser trop dans le domaine des réseaux (Barry M. Leiner, 1997).

1.3.2 La théorie de la commutation des paquets

Le travail de Kleinrock sur la théorie de la communication des paquets en 1961 (Barry M. Leiner, 1997) est devenu très important dans l'évolution de l'internet. Il rêvait remplacer la commutation par circuits par un système beaucoup plus efficace offrant un partage des lignes de transmission entre les utilisateurs. L'inconvénient de la commutation par circuit c'était le faible débit offert, et les lignes dédiée pour chaque transmetteur ce qui rend la technologie trop chère.

En effet c'est monsieur L.G. Roberts qui a fait la planification et implémentation d'ARPANET (Goldberg, 1988). Donald Davies définit le mot paquet. Au cours de son travail, L.G. Roberts accède au travail de Paul Baran sur les réseaux distribués qui allait faciliter la construction des réseaux militaires pouvant être capable de survivre des attaques de bombardement (Baran, 1964). Aujourd'hui l'internet est basé sur la technologie de la commutations des paquets.

1.3.3 Le premier réseau 1966

L.G. Roberts a mis deux réseaux informatiques entre l'ordinateur TX-2 du Lincoln Laboratory et l'ordinateur Q-32 de la System Development Corporation en utilisant un canal téléphonique de 1200 bps (haute vitesse à l'époque) (Goldberg, 1988).

Chaque ordinateur fonctionnait en mode partage de temps et permettait à n'importe quel logiciel de composer le numéro de l'autre ordinateur, de se connecter (log in) et d'exécuter les programmes (Goldberg, 1988). L'expérience a montré que qu'il n'y avait aucun problème pour que les ordinateurs se parlent entre eux et à utiliser les ressources de l'autre ordinateur. Les systèmes d'exploitation en temps partagé rendaient cela facile.

Le vrai problème découvert était que les communications téléphoniques basées sur le réseau téléphonique étaient trop lentes et peu fiables pour être utiles sur le plan opérationnel.

1.3.4 Lancement du ARPANET

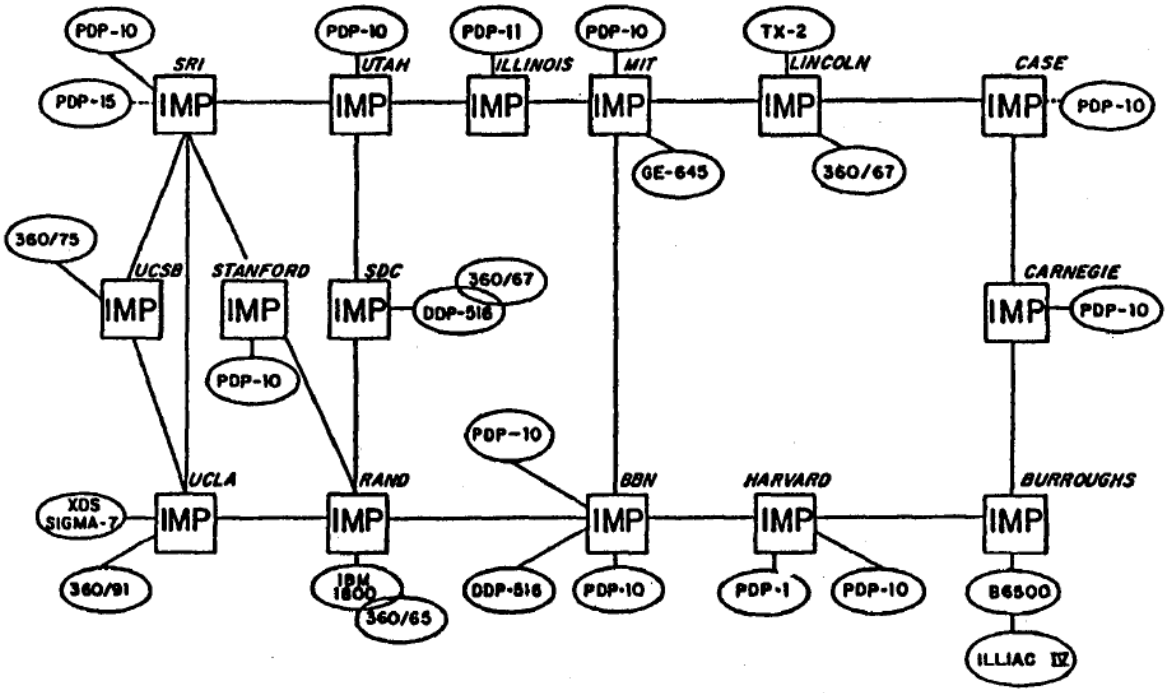

Figure 1 : Le réseau d'ARPANET en 1971 (Goldberg, 1988, p. 151)

Le projet ARPANET était finalement lancé en Octobre 1967 par L.G. Roberts. La société de BBN et Robert Khan ont développés les commutateurs IMP pour ARPANET (F. E. Heart, May 5-7,1970), voire la figure 2.

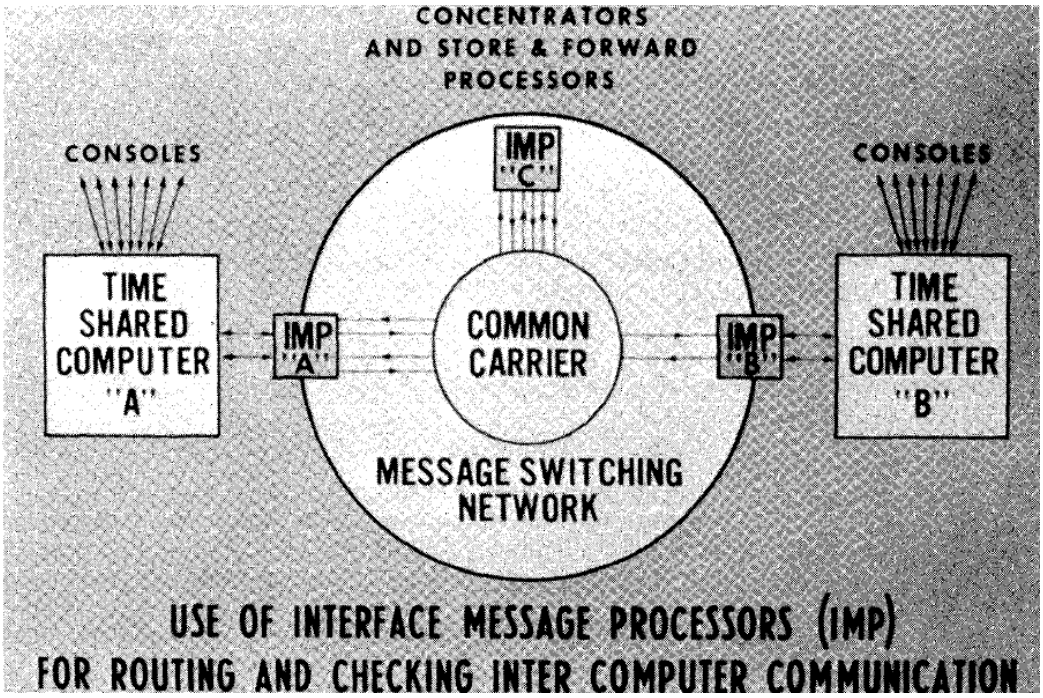

Figure 2 : Les premières communications employant des IMPs à chaque nœud du réseau (Goldberg, 1988, p. 146)

La société Network Analysis Corp a travaillé avec L.G. Roberts pour optimiser le réseau ARPANET et la topologie. Le premier nœud ARPANET se fut installé dans le bureau de Kleinrock à UCLA en 1969. L'année suivante Steve Crockes et NWG finissent le protocole NCP pour la communication host-to-host. Pendant les années 1971 à 1972, L.G. Roberts s'occupe avec l'implémentation de NCP sur le réseau ARPANET (Barry M. Leiner, 1997, p. 103).

1.3.5 Services et évolution d'ARPANET

L'année 1972 a apporté l'invention d'email par Ray Tomlison de BBN. Email deviens le plus utilisé service d'ARPANET. En 1974 Cerf et Khan ont publié un article sur le programme internet TCP/IP (Kahn, May 1974), cela a approché plusieurs avantages que NCP. La suite TCP/IP gagne de popularité. Cela pousse les développements des terminaux (Workstations), les ordinateurs personnels conformément aux standards de TCP/IP.

Bob Metcalfe un ingénieur travaillant à Xerox développe la technologie d'Ethernet utilisé comme interface de connexion entre les nœuds du réseau. Un service de traductions des noms de domaines en adresse IP, DNS, est développé par Paul Mockapetris (P. Mockapetris, 1988). En 1980, TCP/IP est adopté comme standard pour les ordinateurs. NCP est remplacé par TCP/IP en 1983. En 1985, L'internet devient une technologie supportant une grande communauté des chercheurs et développeurs. Le réseau ARPANET est remplacé en 1990 par NFSNET et les fournisseurs d'internet privés (ISP).

1.4 Protocoles d'internet

D'après le dictionnaire IEEE Standard Dictionary, un protocole c'est « un ensemble des règles qui régissent les unités fonctionnelles pour assurer la communication ». Ces sont des méthodes et des règles utilisés pour la communication. Sur l'internet, les protocoles utilisés font partie d'une suite de protocoles, un ensemble de protocoles reliées entre eux. Cette suite de protocole s'appelle TCP/IP.

Elle contient les protocoles suivants :

1.4.1 HTTP

C'est un protocole qui permet le transfert d'un fichier de forme HTML grâce au URL entre le client et le serveur web. L'utilisateur choisit dans son navigateur d'employer la navigation classique **(http**) ou la navigation sécurisé (**https**), ce qui se lit dans l'URL affichée (Jill West, 2018, p. 9).

1.4.2 FTP

Protocole de transfert de fichiers, leur mode de fonctionnement est de type client-serveur. Le transfert de fichiers assurés par FTP utilise les services TCP. En effet FTP c'est un protocole complexe nécessitant une identification et une authentification de l'utilisateur par login et le mot de passe. Le FTP utilise deux numéros de ports distincts par le serveur et il gère deux connexions TCP par session d'échange.

1.4.3 ARP

Le protocole ARP établit une correspondance dynamique entre les adresses physiques et adresses logiques. Il permet à une machine de connaitre et de trouver l'adresse physique d'une autre machine située sur le même réseau local à partir de sa seule adresse IP (Gilb, 2005).

1.4.4 ICMP

Un protocole qui s'occupe de la transmission des messages de contrôle. ICMP est donc un mécanisme de contrôle des erreurs au niveau IP. Chaque message ICMP traverse le réseau en tant que données d'un datagramme IP.

1.4.5 IP

Protocole implémenté dans toutes les machines hôtes d'internet ainsi que dans tous les routeurs. Il comprend la définition du plan d'adressage, la structure de l'unité de données transférées (Datagramme IP) et des règles de routage. Il existe deux version, IPv4 qui utilise 32 bits pour l'adressage des hôtes et IPv6 qui utilise 128 bits.

1.4.6 TCP

Protocole orienté connexion c'est-à-dire qu'il permet à deux machines qui communique de contrôler l'état de la transmission (Kahn, May 1974). Ce protocole met on œuvre la détection et la correction d'erreurs, gère le contrôle de flux et négocie les conditions du transfert des données entre les deux extrémités de la connexion. L'entête gérée par le protocole s'appelle le segment.

1.4.7 UDP

Protocole de transport non orienté connexion (sans connexion) qui permet l'émission de messages sans l'établissement préalable d'une connexion. Les messages UDP sont généralement appelés datagrammes UDP. Ils contiennent deux parties, un entête et des données encapsulées dans les datagrammes IP, comme les segments TCP (Danièle Dromard, 2009, p. 188).

1.4.8 DNS

C'est un simple protocole de requête-réponse dont les messages dans les deux sens ont le même format. Ses terminologies sont bien décrites dans le RFC 8499. DNS c'est un système de mappage noms de domaines en adresse IP et vice-versa. Avant l'apparition du DNS, le réseau d'ARPANET employait un fichier texte ASCII pour faire ces mappages. Depuis l'ARPANET, l'internet a tellement grandi, un système beaucoup évolué devient nécessaire afin de bien effectuer les mappages des adresses IP pour des milliards des machines sur l'internet.

1.4.9 Telnet

Le protocole de telnet est utilisé pour accéder aux autres ordinateurs à distance (Jill West, 2018). L'authentification de l'utilisateur se fait par un mot de passe. L'inconvénient majeur de telnet c'est que les informations échangées ne sont pas chiffrées, ils sont transmis en clair. Cela a abouti à l'utilisation de SSH au lieu de telnet à cause du chiffrement des données apporté par ce protocole.

1.5 Les services de l'internet

1.5.1 Communication personne à personne

Aujourd'hui la plus célèbre application de la communication personne à personne c'est le twitter. Twitter permet la communication entre plusieurs utilisateurs en ligne (Andrew S. Tanenbaum, March 3, 2021, p. 5). Les utilisateurs peuvent partager des idées et des opinions librement en ligne. Les réseaux sociaux comme le Facebook, Instagram et WhatsApp dominent le domaine de communication personne à personne. Meta continue à investir trop dans ce domaine afin de permettre la communication entre les utilisateurs des leurs réseaux sociaux.

1.5.2 E-mail

L'ARPANET a commencé étant un projet où les chercheurs pouvait utilisés les ordinateurs d'autrui à distance afin des faire des calculs très importants. Suite à l'invention d'email par Tomlison en 1972, email deviens le plus utilisé service de l'internet pour le partage des informations des recherches entre les utilisateurs. E-mail utilise le modèle peer-to-peer (client-client) afin de faire les échanges des mails.

1.5.3 Les loisirs

Suite à l'évolution de l'internet depuis ARPANET et NFSNET et les nombreux investissements dans les infrastructures de l'internet par les sociétés privés, la capacité de transfert de données a beaucoup augmenté. Ce haut débit offert par les réseaux d'aujourd'hui permet l'audio streaming pour la musique (Spotify), les podcasts et la radio en ligne. Les utilisateurs peuvent également faire le video streaming sur des plateformes comme Netflix, YouTube, AppleTV, etc. L'industrie de jeux en ligne a beaucoup bénéficié, les sociétés du gaming comme PUBG, Call of Duty, PES online, etc.

1.5.4 E-commerce

L'e-commerce s'agit de l'achat et la vente des produits sur internet. L'e-commerce permet les utilisateurs d'accéder à un magasin en ligne, commander quelque chose, les options de livraison à domiciles sont disponibles. Le paiement des produits s'effectue par voie de Visa, MasterCard ou Carte Edhabia (Hocine SAM, 2022). L'internet a alors permis à un utilisateur de faire les achats et des ventes sans besoin de se déplacer. Nous pouvons également accéder à nos comptes bancaires d'une manière sécurisée à travers l'internet.

1.5.5 Internet des objets interconnectés

Le domaine d'internet des objets interconnectés (en anglais Internet Of Things) emploie les systèmes embarqués (en anglais Embedded Systems) avec une connexion à l'internet. Ces appareils qu'on dit intelligent sont autonomes et capables de faire des décisions sans l'intervention de l'être humain. Cela permet l'automation de n'importe quel processus répétitif, ou nécessitant une surveillance très pointue surtout dans le domaine industriel et la génie des procédés. Les applications de ces systèmes seraient dans tous les domaines concernés par une automation précises des taches, les systèmes intelligent et dans la communication machine à machine, etc.

1.6 Le Web

1.6.1 Introduction

Selon (Harvey M. Deitel, 2001) le World Wide Web permet les ordinateurs de repérer et voir des documents de la multimédia (textes, graphiques, animations, audios et vidéos). En 1990, Tim Berners-Lee travaillant pour CERN (The European Laboratory for Particle Physics) a développé le World Wide Web et plusieurs protocoles de communication sur le web. Les sites web facilitent notre vie quotidienne. Nous pouvons facilement accéder à des informations en ligne à n'importe quel moment à travers d'un moteur de recherche comme Google.

1.6.2 Historique

Après l'invention de l'email par Tomlison, le web devient le plus utilisé service de l'internet. Le premier prototype de web était fait en 1990-1991 et entièrement accepté en 1994. La première application du web était le logiciel « Enquire » crée par Tim.

A propos de ce logiciel il dit que « …C'est là que j'ai écrit Enquire, mon premier programme de type web. Je l'ai écrit pendant mon temps libre et pour mon usage personnel, sans autre raison que de m'aider à me souvenir des connexions entre les différentes personnes, ordinateurs et projets du laboratoire. » (Berners-Lee, November 7, 2000)

Dans sa vision du web, il voulait créer une espace universelle de partage des informations entre les ordinateurs à travers l'internet, la croissance organique et décentralisée des idées, des technologies et de la société. Aujourd'hui le web englobe plusieurs domaines, la commerce en ligne, la recherche des informations, l'audio streaming, le video streaming, les encyclopédies en ligne, etc.

1.6.3 World Wide Web Consortium (W3C)

En Octobre 1994, Tim Berners-Lee crée une organisation, the World Wide Web Consortium (W3C). Le W3C est une organisation de standardisation spécialisée dans le développement des technologies non propriétaire, interopérable pour le World Wide Web (Harvey M. Deitel, 2001). Ces technologies s'appellent des Recommandations. D'ici on comprend les Recommandations, XHTML, CSS, HTML, XML. Aujourd'hui le W3C est composé de trois membres majeurs, Massachussetts Institute Of Technology (MIT), Institut National de Recherche en Informatique et Automatique (INRIA) et Keio University of Japan et plus de 400 membres.

1.6.4 L'Architecture du Web

Il existe deux architectures des réseaux, l'architecture client-serveur (en anglais client-server architecture) et l'architecture P2P (peer-to-peer.) L'architecture la plus répandue dans le réseau internet c'est le modèle client-serveur (Andrew S. Tanenbaum, March 3, 2021). Sa visualisation est montrée dans la figure 3.

1.6.4.1 L'architecture client-serveur

La plus utilisé application sur l'internet est le web. D'après Larousse en ligne, le web 2.0 « est un système hypermédia de seconde génération autorisant l'accès à internet, axé sur des fonctionnalités visuelles et interactives enrichies et spécifiquement adaptées à chaque utilisateur. »

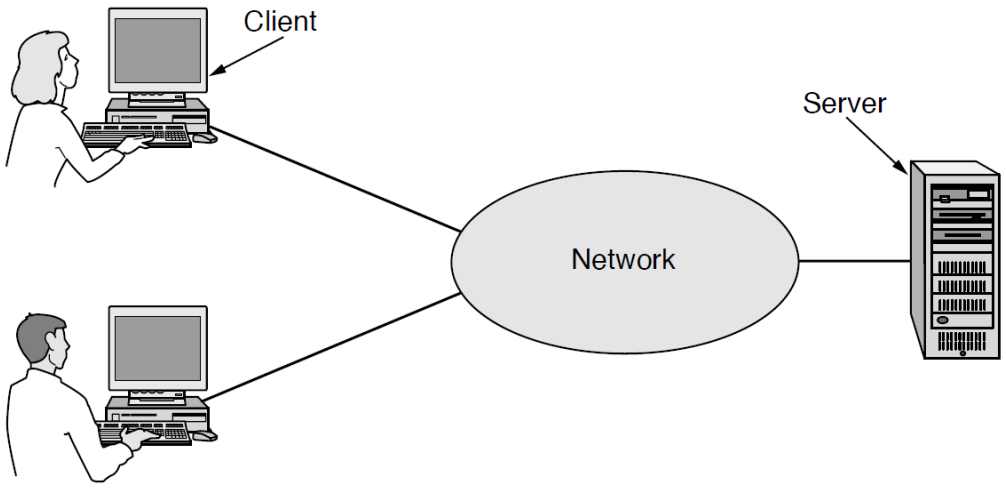

Figure 3 : Le modèle client-serveur (Andrew S. Tanenbaum, March 3, 2021, p. 3)

Les sites web se trouvent sur le World Wide Web. Ces pages web sont disponible à tout moment suit à la requête d'un utilisateur. Un usager peut accéder à un site web en situ chez sa propre entreprise ou à distance. Dans le modèle client-serveur, voire la figure 3, le serveur web s'agit de la partie serveur du modèle. L'utilisateur s'agit du côté client du modèle. Un serveur web se charge de l'accueil des pages web. Il peut accueillir jusqu'à des centaines des milliers des pages web. A la réception d'une requête http, il répond le client avec une réponse http en forme du page web.

1.6.4.2 L'architecture P2P

Dans l'architecture peer-to-peer, voire la figure 4, un utilisateur communique avec d'autres utilisateurs sans l'intermédiaire d'un serveur. Chaque ordinateur possède les mêmes responsabilités et capacités par rapport aux autres. Un exemple d'un système peer-to-peer c'est le BitTorrent (Cohen, 2003) qui n'a pas une base des données centralisée. Chaque utilisateur maintient une base des données locale et une liste des autres utilisateurs. Il ne reste que de consulter les utilisateurs voisins afin de retrouver les informations recherchées.

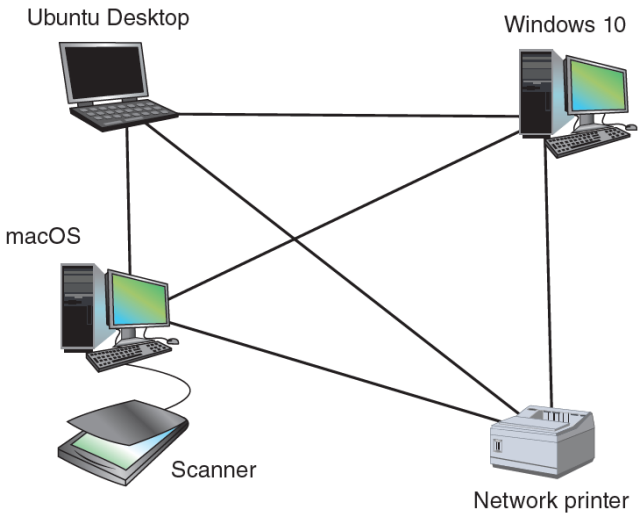

Figure 4 : Le modèle peer-to-peer (P2P) (Jill West, 2018, p. 4)

Le modèle peer-to-peer est très utilisé pour le partage de la musique et des vidéos (Ramayya Krishnan, 2003). Malgré qu'il y ait des applications illégales, il existe des applications légales où les utilisateurs peuvent partager des photos, des films et des logiciels publiques.

1.6.5 Définition des termes

1.6.5.1 Les protocoles du web

Dans son livre Weaving the Web, Tim Berners-Lee le créateur du World Wide Web décrit qu'il est primordial de définir les règles de communication entre les ordinateurs en ligne (sur l'internet). Ces règles s'appellent des protocoles du web. Les protocoles du web c'est l'URL, HTTP et HTML (Berners-Lee, November 7, 2000). Tim Berners-Lee décrit le URL comme l'adresse du page web, HTML étant le langage utilisé par les ordinateurs et HTTP un règle qui définit la machine qui parlent le premier, et comment parler.

1.6.5.2 Navigateur du web

Le navigateur web, voire la figure 5, est un logiciel qui permet un utilisateur des localiser des pages web en ligne (sur internet) et présente celui-ci dans un environnement d'interaction. Il s'agit de fournir l'adresse du site concerné (URL) dans le champ d'adresse offris par le navigateur qui se trouve très souvent en haut de son environnement ou au milieu, après on appuie sur entrée ou on clique sur aller.

Figure 5 : Moteurs de recherche, Google Chrome, Mozilla Firefox et Microsoft Edge

1.6.5.3 URL

L'URL est l'adresse du page web. Afin d'accéder à une page web quelconque, il nous faudrait son URL. Cette adresse est unique pour chaque site web, cela veut dire on ne peut qu'accéder à une seule page web avec un URL. Un exemple d'un URL c'est **http://www.google.com** pour accéder à Google.

1.6.5.4 Hypertexte

D'après (Julie C. Meloni, 2009), hypertexte signifiait à l'origine un texte stocké sous forme électronique avec des liens de renvoi entre les pages. Il s'agit désormais d'un terme plus large qui désigne à peu près n'importe quel objet (texte, images, fichiers, etc.) pouvant être liées à d'autres objets.

1.6.5.5 HTTP

Les URLs des sites web commence toujours par **http://** (pour les connections non sécurisée) ou **https://** (pour les connections sécurisée). Http est un standard pour les transferts des sites web entre les hôtes de l'internet, voire la figure 6.

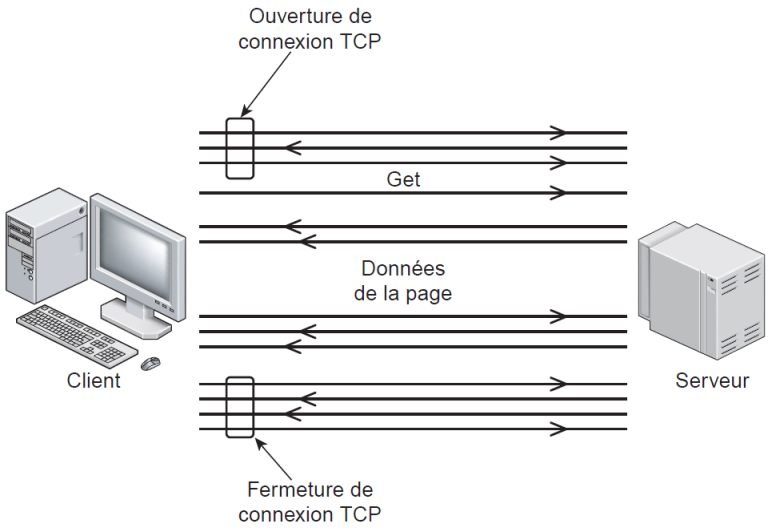

Figure 6 : Echanges HTTP (Danièle Dromard, 2009, p. 232)

Le serveur met des informations à disposition. Le client, avec son navigateur, se connecte pour demander à recevoir ces informations qui s'affichent sur son écran. Le protocole de transport sous-jacent est TCP. Le serveur Web reçoit une demande d'ouverture de connexion sur le port 80 (par défaut), puis une fois la connexion établie, une requête GET qui demande un document particulier. Le serveur recherche dans son environnement de stockage le document en question et crée le flux de données correspondant au contenu du document décrit en HTML et, enfin, la connexion avec le client est rompue (Danièle Dromard, 2009).

1.6.5.6 HTML

HTML est un standard des présentations des pages web au niveau d'utilisateur. HTML décrit au navigateur web la façon dans laquelle la page web doit être afficher. Il s'en sert de ce qu'on appelle des balises pour présenter au navigateur, la parties entête, paragraphe, corps, le début et la fin, les liens etc. HTML aide le navigateur alors, de savoir comment afficher le contenu d'un site web.

1.6.6 Comment réaliser un site web ?

Il existe deux méthodes pour la création des sites web, les éditeurs de texte (le plus utilisé) et la méthode WYSIWYG.

1.6.6.1 Les éditeurs de texte

Un site comprend trois parties en général. La partie HTML, CSS et Javascript. Son code est rédigé en utilisant un environnement de développement comme Atom ou Visual Studio Code comme montré dans la figure 7 ou tout simplement avec le bloc-notes pour les systèmes Windows. HTML et CSS sont deux langues qu'il faut savoir parler pour créer des sites web. C'est le navigateur web qui fait la traduction entre ces langages informatique.

Pour la création d'un site web, on doit donner des instructions à l'ordinateur. Il ne suffit pas simplement de taper le texte qui devra figurer dans le site (comme on le ferait dans un traitement de texte Word par exemple) il faut aussi indiquer ou placer ce texte, insérer des images et faire des liens entre pages.

Figure 7 : Quelques environnements de développement des sites web

1.6.6.2 WYSIWYG (What You See Is What You Get)

Cela veut dire, ce que vous voyez est ce que vous obtenez. Ces sont des programmes qui se veulent très facile d'emploi, ils permettent de créer des sites web sans apprendre de langage particulier. Parmi les plus connus d'entre eux : Mozilla composer, Microsoft Expression Web, Dreamweaver …et même Word ! Leur principal défaut est la qualité souvent assez mauvaise du code HTML et CSS qui est automatiquement généré par ces outils. Un bon créateur de site web doit tôt ou tard connaitre HTML et CSS (Nebra, 2013).

1.6.7 Types des sites web

1.6.7.1 Les moteurs de recherche

Un moteur de recherche est un serveur très indispensable permettant de rechercher et de localiser les informations sur l'internet à partir des mots clés (Danièle Dromard, 2009). Les moteurs de recherche maintien des base des données contenant les informations sur les sites web. Des sites web comme Google (www.google.com), Yahoo ! (www.yahoo.com), AltaVista (www.altavista.com) et HotBot stockent les informations dans les bases des données.

Quand un utilisateur tape une phrase ou un mot de recherche, le moteur retourne des liens (en anglais hyperlinks) à l'utilisateur qui repèrent les sites web contenant l'information recherchée. D'ailleurs, des autres sites web comme Microsoft Network (www.msn.com) utilisent des moteurs des recherche appelé **métamoteurs** (en anglais metasearch engine). Ce type de moteur ne maintien pas une base des données. Il envoie le critère de recherche à d'autres moteurs et ensuite il rassemble les résultats et les présente à l'utilisateur.

1.6.7.2 Wiki

Un wiki est un site web qui permet plusieurs utilisateurs de se collaborer et créer du contenu, dont le plus célèbre wiki c'est le Wikipédia parmi plusieurs wikis existants. Wikipédia était inventé par Ward Cunningham en 1995.

1.6.7.3 Les pages dynamiques

Ces sont des pages web crée spécialement en réponse à la requête d'un utilisateur. Elles possèdent une forme et une contenu variable adaptés à ses besoins.

1.6.7.4 Les pages statiques

Les premiers générations des sites web étaient les pages statiques. Leur contenu et la présentation ne sont pas séparés (Filippo Ricca, 2003). Le site web est livré à l'utilisateur tel qu'il est dans la base de données. Le problème qui se pose à ces sites web ce qu'il devient très complexe de le mettre à jour. A chaque fois qu'il y a des modifications, on doit les refaire indépendamment pour chaque réplication.

Le type des sites web le plus utilisé c'est les pages web dynamique à cause de leur souplesse de modification.

1.6.7.5 Les blogues

Un blogue est un site web personnel, évolutif et non conformiste. Elle est rédigée par l'auteur du blogue, le propriétaire. L'auteur présente ces réflexions en courtes messages pour son audience, les lecteurs du blogue. Les lecteurs peuvent faire de commentaires sur ces messages et participer dans les discussions.

1.6.7.6 D'autre types des sites web

Il existe plusieurs types des sites web. Nous avons parlé sur les plus commun mais il en existe d'autres types comme les sites des réseaux sociaux, les sites des organismes, les portails web, les sites d'actualités, les sites de e-commerce, etc.

1.6.8 Conclusion

Dans ce chapitre nous avons vu que le prédécesseur de l'internet c'était le réseau ARPANET. La technologie employée dans les réseaux d'aujourd'hui c'est la commutation des paquets qui permettent une partage des supports de transmission entre les utilisateurs. Nous avons présenté l'impact de l'internet sur notre vie quotidienne et les protocoles majeurs de l'internet. Nous avons aussi parler sur comment créer un site web, ses différents types, les protocoles du web, l'architecture du web et les avantages apportés par les sites web.

CHAPITRE 2

Authentification, Sécurité Web et l'état de l'art de la biométrie

2.1 Introduction

Depuis des siècles, notre civilisation a toujours l'envie de reconnaitre des individus. Il y a toujours besoin d'identifier quelqu'un en particulier les personnes qu'on ne connait pas comme les étrangers par exemple ou les gens qu'on rencontre pour la première fois. C'est trop facile d'identifier son voisin, ses amis et ses collègues par voie de leurs visages, leur voix et parfois par leur démarche ! L'authentification c'est l'action de vérifier une identité d'un individu. C'est tout simplement l'action de prouver une identité réclamée par un individu. La vérification d'un individu est très importante afin de contrôler l'accès à un endroit privilégié par exemple l'accès à un aéroport, l'accès à une base des données et même pour protéger la vie privée d'un individu. Le but c'est de bloquer l'accès à un individu non autorisé !

Nous vérifions l'identité de quelqu'un soit à l'aide d'un passeport, une carte d'identité nationale, une carte de séjour, le permis de conduire… etc. Cela est une moyenne d'authentification « physique » qu'on appelle « une possession » le Something You Have (Chen Wang, 2020). En accédant au site web c'est plus pratique de s'authentifier d'une manière logique par exemple en utilisant un mot de passe ou un code PIN. D'ici on parle d'un facteur d'authentification basée sur une « connaissance » le Something You Know. Nous pouvons également utiliser une biométrie pour s'authentifier par exemple, l'empreinte digitale, la reconnaissance de visage, la reconnaissance de la voix… etc. le Something You Are.

Dans ce chapitre nous allons parler sur les diffèrent types d'authentification, l'utilisation de l'authentification comme mesure de la sécurité et l'état de l'art de la biométrie.

2.2 Qu'est-ce que c'est l'Authentification ?

L'authentification est le processus de vérification fiable de l'identité de quelqu'un (ou de quelque chose)(Kaufman et al., 1995). Le but de l'authentification c'est de contrôler l'accès à un service ou une facilité. Les personnes non autoriser ne doivent pas avoir accès à ses services. Un système d'authentification se charge de processus de vérification de l'identité d'un utilisateur.

Un utilisateur c'est la personne qui fait une demande d'authentification. Il réclame une identité, le système vérifie si cette identité existe dans sa base de données. Si l'identité réclamé existe, le système d'authentification demande l'utilisateur à prouver qu'il est ce qu'il réclame d'être. Le plus utilisé méthode d'authentification c'est le mot de passe. Supposons notre utilisateur connais un secret que seulement lui et le système connaissent. En présentant ce secret au système, son identité est validée. Il existe d'autre système beaucoup fiable comme la biométrie pour la vérification de l'identité et les jetons de sécurité.

2.3 Pourquoi faire l'authentification ?

L'authentification est utilisée dans les applications web et les applications informatiques pour garantir la sécurité d'une application. L'authentification garantit la sécurité d'une application en limitant l'accès aux seuls utilisateurs autorisés. Les utilisateurs autorisés sont déterminés par un système d'authentification qui utilise ce que l'on appelle des facteurs d'authentification pour déterminer de manière fiable l'identité d'une personne. Il existe plusieurs moyennes d'authentification en fonction de nombre des facteurs d'authentification utilisé pour déterminer si un utilisateur est autorisé ou non.

2.4 Moyennes d'authentification (SFA, 2FA, MFA.)

L'utilisation d'un seul facteur pour vérifier l'identité d'un individu s'appelle l'authentification à un seul facteur (SFA) en anglais single factor authentication. Un exemple de l'authentification à un seul facteur est la combinaison d'un nom d'utilisateur et un mot de passe (Papathanasaki et al., 2022).L'authentification à double facteur ou vérification à deux étapes ou en anglais dual-factor authentication (2FA), est une manière de la vérification de l'identité d'un individu à l'aide de deux paramètres qu'on appelle les facteurs d'authentification, voir le Tableau 1.

L'utilisation de deux ou plusieurs facteurs d'authentification s'appelle authentification à multi-facteurs (MFA) dont 2FA et 3FA (authentification à trois facteurs) sont des exemples de MFA.

2.4.1 Authentification à un seul facteur (SFA)

Le système à un seul facteur d'authentification (single factor authentication) vérifie un individu par voie d'un seul paramètre. En général la plupart de ces systèmes sont basés sur une connaissance, un secret connu que par l'utilisateur. Le plus utilisé facteur dans cette catégorie est le mot de passe.

Figure 8 : L'authentification à un seul facteur, SFA (single factor authentication), (Sabina, 2023)

Un mot de passe est une suite des caractères alphanumériques. Un très bon mot de passe contient une mélange des caractères spéciaux ($, £, %...etc.), une mélange des lettres majuscules, minuscules et des nombres. Une grande entropie dans le mélange des caractères et un mot de passe très long, rend le mot de passe plus sécurisé. Cependant, des longs mots de passe sont faciles à oublier. Étant donné qu'un mot de passe ne contient que des caractères alphanumériques et spéciaux, tout système sécurisé par un mot de passe peut être piraté si l'on dispose de suffisamment de temps(Eng & Wahsheh, 2013).

2.4.1.1 Gestionnaire de mots de passe

Pour n'est pas oublier ses nombreux mots de passe, il existe des solutions fiables comme les gestionnaires de mots de passe (J. Alex Halderman, 2005). Google offre un mécanisme de pouvoir générer de mots de passe automatiques avec une grande entropie des caractères. Ces sont des forts mots de passe qu'on peut stocker dans un gestionnaire de mots de passe (password manager), une fonctionnalité offerte par Google.

Les mots de passe sont cryptés au niveau de gestionnaire de mots de passe, l'accès à un mot de passe quelconque se fait via son compte google ou par un système d'authentification déjà présente sur son appareil (par exemple par une reconnaissance de l'empreinte). Un login dont ses paramètres est déjà enregistré dans le gestionnaire de mots de passe est fait automatiquement, c'est-à-dire quand vous visitez le site pour la deuxième fois, les identifiants de connexion sont remplis automatiquement.

Les avantages d'utilisation des mots de passe :

1. Le système à mot de passe est très facile à implémenter et ne requière pas des dispositifs additionnels. Les smartphones, les ordinateurs et les tablettes supportent tous l'utilisation du mot de passe.
2. L'utilisation du mot de passe est très pratique pour l'utilisateur. Il s'agit de saisir juste un nom d'utilisateur et un mot de passe sans besoins des facteurs additionnels. Le processus d'authentification est simple et rapide.
3. L'emploie de cette technologie est moins cher au niveau du matériel.

Les inconvénients d'utilisation de mot de passe :

1. Nous utilisons plusieurs services de l'internet aujourd'hui. Il devient très difficile à se rappeler à des plusieurs mots de passe à ses services (Petsas et al., 2015). Cela mène à la réutilisation du même mot de passe sur plusieurs sites web. Si ce mot de passe est compromis, l'imposteur gagne l'accès à tous les sites utilisant ce mot de passe (J. Alex Halderman, 2005).
2. Les mots de passe sont faciles à oublier et à perdre.
3. Les mots de passe sont susceptibles à des attaques de type « brute-force », « Dictionary attack » et le phishing (DeFigueiredo, 2011) .

Les systèmes à mots de passe ne garantissent pas que l'individu qui a fourni le mot de passe est vraiment l'utilisateur désirée. N'importe quelle personne qui connaisse le mot de passe peut accéder au système. Les mauvaises pratiques des gestions de base des données de mots de passe ont assez contribué à la faiblesse des ces systèmes. Pour ces raisons et les inconvénients cité en dessus, le SFA n'est pas assez sécurisé pour authentifier les individus. D'ailleurs, le SFA de systèmes à biométrie autonome offre une meilleure sécurité. Il nous faut un système beaucoup mieux qui répond à ces inconvénients et qui est plus sécurisé.

2.4.2 Authentification à double facteur (2FA)

L'authentification à double facteur ou vérification par deux étapes est un processus de sécurité visant à vérifier un individu en fonction de deux facteurs d'authentification, voire la figure 9. Un facteur d'authentification est un critère par laquelle on peut prouver son identité à un système de vérification. Le 2FA est beaucoup utilisé dans les systèmes de banque en ligne et par les fournisseurs des services Internet. Les facteurs les plus employés sont bien détaillés dans le Tableau 1.

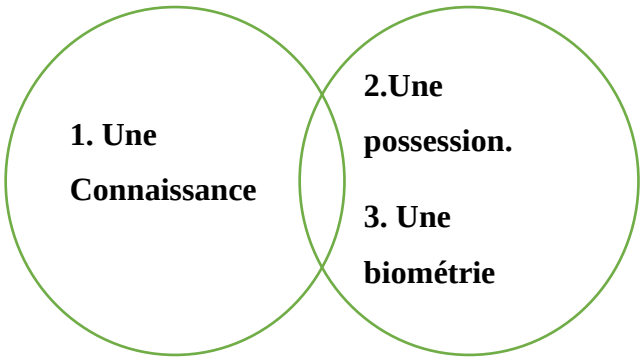

Figure 9 : La vérification à deux étapes emploie deux facteurs provenant des différentes familles d'authentification, le deuxième facteur est soit une possession ou une biométrie.

Il existe d'autres facteurs d'authentification, voir le Tableau 2, qui renforce le contrôle d'accès à un système quelconque comme la localisation d'un smartphone par exemple et la période limitée pour faire une authentification valide (Linda Rosencrance, 2023). L'authentification à double facteur nécessite un deuxième appareil comme un smartphone, ordinateur ou un dispositif électronique (par exemple un capteur de l'empreinte).

Les facteurs d'authentification les plus utilisés	Exemples
1. Une connaissance (quelque chose que vous connaissez) en anglais (knowledge-based authentication)	Mot de passe, PIN, code de téléphone…etc.
2. Une possession (quelque chose que vous possédez) en anglais (token-based authentication)	Une clef, un badge, une pièce d'identité, clé USB, carte à puce, carte magnétique...etc.
3. Une biométrie (une modalité biométrique)	L'empreinte digitale, la voix, le visage, la géométrie de la main, les thermogrammes, l'iris, la rétine, la démarche …etc.

Tableau 1 : Les trois plus utilisés facteurs d'authentification.

Les facteurs d'authentification additionnels	Exemples
4. Une localisation	Localisation de l'appareil qui fait une tentative d'authentification
5. Le temps	Don d'une période limité pendant laquelle on peut s'authentifier, hors de cette durée du temps, l'authentification n'est plus valide.

Tableau 2 : Les autres facteurs d'authentification

Lors de l'authentification à double facteur, c'est obligatoire de présenter au système ses deux facteurs d'authentification. Deux facteurs appartenant à une même famille par exemple (mot de passe et PIN) n'est pas une authentification à double facteur !

Le premier facteur appartient à la famille « une connaissance ». Il s'agit d'un nom d'utilisateur et le mot de passe. Le deuxième facteur comprend soit « une possession » ou « une biométrie », voire la figure 9. Pour accéder au système, il faudrait tous les deux facteurs. Un imposteur peut intercepter le mot de passe mais sans le deuxième facteur, l'authentification est impossible. Pour ces raisons, l'authentification à double facteur apporte un meilleur niveau de sécurité par rapport à l'authentification à un seul facteur (SFA).

2.4.2.1 Mode de fonctionnement de l'authentification à double facteur

Le mode de fonctionnement d'un système 2FA peut être décomposé en 4 étapes :

Etape 1 : L'utilisateur est demandé de faire un login par le site web ou l'application.

Etape 2 : L'utilisateur fournisse « une connaissance » (nom d'utilisateur + mot de passe). Le serveur cherche à repérer cet utilisateur dans sa base de données. En le trouvant on passe à la troisième étape. Pour les processus qui ne nécessitent pas le mot de passe le système offre un jeton de sécurité à l'utilisateur. L'outil d'authentification vérifie ce dernier et après le serveur le valide (Linda Rosencrance, 2023).

Etape 3 : Ici l'utilisateur passe à la deuxième étape d'authentification. L'utilisateur doit présenter au système d'authentification « une possession » ou « une biométrie ». Le système peut générer un code sécurisé dont l'utilisateur doit fournir. Ce code est appelé code OTP, le one-time password.

Etape 4 : Si les facteurs fournis sont reconnus au niveau de serveur, l'authentification est réussie ! L'utilisateur est autorisé à accéder au site web ou à l'application.

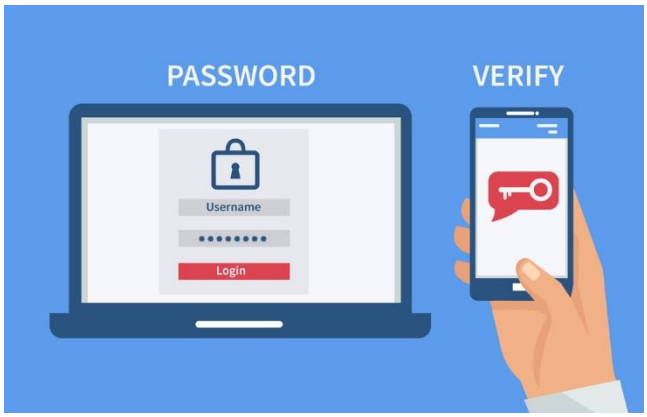

Figure 10 : L'utilisation d'une empreinte digitale comme deuxième facteur d'authentification (Arntz, 2023)

2.4.2.2 Type des produits à 2FA

- Le jeton de sécurité donné à un utilisateur qu'il utilisera pour faire un login.
- Des infrastructures ou des logiciels chargé de la reconnaissance et l'authentification des utilisateurs qui utilise des jetons de sécurité.
- Le 2FA supporte des jetons de matériel pour faire l'authentification par exemple YubiKey (un petit clé USB qui utilise les OTP, le chiffrement à clé publique, l'authentification et le Universal 2nd Factor Protocol développé par FIDO alliance.)

2.4.2.3 2FA pour les Smartphones

La plupart des smartphones d'aujourd'hui offre une gamme des capteurs utilisé dans l'authentification à double facteur. D'ici on comprend le capteur de l'empreinte digitale, la caméra à haute résolution pour la reconnaissance faciale, le microphone pour la reconnaissance de la voix, le GPS pour déterminer la location de l'appareil…etc. En plus, le SMS peut être utilisé comme un canal hors bande (OOB) le out-of-band channel authentication. Un numéro de téléphone de confiance est chargé de recevoir les codes de vérification par texte ou appel téléphonique (Linda Rosencrance, 2023).

Apple iOS, Google Android et Windows Hello ont tous des applications qui supporte le 2FA. Nous pouvons également marquer un appareil comme étant un dispositif de confiance (Dostálek, 2019). Seul l'authentification reçu à partir de cet appareil sera accepté. Des applications comme Google Authenticator peut également être utilisé pour gérer les messages de vérification.

2.4.2.4 Notifications push pour le 2FA

Les notifications en push ou push notifications en anglais (password-less authentication) vérifie l'individu en envoyant une alerte d'une tentative d'authentification à une application sécurisé au niveau de l'appareil de l'utilisateur (Oskar Persson, 2017). L'utilisateur doit autoriser ou denier cette demande d'authentification par appuyant sur un bouton « oui » ou « non ». Si l'utilisateur accepte la requête d'authentification, le serveur traite la demande et donne l'accès au demandeur de login.

Le but de notification en push est d'établir si l'appareil enregistré avec le système d'authentification est vraiment dans la main de l'utilisateur. Ce processus élimine les attaques de type « man-in-the middle attack » où un intercepteur des identifiants de connexion peut tenter de faire un login, elle élimine également les accès non-autorisé et les attaques d'ingénierie sociale (Linda Rosencrance, 2023).

2.4.2.5 Mot de passe à usage unique (OTP)

OTP c'est une abréviation anglaise pour one-time password qui signifie mot de passe à usage unique. Ce mot de passe est relié à une seule transaction. Elle est valide pour seulement cette transaction une seule fois. Elle n'est peut pas être réutilisée. Un OTP peut être généré au niveau du client (client-side) ou au niveau du serveur (server-side). Le OTP généré au niveau du serveur est envoyé à l'utilisateur par SMS via un canal hors bande (OOB) le out-of-band channel (Dmitrienko, 2014). L'OTP peut être envoyé par voie de l'internet. Cette solution exige que l'appareil soit connecté en ligne.

2.4.2.6 Authentification 2FA à SMS (mTAN, SMS TAN)

Les systèmes SMS TAN nous permet de protéger un compte bancaire en cas où les identifiants de connexion soit compromis. Le système informatique de la banque génère un jeton de sécurité TAN (Transaction Authentication Number) qui est en fait un OTP cryptographiquement lié aux données de transaction. Le code TAN est envoyé par SMS au téléphone de client. Afin de compléter une transaction, l'utilisateur doit saisir ce code TAN par un autre appareil. Sans le code TAN, la transaction n'est pas validée.

Ces systèmes permettent de mitiger contre les attaques sur les mots de passe comme le phishing et les keyloggers. Le 2FA à SMS est moins cher, facile à implémenter et acceptable par les utilisateurs. Néanmoins, selon un rapport par NIST dans leur publication 800-63-3 : digital identity guidelines (Grassi et al., 2017), Le 2FA est maintenant déconseillé puisqu'il est sujet à des attaques de type « mobile phone portability attack ». Il s'agit d'attaques contre le réseau de téléphonie mobile et des logiciels malveillants qui peuvent être utilisés pour intercepter ou rediriger des messages textuels.

2.4.2.7 Modalités biométriques

Nous avons dit que l'authentification à double facteur emploie deux facteurs d'authentification dont le premier est basé sur « une connaissance ». Le deuxième facteur d'authentification peut être basé sur une modalité biométrie qui est le sujet de notre étude, voire la figure 10.

Dans cette étude nous allons réaliser un système à 2FA employant une empreinte digitale ou une reconnaissance du visage comme le deuxième facteur d'authentification. Nous allons parler beaucoup sur la biométrie dans la deuxième partie de ce chapitre.

2.4.3 Authentification à multi-facteurs (MFA)

L'authentification à multi-facteurs cherche à augmenter le niveau de sécurité d'un système informatique contre les accès non-autorisés en employant au moins trois facteurs d'authentification, voire la figure 11, la connaissance, une possession et une biométrie (Ali et al., 2020). Un exemple d'une authentification MFA sera par exemple, disons qu'on veut retirer de l'argent d'un guichet automatique. Nous présentons trois facteurs d'authentification :

- La carte bancaire
- Le PIN
- Une modalité biométrie (par exemple l'empreinte digitale)

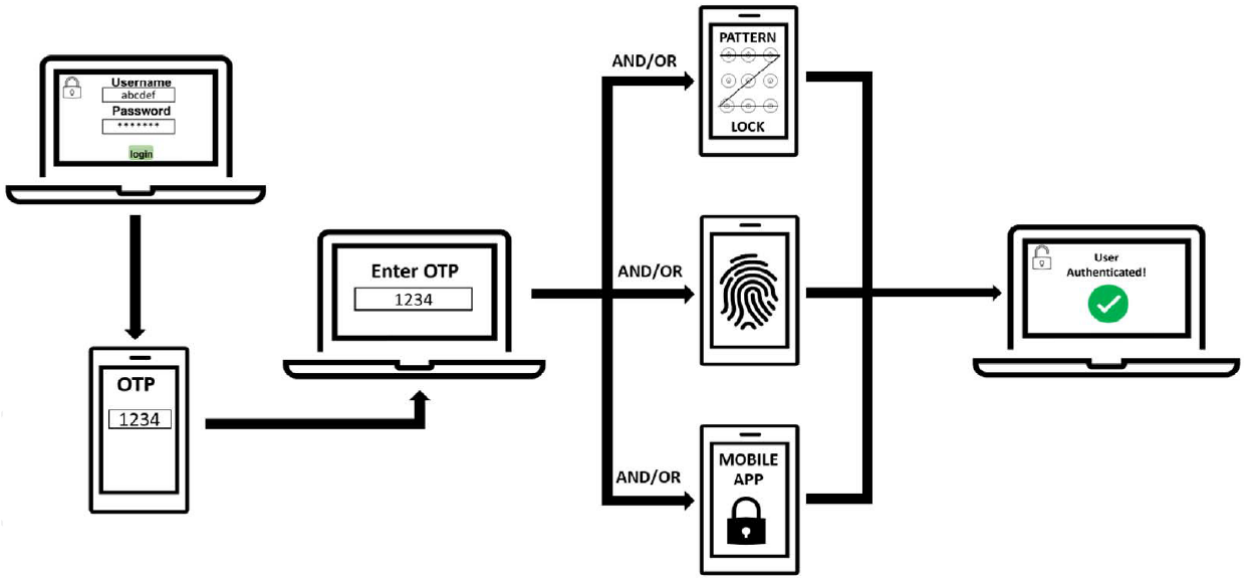

Figure 11 : L'authentification à multi-facteurs (Papathanasaki et al., 2022)

Le MFA emploie plusieurs facteurs d'authentification ce qui le rend difficile pour une usurpation d'identité ce qui mène à un système de haute sécurité(Papathanasaki et al., 2022). D'une perspective de l'utilisateur, l'utilisation de nombreux facteurs de l'authentification est gênante. L'acceptabilité de ces systèmes est bas parce qu'il prend beaucoup de temps pour faire un login. Les systèmes à MFA sont très utiles dans les applications nécessitant des niveaux de très haute sécurité comme le système bancaire, la protection de dossiers médicales des patients et les cours en ligne (MOOC).

Cependant, les systèmes MFA sont susceptibles aux erreurs FAR et FRR. Le système à MFA est cher à implémenter puisque les critères d'authentification ont augmenté, il nécessite plus de l'infrastructure plus que le 2FA.

2.5 Reconnaissance Biométrique

Dans notre vie quotidienne, il est très pratique de reconnaitre une personne en se rappelant de leur visage, le son de leur voix ou lorsque la personne marche à distance, par leur démarche. Ce processus est un exemple d'une utilisation de la biométrie pour reconnaitre une personne. La biométrie est un processus de mesure statistique des caractéristiques physiques ou comportementales d'un individu.

Nous allons identifier une personne en lui associant ces attributs personnels par exemple, le visage, la voix, l'iris, l'empreinte digitale…etc. Il est difficile de les partager, de les voler ou de les falsifier et contrairement aux possessions et aux connaissances, ils ne peuvent être modifiés. La biométrie est le troisième facteur d'authentification en Tableau 1 (quelque chose que vous êtes) le Something You Are.

2.5.1 Historique

Le mot biométrie vient des mots grecs "bios" (vie) et "metrikos" (mesure). Les premiers exemples connus d'identification biométrique ont eu lieu dans l'Égypte ancienne à l'époque du pharaon Khaefre (2558-2532 av. J.-C.). L'identification biométrique a été utilisée pour identifier les ouvriers du bâtiment, afin de garantir que la nourriture fournie par l'État soit répartie équitablement entre les personnes légitimement éligibles à la recevoir. Les administrateurs ont développé un système qui enregistrait les caractéristiques physiques et comportementales distinctives des travailleurs, ainsi que les données relatives à leur âge et leur lieu de résidence.

Ce système a permis de résoudre les problèmes liés au fait que certains employés tentaient d'obtenir plus que l'allocation alimentaire qui leur était allouée (Smith et al., 2018).

Dans les années 1800, les législateurs utilisaient des photographies pour identifier de petits groupes de personnes. Les autorités chargées de l'application de la loi identifiaient ainsi les récidivistes, mais cette méthode s'est ensuite révélée inefficace pour les grands groupes de personnes. Il fallait conserver un grand nombre de photographies et le système de récupération était manuel. La police a alors adopté le système Bertillon, un système biométrique développé par un français appelé Alphonse Bertillon basé sur l'anthropométrie. Ce système permet d'identifier les criminels sur la base de caractéristiques anatomiques.

Les mesures de la largeur de la tête, de la longueur du pied gauche, de la longueur de l'avant-bras jusqu'à l'extrémité du majeur et de la longueur du majeur étaient utilisées pour identifier un individu (nlm.nih.gov, 2023). Au début des années 1900, l'utilisation des empreintes digitales a supplanté le système Bertillon.

Jan Evangelista Purkinje (1787-1869), scientifique tchèque, a établi que les empreintes digitales étaient uniques, ce qui a eu des répercussions sur l'identification des personnes impliquées dans des activités criminelles (Smith et al., 2018). Le système initial d'utilisation des empreintes digitales pour identifier un individu a été mis au point par Sir Francis Galton. Galton a déterminé le caractère unique des empreintes digitales d'une personne et les a classées en trois types : les tourbillons (spires ou verticilles), les boucles et les arches, voire la figure 17. L'associé de Galton, Edward Henry, a ensuite poursuivi ses recherches pour faire des empreintes digitales des éléments d'identification uniques. En raison de l'efficacité du système Henry, Scotland Yard, un organisme chargé de l'application de la loi l'a adopté.

En 1936, le Dr Frank Birch a proposé d'utiliser le motif de l'iris de l'œil comme identifiant. Le ministère de la défense américain a lancé le programme de reconnaissance faciale (FERET) en 1993 afin de mener des activités de recherche et de développement dans le domaine de la technologie de la reconnaissance faciale (Eng & Wahsheh, 2013).

Le FBI a ensuite lancé le système CODIS (Combined DNA Index system) en 1998, une base de données médico-légales stockant l'ADN des criminels et des victimes en vue d'une identification ultérieure. L'ISO, fondée en 2002, a été chargée de superviser les normes utilisées pour les mesures biométriques.

Le ministère de la défense américaine a mis en place le système d'identification biométrique automatisé (ABIS) en 2004 afin de suivre les menaces qui pèsent sur la sécurité nationale des États-Unis. Les identifiants biométriques utilisés dans ce système sont les empreintes digitales, les photos d'identité, les échantillons de voix et l'ADN(Eng & Wahsheh, 2013).

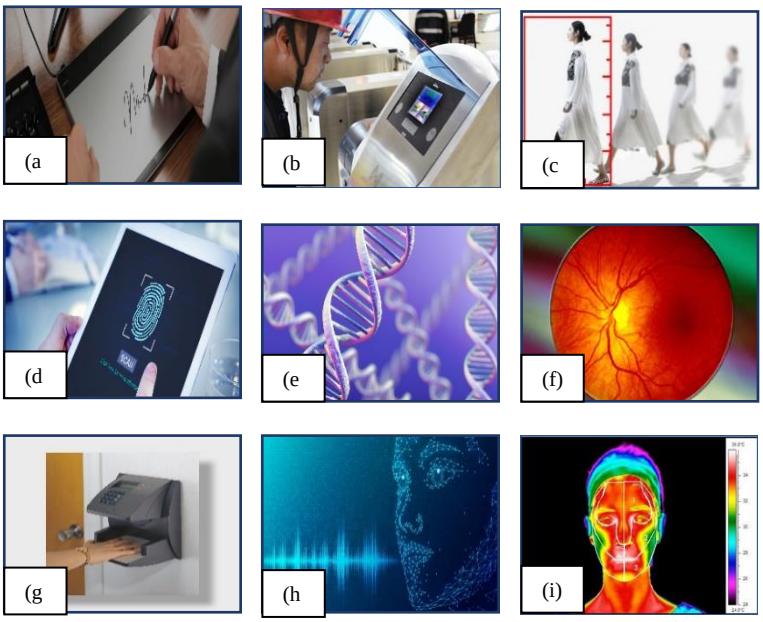

Figure 12 : Différents modalités biométriques (a) la reconnaissance du signature (www.01systems.com, 2023) (b) Un système de reconnaissance de l'iris a été installé dans les mines pour identifier les mineurs autorisés avant qu'ils ne descendent sous terre (Xinhua, 2023) , (c) la reconnaissance du démarche d'un individu (Zdziarski, 2023) (d) un lecteur de l'empreinte sur un tablette (www.futura-sciences.com, 2023), (e) le génome humain (www.alliancevita.org, 2023), (f) la rétine (www.cite-sciences.fr, 23), (g) la reconnaissance de la géométrie de la main (www.zalix.fr, 2023), (h) un échantillon de la voix est utilisée pour la reconnaissance de la voix (www.xrtoday.com, 2023), (i) la reconnaissance à thermogramme faciale (Brioschi, 2023)

2.5.2 Pourquoi utilise-t-on la biométrie ?

L'utilisation de la biométrie est une solution naturelle et fiable. Les modalités biométriques sont difficiles à manipuler et à reproduire. Ils offrent un lien fort et permanent entre la personne et son identité. Ces modalités ne peuvent pas être oublier ou partager contrairement aux mots de passe.

2.5.3 Propriétés d'une caractéristique biométrique

Les propriétés pour une biométrie parfaite étaient bien expliquées par Roger Clarke en (Clarke, 2023) . En général, sept propriétés doivent être pris en compte pour déterminer si un trait physique ou comportemental peut être utilisé dans une application biométrique. Dans la réalité, une biométrie ne peut pas avoir tous ces propriétés. La pertinence d'une donnée biométrique spécifique pour une application est établie en fonction de la nature et des exigences de l'application et des propriétés de la caractéristique biométrique.

- Universelle : toutes les membres de la population à identifier doivent la posséder
- Mesurable : facilement et quantitativement mesurable
- Unique : deux personnes ne doivent pas posséder la même caractéristique
- Permanence : ne doit pas varier au cours de temps
- Performante : l'identification doit être précise et rapide
- Acceptance : doit être accepté par les utilisateurs de système
- Doit être difficile à dupliquer par un imposteur

2.5.4 Système Biométrique

Un utilisateur est une personne qui présente son identifiant biométrique au système afin d'être reconnue. Un élément biométrique peut être appelé indifféremment une biométrie ou identificateur biométrique ou modalité biométrique. Les systèmes biométriques exigent que la personne soit présente au moment de l'authentification. Le système évite les imposteurs car il dispose déjà d'une base de données prédéfinie. Les systèmes biométriques sont utilisés pour remplacer ou compléter les mécanismes existants basés sur les connaissances ou les jetons de sécurité.

2.5.4.1 Mode de fonctionnement d'un système biométrique

Il mesure une ou plusieurs caractéristiques physiques ou comportementales d'une personne. D'ici on comprend l'empreinte digitale, la géométrie de la main, le visage, l'iris, la rétine, l'oreille, le démarche, le rythme de frappe sur un clavier, la voix, la signature, l'odeur, les veines de la main et l'ADN. Ces caractéristiques s'appellent des traits ou indicateurs ou modalités ou identifiants.

2.5.4.2 Enrôlement

Les données biométriques sont recueillies auprès de l'individu et stockées dans la base de données avec son identité. Les données biométriques sont traitées et l'extraction des caractéristiques saillantes et distinctives est effectuées. Les données brutes sont éliminées. L'extraction de caractéristiques est un processus qui consiste à générer une représentation numérique compacte mais expressive d'un trait biométrique sous-jacent, appelé modèle (Template).

Le modèle doit contenir des informations saillantes, discriminatoires et essentielles pour reconnaitre la personne. Un exemple des informations saillantes est les minuties utilisées dans la reconnaissance de l'empreinte. La position et l'orientation des minuties (endroits où les crêtes de frottement d'une empreinte digitale présentent des anomalies) sont uniques pour chaque doigt. Pendant l'enrôlement le modèle est stocké dans la base de données centrale du système biométrique ou dans une base de données distribué (carte à puce).

2.5.4.3 Reconnaissance

Dans l'étape de la reconnaissance les données biométriques sont récupérées auprès de l'individu et comparées aux données stockées dans la base de données afin de déterminer l'identité de l'utilisateur (Faundez-Zanuy, 2006). Les données biométriques récupérées pour la raison de reconnaissance s'appellent une requête ou en anglais « input » ou « query ». Pendant le processus de la reconnaissance, le modèle est comparé avec les caractéristiques extrait d'un utilisateur dans un processus appelé la mise en correspondance (Matching).

2.5.5 Fonctionnalités biométriques

Les deux fonctionnalités biométriques sont la vérification (authentification) et l'identification.

2.5.5.1 Vérification

Dans le cadre de l'authentification, un utilisateur revendique une identité au moyen d'un code PIN, d'un nom d'utilisateur ou d'un jeton (carte à puce), puis le système vérifie si la revendication est authentique. Le système possède une grande base des données contenant une liste des modèles et les noms d'utilisateurs correspondants. L'entrée de l'utilisateur est utilisée pour sélectionner le modèle dans la base de données. Si la saisie de l'utilisateur présente un degré élevé de similitude avec le modèle, la demande est acceptée comme authentique, sinon l'utilisateur est considéré comme un imposteur(Jain et al., 2011).

L'authentification peut être posé comme un problème de classification en deux catégories. Une identité revendiquée, I, et un ensemble de caractéristiques Y^Q. Nous devons déterminer si I et Y^Qappartiennent à la classe des identités authentiques ou à celle des imposteurs. Y^M est un modèle stocké appartenant à l'identité I. Y^Qest comparé à Y^M et un score de correspondance s, qui mesure la similarité entre Y^Q et Y^Mest calculé.

La règle de décision :

I et Y^Q ϵ	Authentique, si $s \geq \eta$ Imposteur, si $s \leq \eta$

η : un seuil prédéfini

Lorsque la demande d'identité est jugée authentique, l'utilisateur est autorisé à accéder aux services fournis par le système. Cette règle de décision qui renvoie un résultat indiquant que l'utilisateur présentant ses caractéristiques biométriques ne fait pas partie des utilisateurs inscrits est appelée le open set identification. Presque tous les systèmes pratiques d'identification biométrique utilisent le open set identification.

2.5.5.2 Identification

L'identification biométrique est basée sur des caractéristiques biométriques et repose uniquement sur les données biométriques. Ce système a accès à une vaste base des données contenant plusieurs modèles des différentes personnes. Il peut parcourir cette base des données afin de faire la correspondance entre une requête (query) et le modèle (Template)(Jain et al., 2011). Il fait ceci modèle par modèle, à chaque instant il compare le modèle avec la requête (query) dans un processus appelé Matching ou la mise en correspondance. Le résultat est une liste de candidats qui ressemble beaucoup à la biométrie d'entrée.

Un système d'identification biométrique fonctionne selon deux modes différents :

2.5.5.2.1 Identification positive

Dans ce mode, le système détermine si un individu figure dans une base de données. Les erreurs possibles sont une fausse acceptation (FAR) et un faux rejet (FRR). Une fausse acceptation se produit lorsqu'un imposteur est accepté. Un faux rejet se produit lorsqu'un utilisateur légitime est rejeté à tort.

2.5.5.2.2 Identification négative (dépistage)

Dans ce mode, le système détermine si l'utilisateur n'apparaît pas dans une base de données négative, par exemple sur une liste des personnes les plus recherchées. Ce mode est également appelé filtrage(screening), car le sujet saisi est en fait soumis à un filtrage par rapport à la base de données biométriques. Les erreurs possibles sont une erreur de faux négatif et une erreur de faux positif. Une erreur faussement négative se produit lorsque le système ne trouve pas de correspondance quand le modèle d'entrée existe déjà dans la base de données. Une erreur de type faux positif se produit lorsque le système détecte incorrectement une correspondance(Bohringer, 2010).

L'identification biométrique peut donner lieu à plusieurs correspondances possibles. Pour une identification positive, il est nécessaire que la liste des candidats correspondants soit unique. Pour une identification négative, la liste de candidats renvoyée doit être réduite afin de pouvoir être examinée par des opérateurs humains.

2.5.6 Eléments constitutifs d'un système biométrique

Tout système biométrique comprend quatre éléments constitutifs basiques :

- Module d'apprentissage (capteur + extracteur des caractéristiques)
- Module de mise en correspondance (Matching module)
- Une base des données
- Module d'adaptation (facultatif)

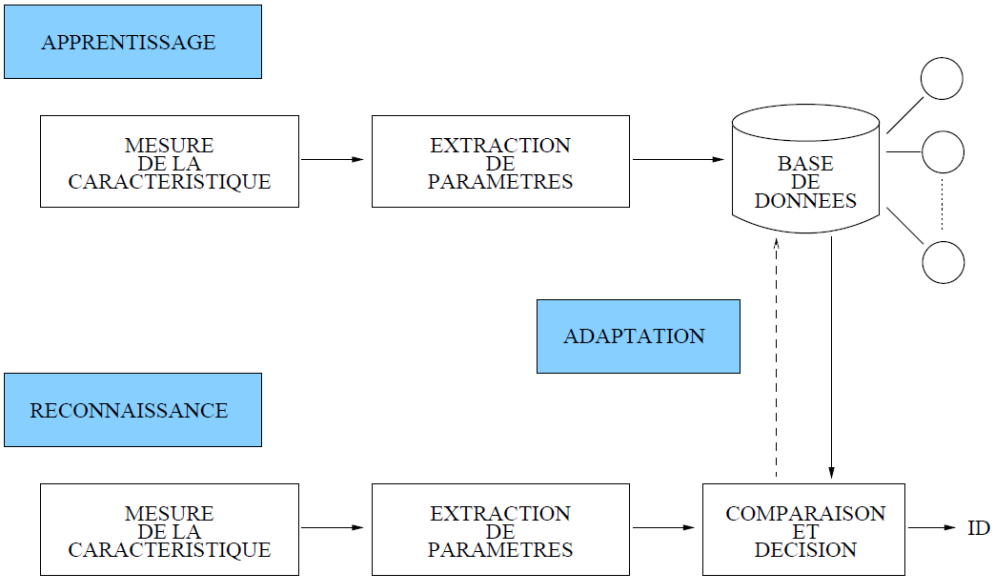

Figure 13 : Les éléments constitutifs d'un système biométrique (Faundez-Zanuy, 2006)

2.5.6.1 Module d'apprentissage

Les données biométriques sont acquises par le module d'apprentissage. Ils ne sont pas stockés directement, des transformations lui sont appliqués(Jain et al., 2011). A la fin d'apprentissage nous nous retrouvons avec un modèle de l'individu qui va servir en tant qu'un point de comparaison lors de la reconnaissance. Le modèle pourra être réévalué après chaque utilisation grâce au module d'adaptation. Le modèle peut être appelé image de référence ou Template en anglais.

2.5.6.2 Le Capteur

Le capteur (sensor module) c'est lui l'interface utilisateur chargé de mesurer la donnée biométrique de l'utilisateur. Pour mesurer les informations de l'empreinte par exemple nous utilisons un capteur optique de l'empreinte afin de capturer les minuties. Le capteur doit être facile à utiliser. La qualité des échantillons acquises par le capteur dépend fortement de caractéristiques de capteur utilisé(Jain et al., 2008).

2.5.6.3 Extracteur des caractéristiques

L'extraction de caractéristiques est un processus qui consiste à générer une représentation numérique compacte mais expressive d'un trait biométrique sous-jacent, appelé modèle (Template). Ce processus peut être subdivisés en trois étapes, l'évaluation de la qualité d'échantillon, la segmentation et l'amélioration(Jain et al., 2011).

2.5.6.4 La base des données

La base de données du système biométrique sert de dépôt pour les informations biométriques (modèles). Un modèle est stocké avec le nom, le code PIN ou l'adresse de l'utilisateur. Une base de données peut être centralisée ou décentralisée.

La base de données centralisée stocke les informations biométriques de toutes les personnes inscrites. Ils sont principalement utilisées dans des applications où seul un petit groupe de personnes est impliqué, par exemple pour contrôler l'accès à un ordinateur portable ou à un téléphone(Bohringer, 2010).

Pour les bases des données décentralisée, les informations biométriques sont stockées de manière distribuée, par exemple sur des cartes à puce. Il n'y a pas de base de données centrale. Un utilisateur présente au système un dispositif biométrique (carte à puce) contenant un modèle biométrique unique. Le système compare l'échantillon d'entrée au modèle stocké dans le jeton pour confirmer une correspondance ou une non-correspondance. Dans la pratique, la plupart des systèmes biométriques utilisent tous les deux types de base de données(Bohringer, 2010).

2.5.6.5 Module de correspondance

Le module de mise en correspondance (Matching module) compare le modèle de la requête avec le modèle stocké pour générer un score de correspondance. Plus le score de correspondance est élevé, plus la similarité entre les deux est grande. Un module de mise en correspondance peut également mesurer la dissimilarité entre les deux ensembles de caractéristiques. Dans ce cas, le score de correspondance est appelé score de distance.

Un score de distance faible indique une plus grande similarité. Dans un système de comparaison d'empreintes digitales, le nombre de points caractéristiques entre l'ensemble de caractéristiques d'entrée et l'ensemble de caractéristiques du modèle peut être considéré comme le score de correspondance(Jain et al., 2011).

2.5.6.6 Module d'adaptation

Lors de l'apprentissage, il est difficile de créer un modèle qui contient toutes les variations d'un attribut biométrique. Les caractéristiques d'une biométrie et ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire améliorer la performance d'un système utilisation après utilisation. L'adaptation possède deux modes, supervisé ou non supervisé. Les paramètres extraits d'un signal servirent alors à re-estimer son modèle. L'adaptation non supervisé est très pratique dans les systèmes autonomes mais il peut poser un problème, en cas des erreurs de module de reconnaissance (Florent Perronnin, 2002).

2.5.7 Précision d'un système biométrique

Lorsqu'une personne enrôlée présente ses données biométriques au système, celui-ci les accepte-t-il toujours correctement et ne les rejette-t-il pas ? Si un imposteur présente ses données biométriques au système, celui-ci les rejette-t-il toujours ? Deux types de taux d'erreur sont utilisés pour mesurer la précision d'un système biométrique. Le risque d'accepter à tort un imposteur est appelé taux de fausses acceptations (FAR) le false accept rate et celui de rejeter un utilisateur légitime est appelé taux de faux rejets (FRR) le false reject rate(El-Abed et al., 2012).

Ces erreurs proviennent du fait que les systèmes biométriques reposent sur les mesures numériques des caractéristiques du corps et non sur la caractéristique elle-même. Le processus de mesure introduit des variations dans les échantillons du même trait biométrique d'un utilisateur sur une longue période de temps.

Des conditions de détection imparfaites peuvent contribuer à une empreinte digitale bruyante en raison d'un dysfonctionnement du capteur, des changements dans les conditions ambiantes affectent grandement la reconnaissance faciale, des variations dans l'interaction de l'utilisateur avec le système introduisent des erreurs (empreinte partielle). En fonction du niveau de stress de l'utilisateur, l'échantillon vocal au moment de l'authentification peut être très différent d'un modèle enregistré.

2.5.7.1 Failure-To-Acquire (FTA)

Les taux d'échec à l'acquisition (FTA) sont définis comme la proportion attendue de transactions pour lesquelles le système n'est pas en mesure de capturer un signal biométrique de qualité adéquate (Faundez-Zanuy, 2006). Les erreurs d'acquisition (FTA) se produisent lorsque l'utilisateur tente d'introduire une requête dans un système pour vérification. Le taux de FTA est calculé en tenant compte de toutes les tentatives d'acquisition d'échantillons qui ont échoué (Eng & Wahsheh, 2013).

2.5.7.2 Failure-to-Enroll (FTE)

Le taux de FTE est la probabilité qu'une fraction d'un groupe de personnes ne puisse pas s'inscrire dans un système biométrique. L'erreur de non-enrôlement (FTE) survient lorsqu'une personne est incapable de s'enrôler dans un système biométrique en raison de ses limitations physiques. Une personne souffrant d'un handicap physique, comme des doigts manquants, ne pourra pas s'inscrire dans un système de reconnaissance d'empreintes palmaires, par exemple. Des yeux endommagés ne peuvent pas être enregistrés pour la vérification de l'iris ou de la rétine. Les brûlures et les blessures sont aussi des source des erreurs FTE. Les systèmes de vérification des empreintes digitales ont un taux de FTE de 2 %. Les systèmes de vérification de l'iris ont un taux de FTE de 1 % (Eng & Wahsheh, 2013).

D'autres erreurs se produisent dans les systèmes biométriques, les erreurs de fausses non-correspondances (FNM) (false non-match) et de fausses correspondances (FM) (false match). Le FM s'agit de la probabilité attendue qu'un échantillon soit déclaré à tort comme correspondant à un seul modèle sélectionné au hasard. Le FNMR s'agit de la probabilité attendue qu'un échantillon soit déclaré à tort de ne pas correspondre à un modèle de la même mesure provenant du même utilisateur que celui qui a fourni l'échantillon.

2.6 Modalités biométriques utilisé pour la reconnaissance

2.6.1 Reconnaissance faciale

La reconnaissance faciale implique la création d'un modèle à partir de la distribution spatiale et géométrique des traits du visage. La reconnaissance faciale compare deux images (le modèle et la requête) à l'aide d'un algorithme similaire à celui de la reconnaissance des empreintes digitales.

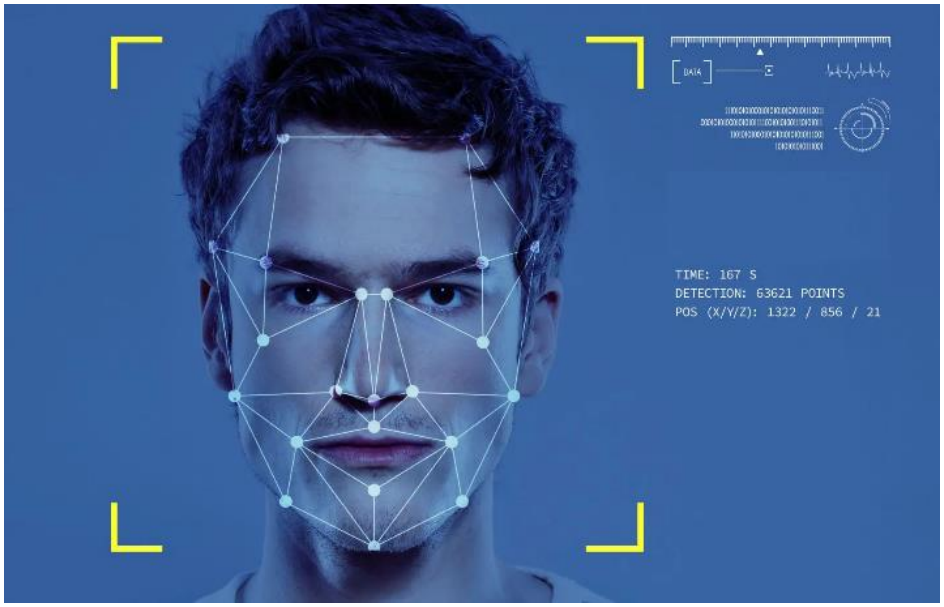

Figure 14 : La reconnaissance de visage (Gagnon-Turcotte, 23)

La reconnaissance de visage repose sur la capture d'une photographie du visage de l'utilisateur par un appareil photo, ensuite, un algorithme convertit la photographie en un modèle numérique en comparant les distances entre les caractéristiques du visage du sujet, telles que la relation entre les yeux, le nez, les lèvres et le menton, voire la figure 15. Les modèles d'images créés par les algorithmes peuvent être stockés sur une puce électronique dans un document ou une carte d'identité (Smith et al., 2018).

Figure 15 : La reconnaissance faciale est une extension de la cartographie faciale, un algorithme est utilisé pour positionner, extraire, numériser et comparer la disposition des traits du visage (Smith et al., 2018).

2.6.2 Thermogramme faciale

La quantité de chaleur émise par les différentes parties du visage caractérise chaque individu. Elle dépende de la localisation des veines, l'épaisseur de squelette, la quantité de tissu, la quantité de muscles et la graisse. L'appareil d'acquisition est un appareil photo fonctionnant dans la bande infrarouge (Florent Perronnin, 2002).

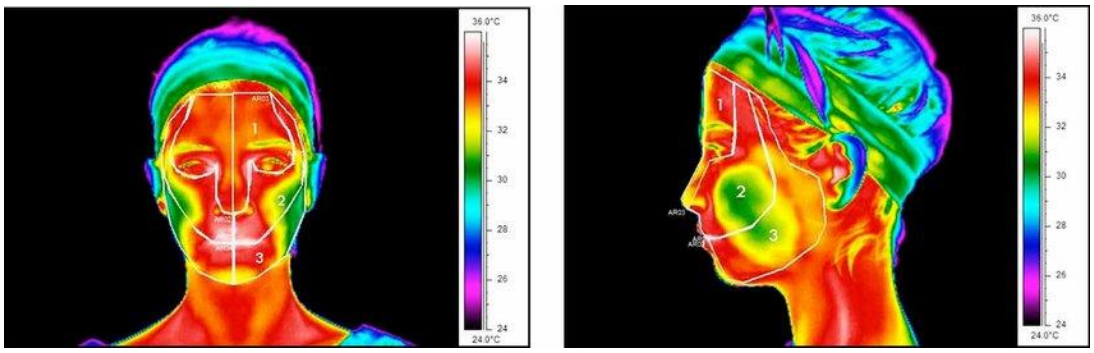

Figure 16 : La reconnaissance à thermogramme faciale (Brioschi, 2023)

L'avantage de cette méthode est qu'il ne dépende pas de la quantité de lumière, l'acquisition peut être faites pendant la nuit que dans la journée. La reconnaissance à thermogramme est cependant sensible à la pose de l'utilisateur, son état émotionnel et sa température corporelle(Papathanasaki et al., 2022). Ces facteurs diminuent l'efficacité du système.

2.6.3 Empreintes digitales

Une empreinte est formée par des crêtes (ridges) et les vallées (furrow) présentes sur la surface du bout des doigts. Les crêtes sont les lignes noirs et les vallées sont les lignes blanc, voire la figure 17. Les empreintes nous aident à saisir les objets. Elles sont complètement formées vers le 7e mois du développement du fœtus et ne changent plus par la suite tout au long de la vie d'une personne.

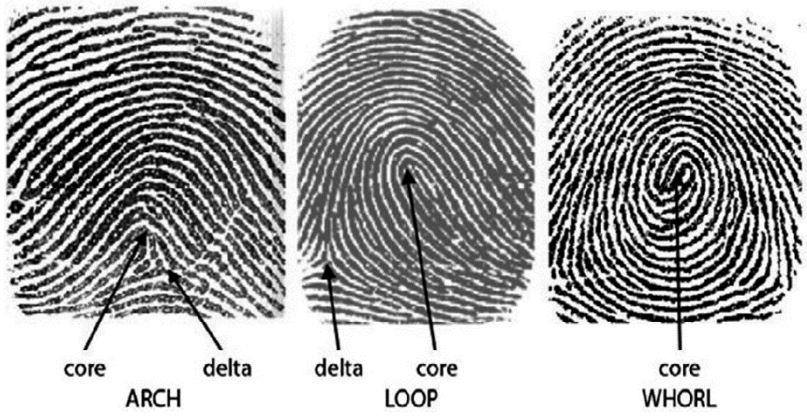

Figure 17 : (a) Les trois types des empreintes l'arche (Arch), boucle (Loop) et tourbillon (Whorl). Les lignes noires représentent les crêtes, les lignes blanc représentent les vallées. Le centre d'un motif est décrit comme le noyau et les points de discontinuité dans les crêtes de l'empreinte digitale sont appelés minuties ou points caractéristiques. (Smith et al., 2018)

2.6.3.1 Acquisition de l'empreinte

Figure 18 : Des empreintes acquises par la technique de l'encre (mobilefingerprintingsolutions, 23)

La technique la plus ancienne consiste à couvrir le bout du doigt d'une fine couche d'encre et à l'imprimer sur une feuille de papier, ensuite l'empreinte imprimée est numérisée, voire la figure 18. L'acquisition numérique se fait par voie d'un capteur optique (Emiko Sano, 2006), le capteur thermique, le capteur électromagnétique, le capteur à ultrasons et le capteur capacitive(Jain et al., 2011) ,voir la figure 19. La qualité d'un scanner d'empreintes digitales, la taille de sa zone de détection et sa résolution déterminent fortement la qualité d'une image d'empreintes digitales.

Lors de la capture d'un query, le modèle ainsi créer est affecté par des variations du processus du mesurage. La position et l'orientation de scanneur peut influer trop sur la construction de la forme du modèle. D'autres facteurs influent sur la forme de modèle prélevé par le capteur, on note l'humidité autour de l'empreinte, la variation de la pression exercée par l'utilisateur entraine des déformations, les blessures permanentes ou temporaires, les personnes âgées et les travailleurs manuels ont des empreintes dégradées. En plus, 4% de la population n'ont pas des empreintes d'assez bonne qualité pour être correctement identifiés (Florent Perronnin, 2002).

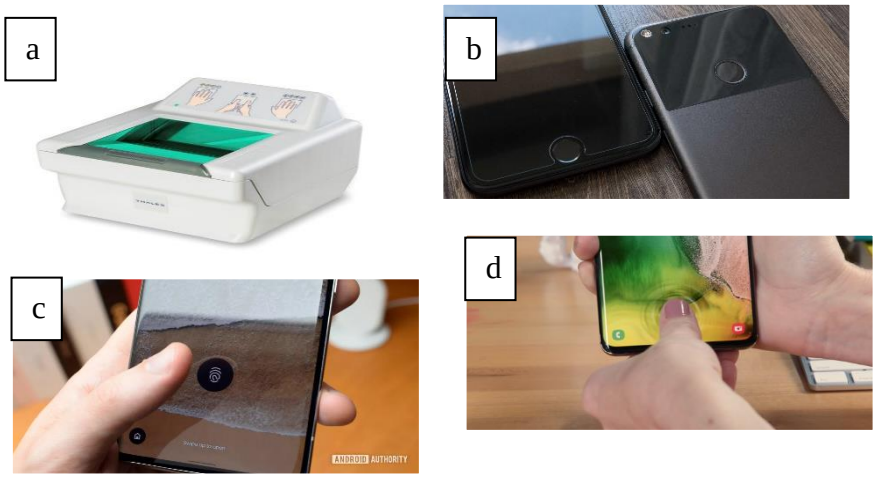

Figure 19 : (a) Le scanneur optique DactyScan84c fabriqué par Thales (www.thalesgroup.com, 2023), (b) un lecteur d'empreinte digitale capacitive (Daley, 2023) (c) un lecteur d'empreinte optique (Triggs, 2023) (d) un lecteur d'empreinte ultrason (Lloyd, 2023)

2.6.3.2 Les minuties

Les caractéristiques importantes utilisées pour identifier un individu sont les minuties. La reconnaissance se fait à partir des minuties. Les minuties ces les propriétés locales des crêtes. L'endroit où une crête émerge, se termine, se divise ou fusionne avec une autre crête est appelé

une minutie(Jain et al., 2011). Une minutie possède deux autres propriétés : la direction et le type.

La direction d'une minutie est l'orientation locale de la crête et le type est une bifurcation ou une terminaison. Il y a d'autres types des minuties, voir la figure 20, comme le pont, le lac et l'ile mais les plus utilisées dans la reconnaissance de l'empreinte est la terminaison et la bifurcation. Le modèle de l'empreinte est fait à partir de la position et l'orientation des minuties.

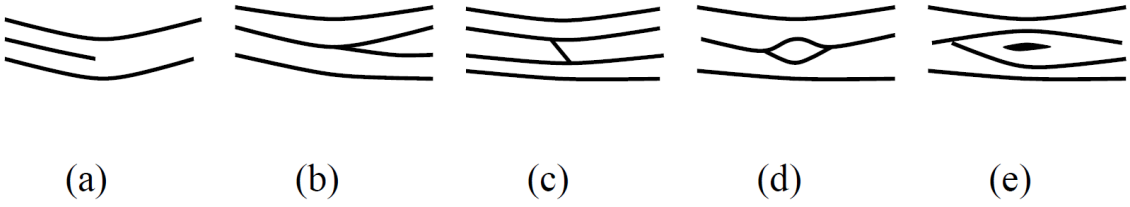

Figure 20 : Différents types des minuties. (a) terminaison (b) bifurcation (c) pont (d) lac et (e) ile (Florent Perronnin, 2002)

2.6.3.3 La mise en correspondance des minuties

Étant donné un ensemble de minuties de requête Y^Q et un ensemble de minuties de modèle Y^M le processus de mise en correspondance comporte trois étapes : l'alignement, la correspondance et la génération de scores, voire la figure 21. Lors de l'alignement, les deux ensembles de minuties ont des orientations géométriques différentes et doivent être transformés de manière à ce qu'ils se trouvent dans le même système de coordonnées.

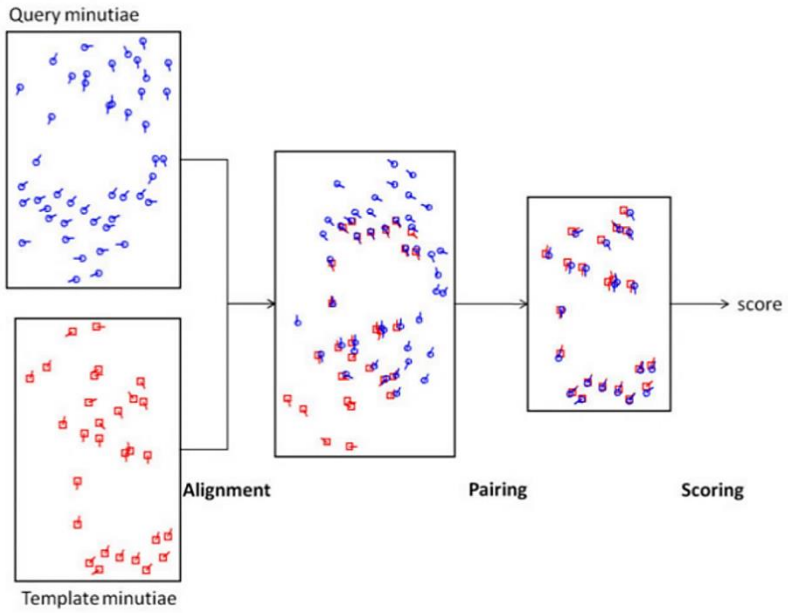

Figure 21 : Calcul d'un score de correspondance entre les minuties de requêtes (query) et les minuties de modèle (Template) stocké dans le système (Jain et al., 2011)

Une fois l'alignement réussi, l'étape suivante consiste à établir la correspondance entre les deux ensembles de minuties. Ensuite, un score est généré sur la base des minuties correspondants. Un utilisateur légitime a un plus grand nombre de points de minuties correspondants qu'un imposteur, d'où un score de correspondance plus élevé, voire la figure 22.

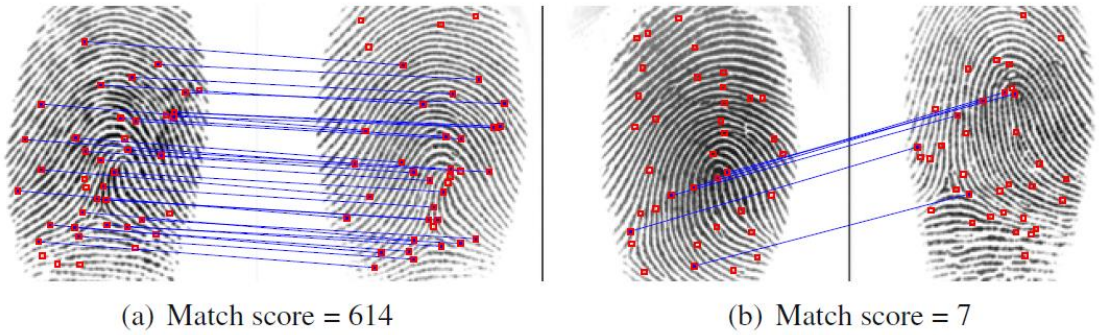

Figure 22 : Comparaison d'empreintes digitales par un comparateur commercial. (a) Une paire d'empreintes digitales authentiques avec 31 points caractéristiques concordants, et (b) une paire d'imposteurs avec 6 points caractéristiques concordants. Les points caractéristiques correspondants entre les deux images sont reliés par des lignes. Le score de correspondance est calculé en fonction du nombre de points caractéristiques concordants et d'autres paramètres qui sont propres à l'outil commercial.(Jain et al., 2011)

Les empreintes digitales sont toutefois vulnérables à l'usurpation d'identité. Sur chaque objet que nous touchons, nous laissons des empreintes digitales. Une empreinte digitale peut être relevée et, un doigt gommeux et dans certains cas violents, le doigt d'une personne peut être coupé et utilisé pour tromper le système (Jain, 2012). La vérification des empreintes digitales n'est pas recommandée pour les applications autonomes (stand-alone applications).

2.6.4 La rétine

L'utilisation de la rétine pour la vérification consiste la reconnaissance des motifs formée par les veines sous la surface de la rétine. Le processus de balayage de la rétine implique une cartographie des vaisseaux sanguins à l'arrière de l'œil. Le scanner nécessite une machine spécialisée, et non une simple caméra (Faundez-Zanuy, 2006).

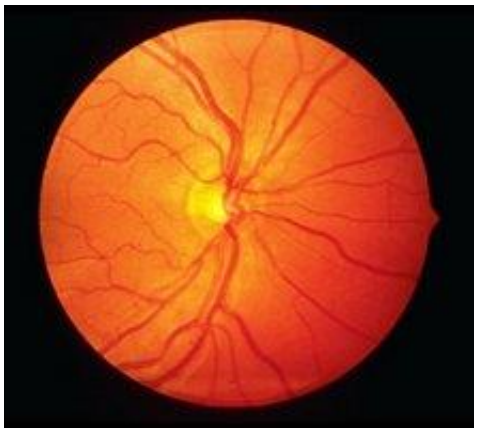

Figure 23 : La rétine de l'œil (www.journaldunet.com, 2023)

Les scanners rétiniens sont très coûteux, ce qui limite le balayage rétinien à des applications de très haute sécurité. Ils sont uniques et stables dans le temps. La reconnaissance de la rétine est considérée comme une de méthodes les plus sures à cause de sa stabilité. Certaines maladies peuvent affecter la structure des veines de la rétine, raison pour laquelle cette procédure est mal accepté car les utilisateurs craints que leur maladie soit dévoilée.

2.6.5 L'iris

L'iris est la région annulaire situé entre la pupille est le blanc de l'œil. Les motifs de l'ris se forme au cours de deux premières années de la vie et ils sont stables au-delà. Les iris sont uniques et les iris d'un même individu sont différents (Florent Perronnin, 2002).

Figure 24 : L'iris est la région colorée de l'œil. Elle se situe entre la pupille et le blanc de l'œil (Mattis2412, 2023)

L'iris n'est pas modifiable par l'intervention chirurgicale. Elle est considérée comme le plus fiable méthode de reconnaissance. La probabilité que deux iris d'individus différents correspondent est de 1 personne sur 10^{35}(Hallinan, 1991). La capture de l'iris se fait par une caméra standard ou par un système kiosque (kiosk-based system)(Eng & Wahsheh, 2013).

Les systèmes de reconnaissance de l'iris sont extrêmement précis. Cependant, la technologie utilisée pour l'acquisition de ces modalités est couteuse. La forme de la rétine apporte des informations sur quelques maladies d'un individu. Il s'agit d'une atteinte à la vie privée d'un individu. La procédure de reconnaissance est gênante pour l'utilisateur. Pour ces raisons, la reconnaissance de la rétine et de l'iris sont mal acceptées par le public. Ils sont généralement réservés pour les applications de très haute sécurité.

2.6.6 La géométrie de la main

La reconnaissance de la géométrie de la main repose sur la détermination des caractéristiques de la main d'un individu. Ces caractéristiques englobent, la forme de la main, la longueur, la largeur et la courbure des doigts (Chen Wang, 2020). Le système de reconnaissance est une plaque au-dessus de laquelle nous posons la main pour la reconnaissance. Elle est simple à utiliser. Cependant, cette méthode n'est pas pratique pour les personnes âgées et pour ceux qui ont l'arthrite puisqu'ils n'arrivent pas à étendre la main (Florent Perronnin, 2002). L'acquisition des informations discriminants est faite par la capture d'une photo de la main par un appareil photo numérique.

Les inconvénients de la reconnaissance de la géométrie de la main :

1. La géométrie de la main possède un faible pouvoir discriminant
2. Le système de reconnaissance est facilement trompé par des jumeaux et par les membres de la même famille.

2.6.7 La Voix

La reconnaissance de la voix est très utilisée dans des plusieurs applications mobiles dont les plus reconnu est Siri développé par Apple et Google Assistant développé par Google. Nous pouvons facilement reconnaitre l'identité de quelqu'un à partir du son de sa voix. En ressortissant des informations sur les amplitudes d'un signal vocale les systèmes électroniques peuvent aussi être capable de faire ceci. La reconnaissance de la voix est bien acceptée parce que le signal vocal est naturel à produire.

Toutefois l'utilisation de la voix pour la reconnaissance apporte plus de risque par rapport à la reconnaissance faciale parce qu'elle est susceptible à l'usurpation d'identité(Papathanasaki et al., 2022).

2.6.8 Signature

Les appareils mobiles permettent aux utilisateurs d'utiliser leur signature digitale pour l'authentification de l'utilisateur. Il y a deux modes de reconnaissance de la signature, le mode statique et le mode dynamique (Florent Perronnin, 2002). Le mode statique de reconnaissance utilise que l'information géométrique de la signature. Seul la forme de la signature est utilisée pendant la reconnaissance.

Le mode dynamique de reconnaissance emploie l'information géométrique et l'information dynamique d'une signature. Ici l'information dynamique décrit la vitesse d'accélération et la pression exercé pendant l'écriture d'une signature (Chen Wang, 2020). Le mode dynamique contient beaucoup des informations donc ce mode est plus discriminant. Un imposteur peut falsifier la signature d'un individu mais il ne peut pas falsifier l'information dynamique. La capture d'une signature se fait par une tablette graphique.

L'inconvénient majeur de l'utilisation de la signature est qu'il y a une très grande variabilité entre deux signatures fait par la même personne. La forme d'une signature est beaucoup affectée par la santé et l'état émotionnel d'un individu.

2.7 Comment améliorer la performance d'un système biométrique ?

- Nous pouvons ajouter un autre facteur à la reconnaissance par une biométrie, une possession. Le problème avec ce dernier ce qu'il apporte les inconvénients de l'utilisation d'une possession pendant la reconnaissance.

- La multimodalité, qui est défini comme l'utilisation des plusieurs modalités biométriques pour faire la reconnaissance. La multimodalité apporte une amélioration de la performance du système au côté de la précision et son efficacité notamment en mode identification.

2.8 Applications de la reconnaissance biométrique

- Contrôle des frontières
- Contrôle d'accès physique
  Ici on authentifie un utilisateur qui cherche à accéder à un lieu sécurisé.
- Contrôle d'accès virtuel
  Ici on authentifie un utilisateur qui cherche à accéder à une ressource ou un service. D'ici on comprend les sites web, les réseaux d'ordinateurs …etc.
- La banque en ligne
  Il s'agit d'une vérification de transfert de fonds par la biométrie
- Accès aux informations sensibles
- Accès aux aéroports
- Transactions financières à distance
- La répression
  Dans le domaine de la criminologie, l'ADN (acide désoxyribonucléique) et les empreintes latentes prélevés d'une scène d'un crime sont utiliser pour identifier un criminel.

2.9 Conclusion

L'utilisation de mots de passe n'est plus sécurisée dû à des inconvénients de celui-ci discuté auparavant. Pour améliorer la sécurité d'une application en plus, au facteur de mot de passe nous rajoutons une modalité biométrique.

CHAPITRE 3

Réalisation d'une application web d'authentification à double facteur biométrique

3.1 Introduction

Dans cette étude nous allons garantir la sécurité d'une page web avec une authentification à double facteur biométrique. Le premier facteur d'authentification que nous avons utilisé repose sur une connaissance, un nom d'utilisateur (l'email d'un individu) et un mot de passe. Le deuxième facteur d'authentification comprend une des deux modalités biométriques disponible sur la plupart des smartphones, la reconnaissance de l'empreinte digitale et la reconnaissance faciale. Si un utilisateur a configuré l'empreinte digitale comme paramètre de la sécurité de son téléphone, ce modèle sera utilisé comme le deuxième facteur d'authentification. Sinon, s'il a configuré la reconnaissance faciale, le modèle de son visage sera utilisé comme le deuxième facteur d'authentification.

Notre solution décrit trois composants distincts, voire la figure 34, une application mobile que nous avons créée (**BiometricAuthentification**), une base des données **Firestore Database**, voire la figure 38, et une application web que nous avons créé (**webpageauthentication**). L'application web traite les deux étapes d'authentification successivement. Lors d'un login (sign in), l'utilisateur ayant un compte déjà existant dans la base des données fournisse ses identifiants de connexion. A la suite, l'application web vérifie s'il existe dans la base de données. S'il existe, il passe à la deuxième étape de vérification.

Dans la deuxième étape de vérification, l'utilisateur est prié de fournir sa biométrie au niveau de l'application mobile. Si la reconnaissance de la biométrie est réussie, l'utilisateur complet le processus d'authentification et il passe à la page web (page de Welcome).

La base des données Firestore Database s'occupe de la stockage des identifiants de connexion pour divers utilisateurs. Il stocke aussi une variable appelée **biometricLogInStatus** qui permet de suivre si l'authentification biométrique est réussie. Pour une authentification réussie il prend la valeur **true**, dans le cas contraire il prend une valeur **false**. Le passage vers la page web s'effectue si et seulement si **biometricLogInStatus** est égal à **true**.

3.2 Les langages et les outils du développement

3.2.1 Les langages du développement

3.2.1.1 React

React (ou ReactJS) est une bibliothèque javascript pour la construction d'interfaces utilisateurs développé par Facebook. React est open source et maintenu par Facebook. Lors de sa première apparition, React a d'abord été utilisé pour construire des interfaces utilisateur pour des applications web. Aujourd'hui, il est également utilisé pour créer des applications côté serveur et des applications mobiles.

3.2.1.2 React Native

React Native est un Framework permettant de créer des applications mobiles natives en JavaScript à l'aide de la bibliothèque JavaScript React. Le code React Native se compile en véritables composants natifs. Les applications construites en React Native peuvent fonctionner à la fois sur iOS et Android.

Les applications Android traditionnelles sont écrites en Java et Kotlin. Quant aux applications iOS traditionnelles, Swift et Objective-C sont utilisés pour écrire ces applications. React Native nous permet d'écrire des applications qui sont indépendantes de la plateforme (cross-platform development) et il permet ainsi un cout de développement moins cher. React Native nous permet d'écrire des applications entièrement en javascript et JSX. Des exemples d'applications écrites en React Native sont Facebook, Instagram, Pinterest, Skype et Uber Eats.

3.2.1.3 JSX

JSX (Javascript XML) est un langage de balisage déclaratif utilisé pour définir la disposition d'un composant React. C'est une combinaison des trois éléments Javascript, HTML et XML. JSX revient à écrire une ligne HTML en javascript, sans les guillemets <html>. Il permet l'utilisation de code javascript dans ses balises et il sera compilé en code javascript compatible avec le navigateur lors de l'exécution. Il n'est pas obligatoire d'utiliser JSX dans votre code React Native mais il est conseillé de le faire car cela rend votre code moins verbal.

3.2.2 Les outils du développement

3.2.2.1 Nodejs

Nodejs est un moteur d'exécution javascript asynchrone piloté par les événements, conçu pour construire des applications réseau évolutives. Il est essentiel pour héberger et faire fonctionner un serveur web pour une application React (Kasundra, 2023). Nodejs regroupe une application React dans un seul fichier pour faciliter la compilation à l'aide de Webpack et de plusieurs autres modules Node.

Figure 25 : Node.js est un environnement d'exécution JavaScript multiplateforme et open-source (Miklashonok, 2023).

3.2.2.2 NPM

Npm est l'acronyme de node package manager (gestionnaire de paquets node). Il s'agit de la plus grande bibliothèque de logiciels au monde (registre), d'un gestionnaire de paquets de logiciels et d'un installateur. L'utilisation du registre npm est gratuite et comprend plus de 800 000 paquets de code. Vous pouvez télécharger tous les paquets de logiciels publics npm sans inscription ni connexion (https://www.w3schools.com, 2023).

Npm comprend un client de ligne de commande (CLI) qui peut être utilisé pour télécharger et installer des logiciels.

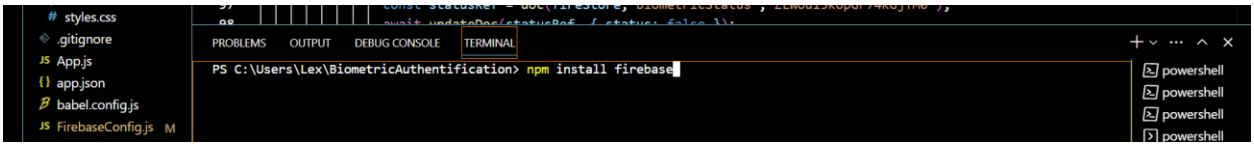

Figure 26 : Installation de Firebase à travers npm

Npm est installé avec Nodejs. Pour installer npm, vous devez installer Nodejs sur votre ordinateur. Npm est également un gestionnaire de paquets pour Nodejs. Tous les paquets npm sont définis dans des paquets appelés « package.json ». Le contenu de « package.json » doit être écrit en JSON.

Npm peut gérer les dépendances (dependencies). En une seule ligne de commande, il peut installer toutes les dépendances d'un projet. Les dépendances sont définies dans le fichier package.json.

3.2.2.3 Visual Studio Code

Dans notre projet nous avons utilisé l'environnement de développement intégré VS code pour développer nos applications React. Il offre des extensions utiles pour faciliter un développement vite et efficace.

3.2.2.4 Firebase Firestore

Cloud Firestore est une solution de base de données flexible et évolutive conçue pour le développement d'applications mobiles, web et serveur, offerte par Firebase et Google Cloud. Il partage des similitudes avec Firebase Realtime Database en ce sens qu'il permet la synchronisation des données entre les applications clientes grâce à des écouteurs en temps réel. De plus, il offre une prise en charge hors ligne pour les appareils mobiles et les applications Web, ce qui vous permet de créer des applications réactives qui peuvent fonctionner même en l'absence de connexion Internet ou en présence d'une latence réseau élevée.

3.2.2.5 Webpack

Webpack est un outil de regroupement de modules statiques pour les applications JavaScript modernes. Lorsque webpack traite votre application, il construit en interne un graphe de dépendances à partir d'un ou plusieurs points d'entrée et combine ensuite chaque module dont votre projet a besoin dans un ou plusieurs bundles, qui sont des actifs statiques à partir desquels vous pouvez servir votre contenu.

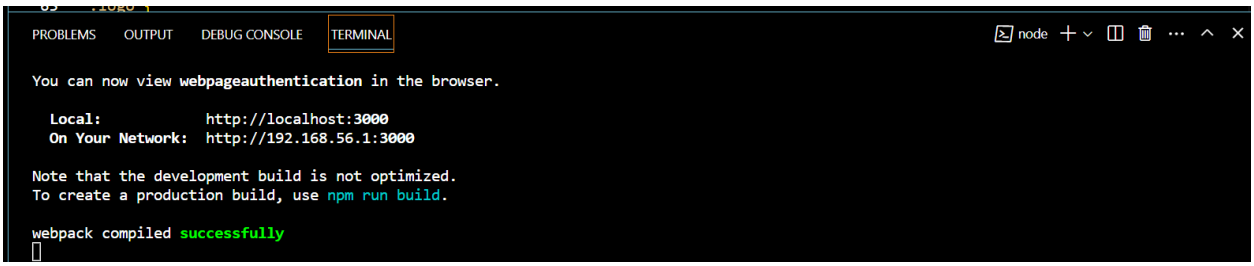

Figure 27 : Compilation automatique de code source de l'application web à travers webpack

3.2.2.6 Metro bundler

Metro bundler est un bundler javascript pour React Native. Il compile tous nos fichiers javascript en un seul fichier.

Figure 28 : Compilation automatique de code source de l'application mobile BiometricAuthentification à travers Metro bundler

3.3 Création des applications React Native

Il y a deux façons de créer des applications React Native :

1. Expo CLI

2. React Native CLI

Expo CLI s'appuie sur React Native. Il masque les complexités du développement d'applications, ce qui rend la création d'applications plus rapide. React Native CLI est un outil très complexe utilisé principalement par les développeurs d'applications professionnels qui ont de l'expérience avec les environnements iOS et Android.

Dans notre projet nous avons utilisé Expo CLI pour la réalisation de notre application mobile BiometricAuthentification.

3.3.1 Installation d'expo-cli

Pour tester et exécuter notre projet pendant le développement, nous allons utiliser Expo Go depuis le Google Play Store. Expo Go est une plateforme qui nous permet de développer et tester des applications mobiles écrit avec javascript et React Native. Expo Go nous permet d'exécuter notre application sur nos appareils physiques. Nous pouvons également partager notre application avec d'autres développeurs dans le monde via Expo Go.

Figure 29 : Installation d'Expo CLI à travers npm

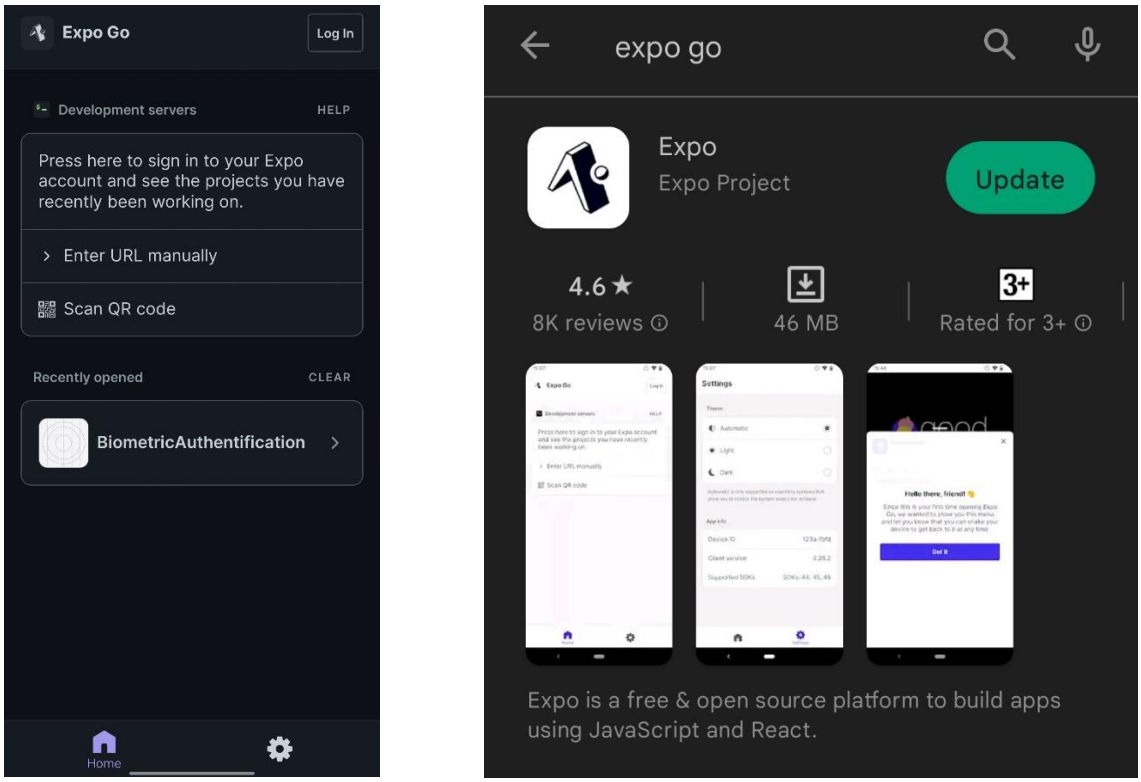

Figure 30 : Nous avons utilisés Expo Go pour développer, tester et visualiser notre application React Native. Expo Go peut etre télecharger depuis Google Play Store

3.3.2 Création de l'application mobile BiometricAuthentification

Pour créer notre application mobile on va saisir la commande suivante :

Figure 31 : Création de notre application mobile BiometricAuthentification avec l'invite de commande Windows (command prompt)

A la suite, on sélectionne le premier modèle :

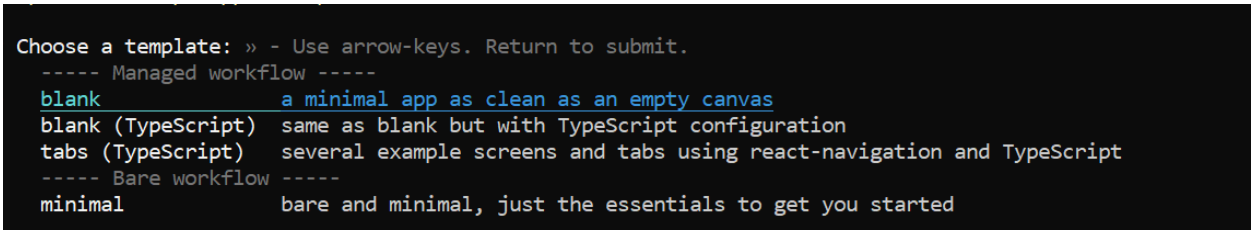

Figure 32 : Nous avons utilisé un managed workflow qui installe automatiquement les dépendances du développement

3.3.3 Création de l'application web webpageauthentication

Pour créer notre application mobile on va saisir la commande suivante :

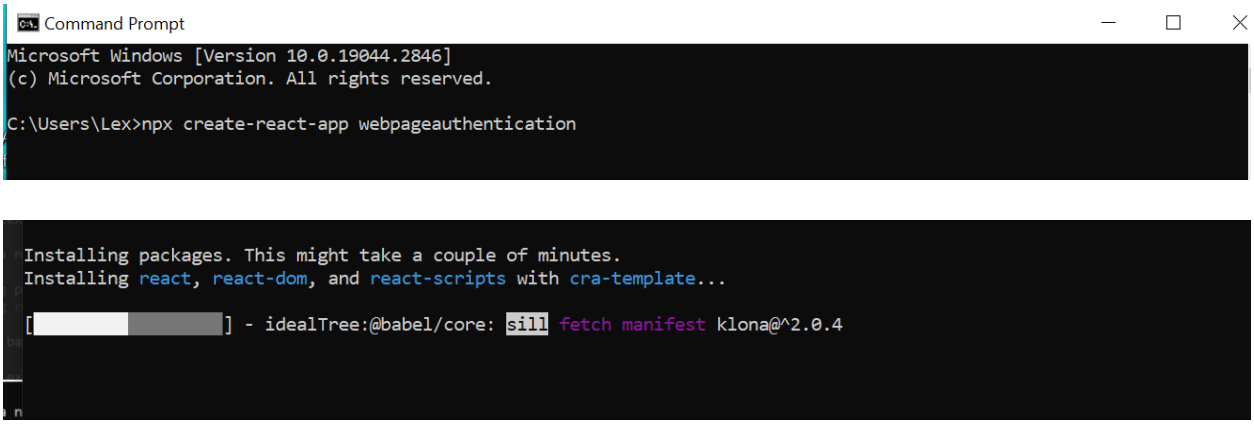

Figure 33 : Création de l'application web à travers npx

3.4 Architecture du système de vérification à deux étapes

Nous avons créé une application web **(webpageauthentication)** et une application mobile **(BiometricAuthentification)** relié entre eux à travers de la base des données Firestore comme montré dans la figure 34. Le téléphone de l'utilisateur s'occupe de la reconnaissance de l'individu par voie de l'empreinte digitale ou de la reconnaissance faciale en fonction de modèle biométrique déjà inscrit dans le système de sécurité Android. Les modèles biométriques sont stockés dans le système Android et le processus de mise en correspondance se passe localement. Le principe de fonctionnement de l'application mobile est détaillé dans le tableau 3.

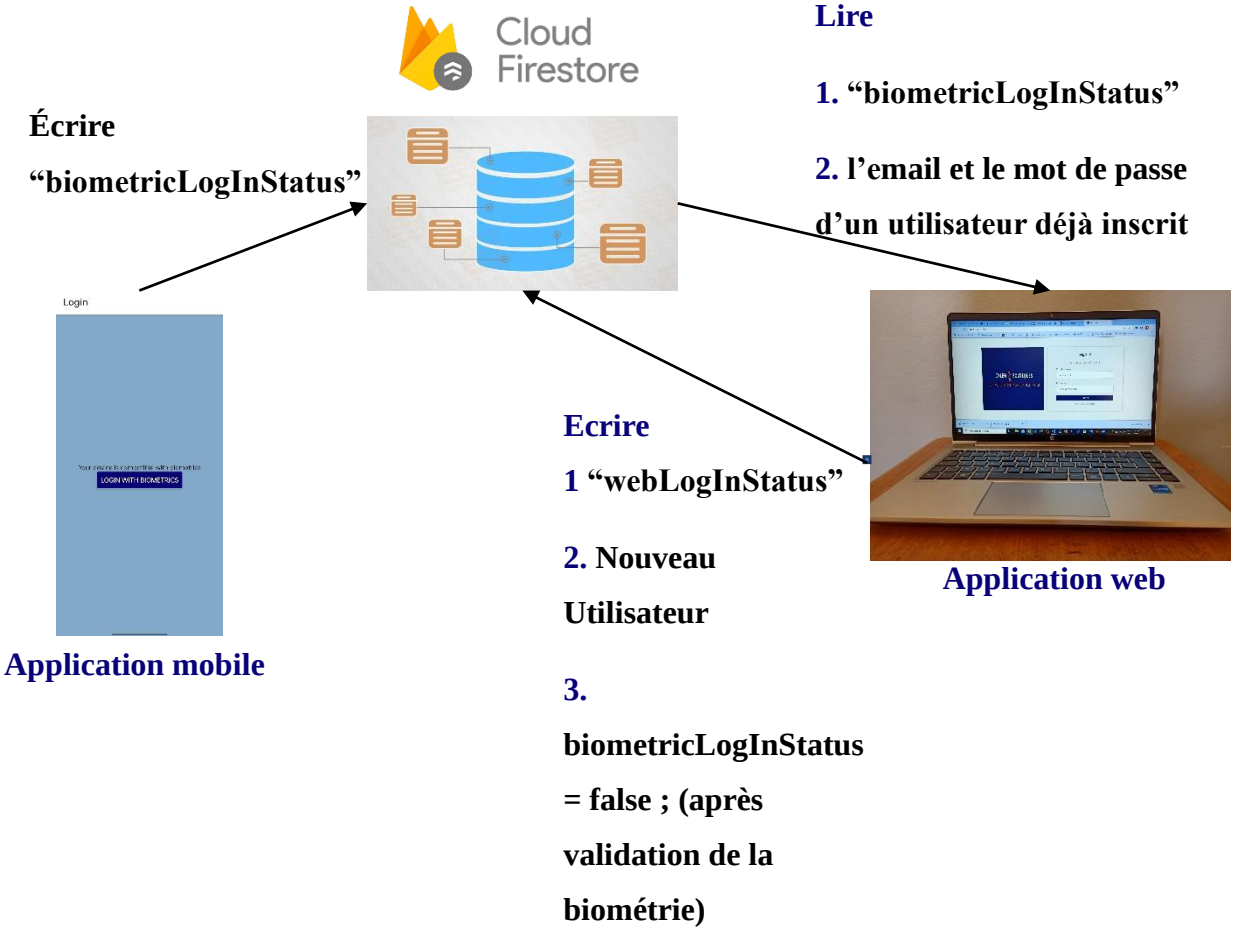

Figure 34 : L'architecture de notre solution de vérification à deux étapes

L'application web s'occupe de la connexion de l'utilisateur et de l'inscription d'un nouvel utilisateur, voire la figure 40. Son principe de fonctionnement est détaillé dans le tableau 4.

- **But :** Accéder à la page de Welcome de l'application web
- **Préconditions :** l'utilisateur doit avoir un compte déjà existant sinon il doit s'inscrire
- **Etape 1 :** l'utilisateur doit faire un login par email et mot de passe
- **Etape 2 :** l'utilisateur doit faire la reconnaissance de sa biométrie (empreinte ou visage)

Si et seulement si, ces deux étapes sont complétées avec succès, l'utilisateur peut accéder à la page web (page de Welcome).

3.4.1 Déroulements des événements (application mobile)

Action	Résultat
1. Reconnaissance de visage ou reconnaissance de l'empreinte	**2.** Correspondance ou non-correspondance
3. Ecriture de résultat de mise en correspondance dans Firebase Firestore	**4.** En cas de correspondance la variable **biometricLogInStatus** prend la valeur **true,** l'application se dirige vers la page « Authentication Successful », voire la figure 35. En cas de non-correspondance la variable **biometricLogInStatus** prend la valeur **false,** l'application se dirige vers la page « Authentication has Failed », voire la figure 35.

Tableau 3 : Principe de fonctionnement de l'application mobile

Le fonctionnement de l'algorithme de l'application mobile « BiometricAuthentification » est bien détaillé dans un diagramme de flux, voire la figure 36.

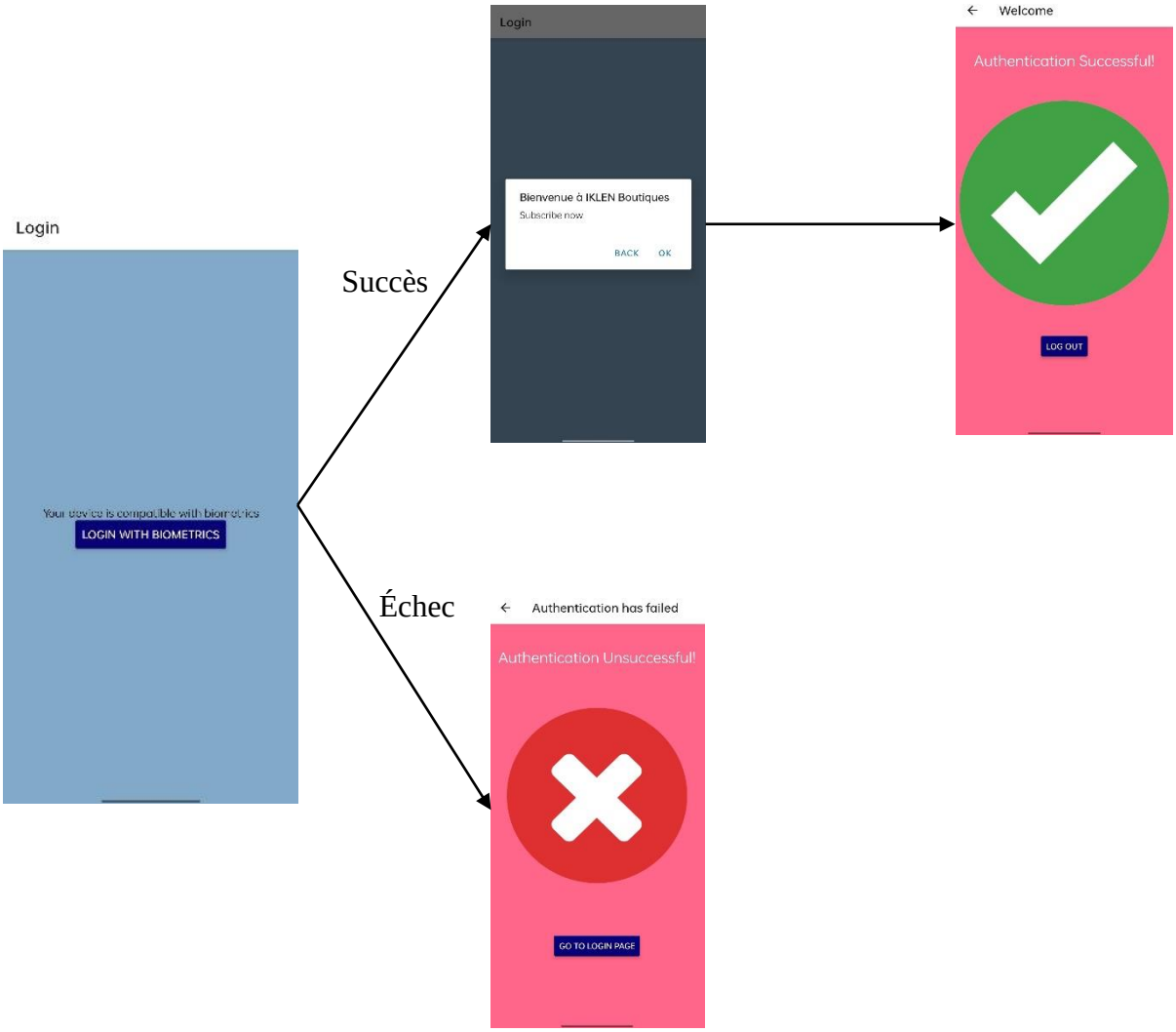

Figure 35 : les différentes pages de notre application mobile BiometricAuthentification

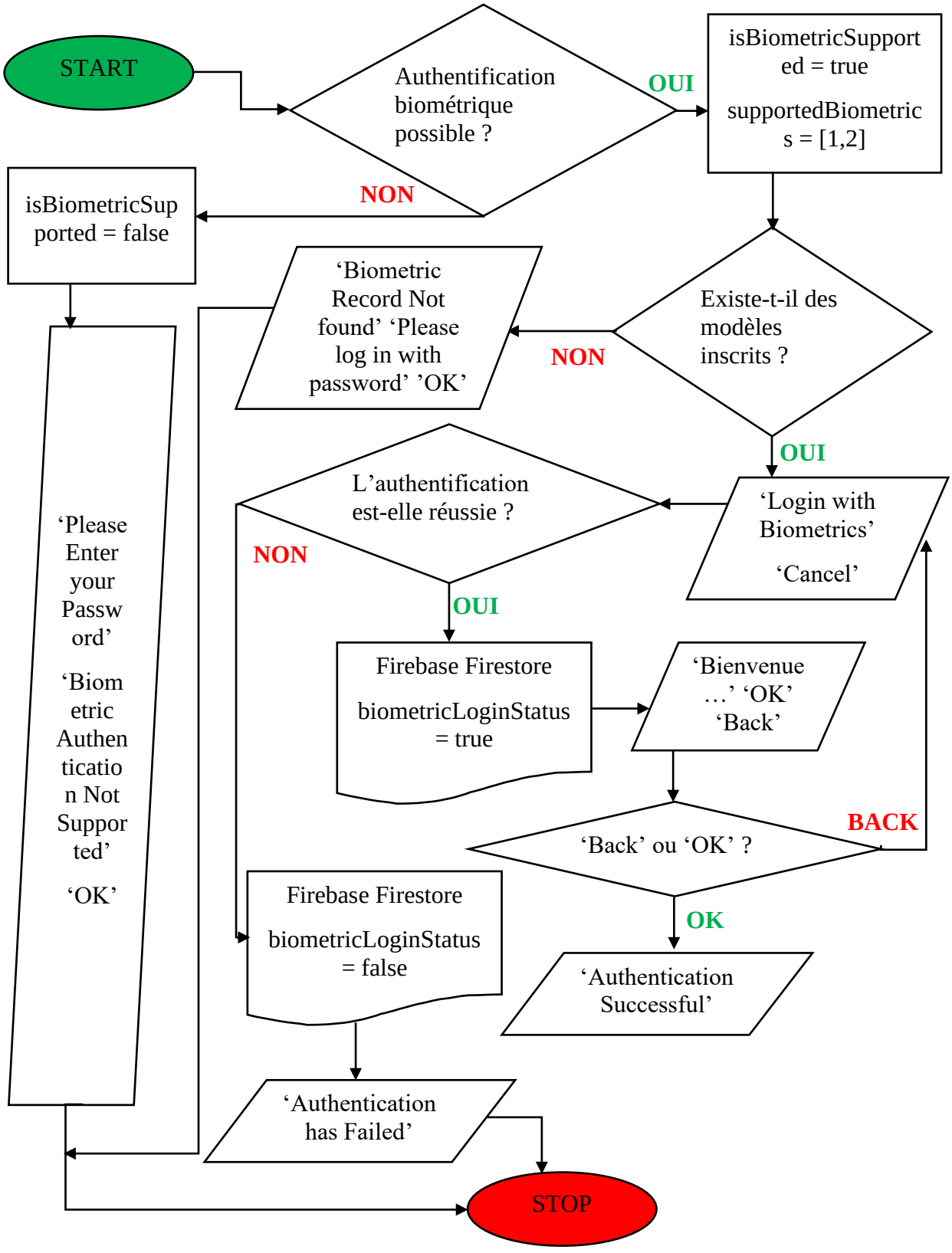

Figure 36 : Diagramme de flux de l'algorithme de l'application mobile

3.4.2 Déroulements des événements (application web)

Action	Résultat
1. L'utilisateur saisie son email et son mot de passe dans la page Sign In	2. L'application Web vérifie dans la base des données si cet utilisateur existe
	3. Si l'utilisateur **n'existe pas** l'application affiche une alerte **'incorrect username or password'**, l'utilisateur doit faire une inscription, voire la figure 39. Si l'utilisateur **existe**, l'application se dirige vers la **page de validation**. Elle demande l'utilisateur de présenter une biométrie au niveau de son téléphone, voire la figure 37.
4. L'utilisateur présente sa biométrie au niveau de son téléphone	
	5. L'application web écoute dans la base des données pour un changement de variable **biometricLogInStatus.** Si cela change vers **true,** la deuxième étape de vérification est complétée. L'utilisateur est dirigé vers la page Welcome. Dans le cas de **false**, l'utilisateur reste sur la page de validation.

Tableau 4 : Principe de fonctionnement de l'application web

Le fonctionnement de l'algorithme de l'application web « webpageauthentication » est bien détaillé dans un diagramme de flux, voire la figure 41.

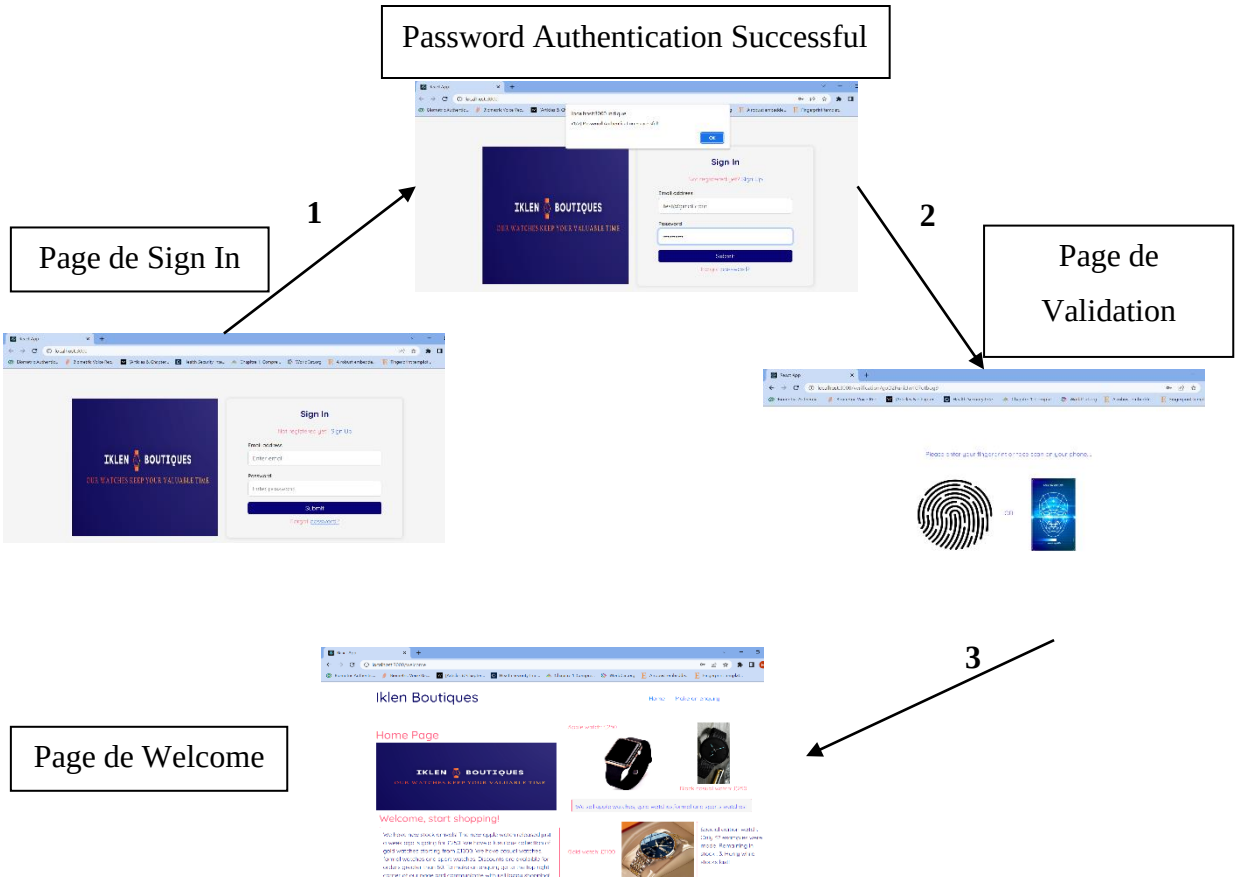

Figure 37 : Les balayages entre les différents pages de l'application dans le cas d'une authentification réussie.

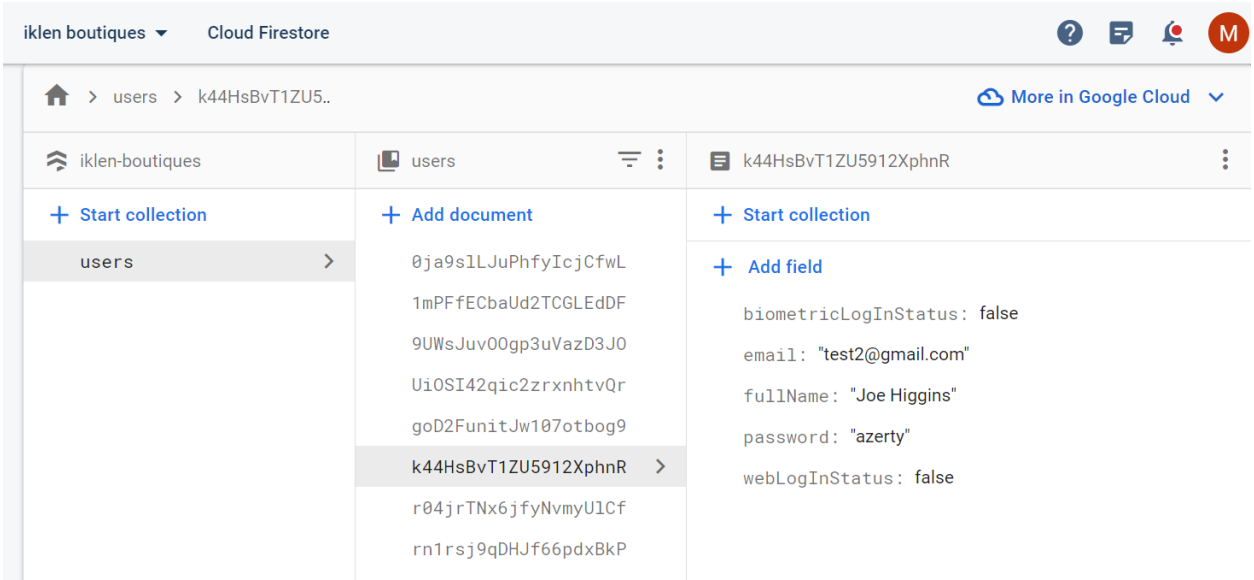

Figure 38 : Dans la base de données de Firestore nous avons un répertoire de tous les utilisateurs appelé users. Chaque utilisateur possède des champs décrivant ses identifiants des connexions et des informations supplémentaires à son compte.

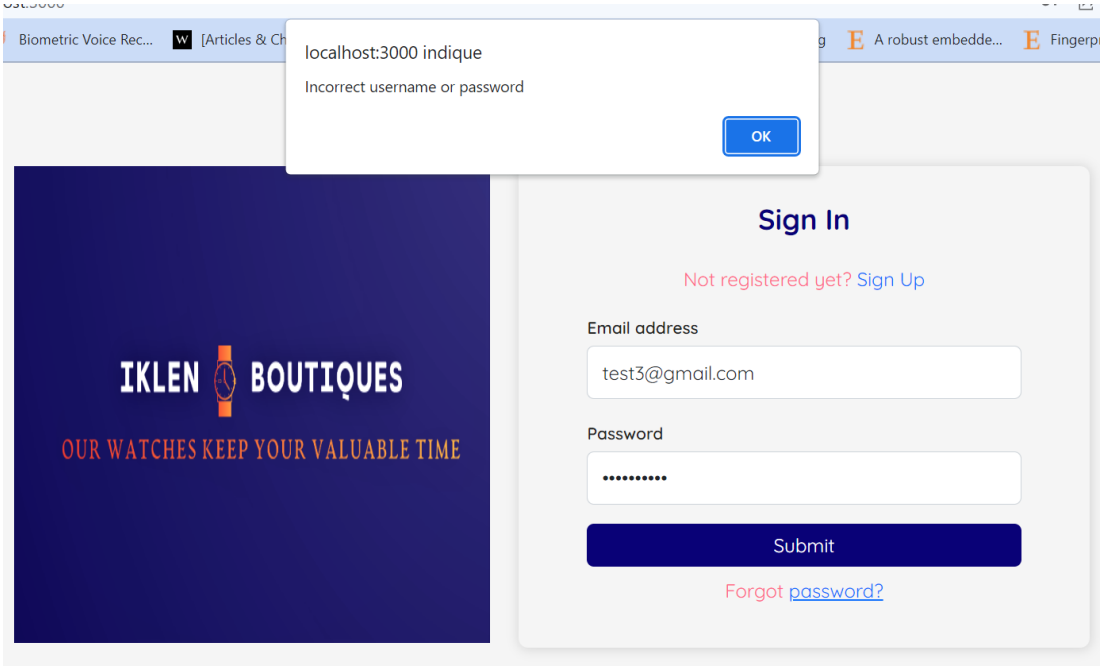

Figure 39 : Si l'utilisateur n'est pas dans la base de données l'application affiche 'incorrect username or password'. Soit le mot de passe et l'email saisies sont incorrect ou ce compte n'existe pas totalement.

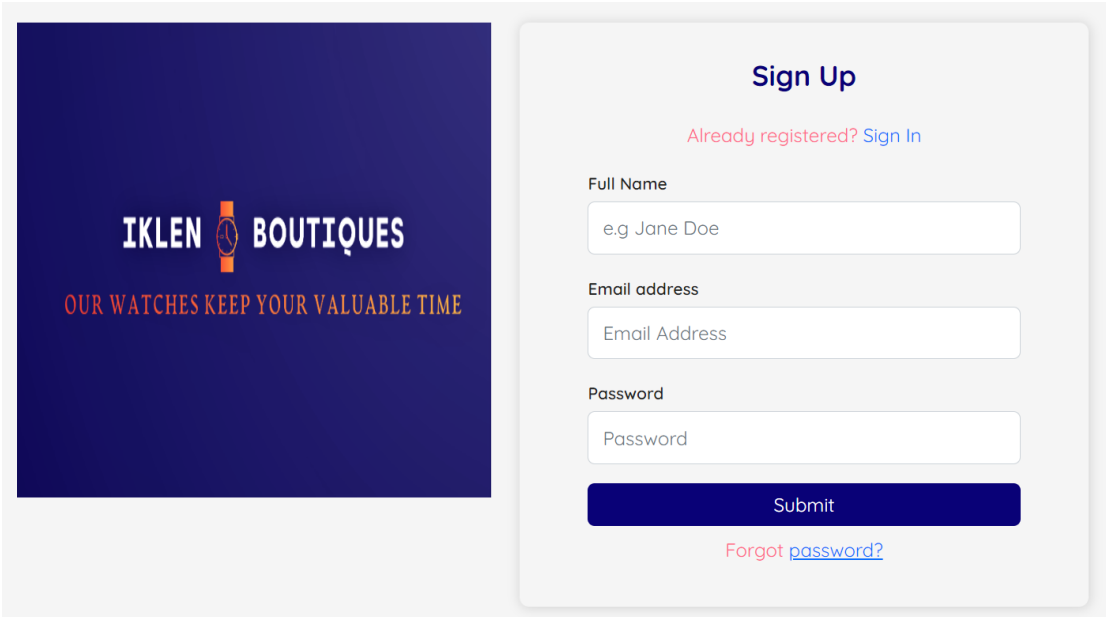

Figure 40 : Dans le cas où l'utilisateur n'a pas un compte il doit faire l'inscription

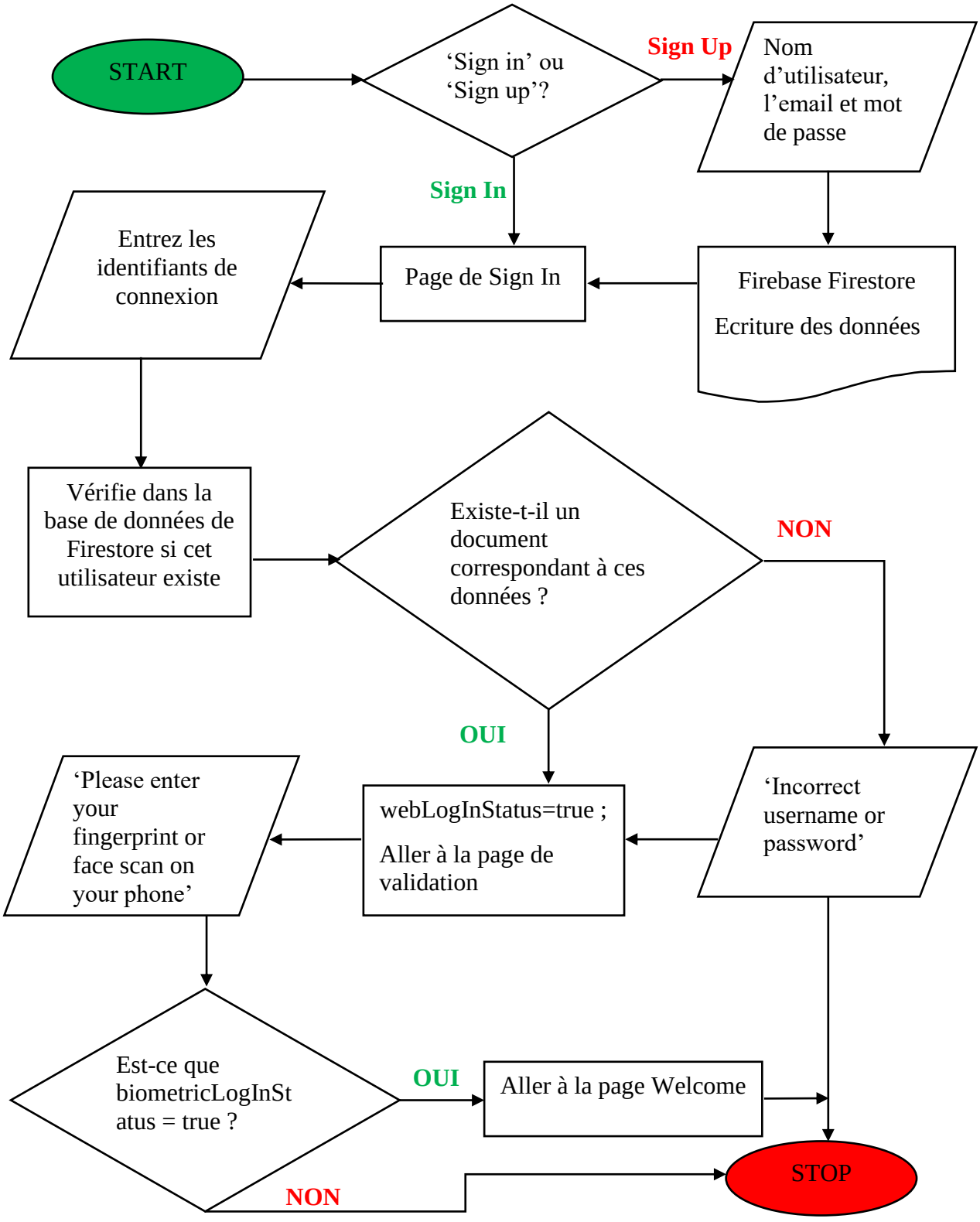

Figure 41 : Diagramme de flux de l'algorithme de l'application web

3.5 Conclusion

Nous avons réussi à créer un processus de connexion à une application web (webpageauthentication) qui utilise l'authentification biométrique à deux facteurs. Nos algorithmes utilisent les deux techniques biométriques les plus populaires en matière de sécurité des smartphones, à savoir la reconnaissance des empreintes digitales et la reconnaissance faciale. L'utilisation de l'une ou l'autre biométrie dans le processus d'authentification dépend de la biométrie que l'utilisateur a configurée dans son système de sécurité Android.

La première étape de vérification de notre processus d'authentification à deux facteurs est la reconnaissance de l'adresse électronique et du mot de passe de l'utilisateur. Une fois cette étape franchie avec succès, nous passons à la deuxième étape de vérification. Lors de cette dernière étape, il est demandé à l'utilisateur de présenter son empreinte digitale ou faciale dans l'application mobile que nous avons créée, BiometricAuthentification. Une fois la vérification réussie, l'utilisateur a accès à la page web d'accueil intitulée Iklen Boutiques.

Conclusion générale

Il n'est plus sûr d'utiliser des mots de passe comme seule mesure de sécurité pour protéger nos comptes en ligne. Les mots de passe peuvent être oubliés, perdus, partagés ou devinés par un imposteur. Ils sont extrêmement vulnérables aux attaques de phishing, d'ingénierie sociale, de keylogger, de force brute et de dictionnaire. L'utilisation d'un mot de passe pour sécuriser le compte d'un utilisateur est un exemple de système d'authentification à facteur unique. L'ajout d'un deuxième facteur d'authentification, tel qu'un identifiant biométrique, est appelé authentification à deux facteurs.

Nous avons démontré un système d'authentification biométrique à deux facteurs pour renforcer la sécurité d'un compte en ligne. Outre l'utilisation d'un mot de passe, un identifiant biométrique est nécessaire pour compléter le processus de vérification en deux étapes. L'avantage de l'utilisation de la biométrie est qu'elle est immunisée contre les attaques mentionnées précédemment. Elles élèvent donc considérablement le niveau de sécurité et rendent l'accès à votre compte extrêmement difficile pour les pirates. Les identifiants biométriques sont uniques et naturels pour tout le monde. Ils vous accompagnent en permanence. Même si un pirate informatique intercepte votre mot de passe, il ne peut pas accéder à votre compte sans votre attribut physique (votre identifiant biométrique).

L'authentification biométrique à deux facteurs est une solution très fiable qui offre une grande sécurité aux utilisateurs lorsqu'ils utilisent l'internet. Cette solution réduira considérablement les cyberattaques. Elle contribuera à la protection des bases de données sensibles et renforcera la protection de la vie privée.

Références

Andrew S. Tanenbaum, N. F. (March 3, 2021). *Computer Networks.* Harlow, United Kingdom: Pearson.

Arntz, P. (2023, 04 13). *Is two-factor authentication (2FA) as secure as it seems?* Récupéré sur www.malwarebytes.com: https://www.malwarebytes.com/blog/news/2018/09/two-factor-authentication-2fa-secure-seems

Baran, P. (1964). On Distributed Communications Networks. *IEEE transactions on Communications Systems, vol.12, no. 1*, 1-9.

Barry M. Leiner, V. G. (1997). The Past and Future History of the INTERNET. *COMMUNICATIONS OF THE ACM, Vol 40, No. 2*, 102-108.

Berners-Lee, T. (November 7, 2000). *Weaving the Web : the original design of the World Wide Web by its inventor.* New York, NY, USA: HarperBusiness.

Brioschi, M. (2023, 04 10). *Thermal Evaluation of Myogenous Temporomandibular Disorders and Myofascial Trigger Points in the Masticatory Muscles*. Récupéré sur www.researchgate.net: https://www.researchgate.net/figure/Facial-thermograms-frontal-and-lateral-views-with-the-trigeminal-ROIs-proposed-by-the_fig3_314243052

Chen Wang, Y. W. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks*. Elsevier.

Clarke, R. (2023, 03 30). *HumanID.html.* Récupéré sur http://www.rogerclarke.com/: http://www.rogerclarke.com/DV/HumanID.html

Cohen, B. (2003). Incentives Build Robustness in BitTorrent. *Workshop on Economics of Peer-to-Peer systems 6*, 68-72.

Daley, D. (2023, 04 19). *Front, back or side: Where should a fingerprint sensor be located?* Récupéré sur www.mobilesyrup.com: https://mobilesyrup.com/2017/07/14/front-back-or-side-where-should-a-smartphone-fingerprint-sensor-be-located/

Danièle Dromard, D. S. (2009). *Architecture des réseaux.* Paris, France: Pearson Education France.

DeFigueiredo, D. (2011). The case for mobile two-factor authentication. *IEEE Security & Privacy, 9(5)*, 81-85.

Dmitrienko, A. L. (2014). On the (in) security of mobile two-factor authentication. *In Financial Cryptography and Data Security: 18th International Conference, FC 2014* (pp. 365-383). Christ Church, Barbados: Springer Berlin Heidelberg.

Dostálek, L. (2019). Multi-factor authentication modeling. *9th International Conference on Advanced Computer Information Technologies (ACIT)* (pp. 443-446). IEEE.

Emiko Sano, T. M. (2006). Fingerprint authentication using optical characteristics in a finger. *SICE-ICASE International Joint Conference* (pp. 1774-1777). Busan, Korea: ICASE.

F. E. Heart, R. E. (May 5-7,1970). The Interface Message Processor for the ARPA Computer Network. *spring joint computer conference* (pp. 551-567). New York, NY, USA: Association for Computing Machinery.

Faundez-Zanuy, M. (2006). Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine, 21(6)*, 15-26.

Filippo Ricca, P. T. (2003). Using Clustering to Support the Migration from Static to Dynamic Web Pages. *11th IEEE International Workshop on Program Comprehension*, 207-216.

Florent Perronnin, J.-L. D. (2002). Introduction à la biométrie authentification des individus par traitement audio-vidéo. *Revue Traitement du Signal, volume 19, num´ero 4*. BP 193, F-

06904 Sophia Antipolis Cedex: Institut Eur´ecom Multimedia Communications Department.

Gagnon-Turcotte, S. (23, 04 08). *Pour un moratoire sur la reconnaissance faciale*. Récupéré sur https://www.ledevoir.com/: https://www.ledevoir.com/opinion/idees/560815/pour-un-moratoire-sur-la-reconnaissance-faciale

Gilb, J. P. (2005). *The IEEE wireless dictionary.* New York, NY, USA: Standards Information Network IEEE Press.

Goldberg, A. (1988). A history of Personal Workstations. Dans L. G. Roberts, *The Arpanet and Computer Networks* (pp. 141-171). New York, NY, USA: Association for Computing Machinery.

Harvey M. Deitel, P. J. (2001). *INTERNET & WORLD WIDE WEB HOW TO PROGRAM.* Prentice Hall; 2nd edition.

Hocine SAM, A. B. (2022). La monétique comme levier de la finance inclusive : synthèse de l'approche quantitative sur la portée de la carte Edahabia au niveau d'Algérie Poste. *Journal of Business and Trade Economics, Volume: 70 / N°: 70*, 745-760.

https://www.w3schools.com. (2023, 05 01). *What is npm?* Récupéré sur https://www.w3schools.com: https://www.w3schools.com/whatis/whatis_npm.asp

J. Alex Halderman, B. W. (2005). A convenient method for securely managing passwords. *Proceedings of the 14th international conference on World Wide Web* (pp. 471-479). Chiba, Japan.: Association for Computing Machinery.

Jain, A. K. (2012). Biometric authentication: System security and user privacy. . *IEEE Computer Society*, 87-92.

Jill West, J. A. (2018). *Network+ Guide to Networks, Eigth Edition.* Boston, MA, USA: Cengage Learning.

Julie C. Meloni, M. M. (2009). *SamsTeachYourself HTML and CSS in 24HRS.* 800 East 96th Street, Indianapolis, Indiana, 46240 USA: Sams Publishing.

Kahn, V. G. (May 1974). A Protocol for Packet Network Intercommunication. *IEEE transactions on communications, VOL. COM-22, NO. 5*, 637-648.

Kasundra, P. (2023, 05 01). *5 Reasons to use Nodejs with React for Web Development*. Récupéré sur https://www.simform.com/: https://www.simform.com/blog/use-nodejs-with-react/#:~:text=It's%20because%20of%20two%20main,and%20several%20other%20Node%20modules.

Linda Rosencrance, P. L. (2023, 03 22). *What is two-factor authentication and why is it used?* Récupéré sur techtarget.com: https://www.techtarget.com/searchsecurity/definition/two-factor-authentication#:~:text=Two%2Dfactor%20authentication%20(2FA)%2C%20sometimes%20referred%20to%20as,resources%20the%20user%20can%20access

Lloyd, C. (2023, 04 19). *How Ultrasonic Fingerprint Sensors Work*. Récupéré sur www.ifixit.com: https://www.ifixit.com/News/14385/how-ultrasonic-fingerprint-sensors-work

Lukasik, S. J. (2011). Why the Arpanet was built. *IEEE Annals of the History of Computing*, 4-21.

Mattis2412, C. b.-s. (2023, 04 08). *L'iris, la partie colorée de l'œil*. Récupéré sur www.futura-sciences.com: https://www.futura-sciences.com/sante/photos/corps-humain-oeil-humain-son-fonctionnement-12-images-1536/medecine-iris-partie-coloree-oeil-11170/

Miklashonok, O. (2023, 05 01). *What Should You Know About the Future of Node.js?* Récupéré sur https://litslink.com/: https://litslink.com/blog/what-should-you-know-about-the-future-of-nodejs

mobilefingerprintingsolutions. (23, 04 08). *Ink Rolled Fingerprinting FD-258*. Récupéré sur https://www.mobilefingerprintingsolutions.com/: https://www.mobilefingerprintingsolutions.com/inkroll-fd-258/

Nebra, M. (2013). *Apprenez à créer votre site web avec HTML5 et CSS3.* www.openclassrooms.com.

nlm.nih.gov. (2023, 04 12). *Visible proofs*. Récupéré sur www.nlm.nih.gov: https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/technologies/bertillon.html

O'brien, L. (23, 04 08). *NIST Measures US-VISIT 10-Fingerprint Speed*. Récupéré sur wired.com: https://www.wired.com/2007/03/nist-measures-u/

Oskar Persson, E. W. (2017). A Theoretical Proposal of Two-Factor Authentication in Smartphones.

P. Mockapetris, K. D. (1988). Development of the Domain Name System. *Symposium Proceedings on Communications Architectures and Protocols* (pp. 123-133). Stanford, California, USA: Association for Computing Machinery.

Ramayya Krishnan, M. D. (2003). The Economics of Peer-To-Peer Networks. *Available at SSRN: https://ssrn.com/abstract=504062*, 1-21.

Sabina. (2023, 04 13). *CISA Bad Practices list updated to include single-factor authentication (SFA)*. Récupéré sur www.itsecurityguru.org: https://www.itsecurityguru.org/2021/08/31/cisa-bad-practices-list-updated-to-include-single-factor-authentication-sfa/

Tolga Acar, M. B. (2013). Single password authentication. *Computer Networks, 57(13)*, 2597-2614.

Triggs, R. (2023, 04 19). *How fingerprint scanners work: Optical, capacitive, and ultrasonic explained*. Récupéré sur www.androidauthority.com: https://www.androidauthority.com/how-fingerprint-scanners-work-670934/

www.01systems.com. (2023, 04 08). *SigCap*. Récupéré sur www.01systems.com: http://www.01systems.com/Products/SigCap.html

www.alliancevita.org. (2023, 04 12). *Décryptage de l'ADN : les scientifiques font de nouvelles découvertes sur le génome humain*. Récupéré sur www.alliancevita.org: https://www.alliancevita.org/2022/04/decryptage-de-l-adn-les-scientifiques-font-de-nouvelles-decouvertes-sur-le-genome-humain/

www.cite-sciences.fr. (23, 04 12). *L'oeil*. Récupéré sur www.cite-sciences.fr: https://www.cite-sciences.fr/archives/francais/ala_cite/expositions/biometrie/nonvoyants/programme_details_6_4.htm

www.futura-sciences.com. (2023, 04 12). *Reconnaissance Digitale : le premier pas en biométrie*. Récupéré sur www.futura-sciences.com: https://www.futura-sciences.com/tech/dossiers/technologie-tendances-biometrie-965/page/2/

www.journaldunet.com. (2023, 04 12). *Biométrie > La rétine*. Récupéré sur www.journaldunet.com: http://www.journaldunet.com/solutions/0611/061127-biometrie/6.shtml

www.thalesgroup.com. (2023, 04 12). *www.thalesgroup.com*. Récupéré sur Thales Cogent DactyScan84c Scanner: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-fingerprint-scanners/DactyScan84c

www.xrtoday.com. (2023, 04 12). *What is speech recognition*. Récupéré sur www.xrtoday.com: https://www.xrtoday.com/virtual-reality/what-is-speech-recognition-technology-in-vr/

www.zalix.fr. (2023, 04 12). *ZX-50 Hand Pass Handkey*. Récupéré sur www.zalix.fr: https://www.zalix.fr/produit/zx-50-hand-pass-handkey/

Xinhua, G. Y. (2023, 04 08). *Global vision drives iris-recognition technology*. Récupéré sur www.global.chinadaily.com.cn: https://global.chinadaily.com.cn/a/201809/14/WS5b9b0fbca31033b4f4655fe8.html

Zdziarski, Z. (. (2023, 04 08). *Gait Recognition – Another Form of Biometric Identification*. Récupéré sur www.zbigatron.com: https://zbigatron.com/gait-recognition-another-form-of-biometric-identification/

Ali, G., Ally Dida, M., & Elikana Sam, A. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. *Future Internet*, *12*(10), 160. https://doi.org/10.3390/fi12100160

Bohringer, J. (2010). *Guide to biometrics*. Springer.

El-Abed, M., Charrier, C., & Rosenberger, C. (2012). Evaluation of Biometric Systems. In J. Yang (Ed.), *New Trends and Developments in Biometrics*. InTech. https://doi.org/10.5772/52084

Eng, A., & Wahsheh, L. A. (2013). Look into My Eyes: A Survey of Biometric Security. *2013 10th International Conference on Information Technology: New Generations*, 422–427. https://doi.org/10.1109/ITNG.2013.65

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). *Digital identity guidelines: Revision 3* (NIST SP 800-63-3; p. NIST SP 800-63-3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

Hallinan, P. W. (1991). *Recognizing human eyes* (B. C. Vemuri, Ed.; p. 214). https://doi.org/10.1117/12.48426

Jain, A. K., Flynn, P., & Ross, A. A. (Eds.). (2008). *Handbook of biometrics*. Springer.

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). *Introduction to biometrics*. Springer.

Kaufman, C., Perlman, R., & Speciner, M. (1995). *Network security: Private communication in a public world*. PTR Prentice Hall.

Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*, *2022*, 1–24. https://doi.org/10.5772/acrt.08

Petsas, T., Tsirantonakis, G., Athanasopoulos, E., & Ioannidis, S. (2015). Two-factor authentication: Is the world ready?: quantifying 2FA adoption. *Proceedings of the Eighth European Workshop on System Security*, 1–7. https://doi.org/10.1145/2751323.2751327

Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, crime and security*. Routledge.