REPUBLIQUE DE COTE D'IVOIRE

Union - Discipline – Travail

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Institut National Polytechnique

Félix HOUPHOUËT-BOIGNY

EDP Ecole Doctorale Polytechnique

THÈSE

Pour l'obtention du grade de

DOCTEUR DE l'INSTITUT NATIONAL POLYTECHNIQUE FELIX HOUPHOUËT-BOIGNY

Mention : PHYSIQUE

Spécialité : Electronique et Electricité Appliquées, Télémédecine, Sécurité informatique

Titre :

CONTRIBUTION A UNE TECHNIQUE D'ACQUISITION ET DE TRAITEMENT DE CONSTANTES DE SANTE, TRANSMISES PAR VOIE SECURISEE AVEC L'ALGORITHME RSA AMELIORE (EMSRSA), A UN MEDECIN DISTANT, PAR TELEPHONIE MOBILE

Présentée et soutenue publiquement le 21 Juillet 2020 par

ACHI HARRISSON THIZIERS

Devant le JURY

M. LOUM L. Georges	Professeur Titulaire	Institut National Polytechnique FELIX HOUPHOUËT BOIGNY, Côte d'Ivoire	Président
M. BEDJA Koffi-Sa	Professeur Titulaire	Université de Lomé, Togo	Rapporteur
M. KRE N'guessan Raymond	Maître de Conférences	Université NANGUI ABROGOUA, Côte d'Ivoire	Rapporteur
M. DIBY K. Ambroise	Maître de Conférences	Université FELIX HOUPHOUËT BOIGNY, Côte d'Ivoire	Examinateur
M. Zoueu T. Jérémie	Professeur Titulaire	Institut National Polytechnique FELIX HOUPHOUËT BOIGNY, Côte d'Ivoire	Co-Directeur de Thèse
M. HABA Cisse Théodore	Maître de Conférences	Institut National FELIX HOUPHOUËT BOIGNY, Côte d'Ivoire	Directeur de Thèse

Résumé

En Afrique subsaharienne, il y a une rareté des centres de santé, des spécialistes et les examens médicaux sont indisponibles dans les endroits reculés de notre pays, la Côte d'Ivoire. Cette situation entraine des diagnostics tardifs ou non faits, qui conduisent à des situations malheureuses et irréversibles. Le problème est donc de trouver comment transmettre plusieurs données médicales acquises directement sur des personnes, analysées puis interprétées, à des spécialistes, de façon sécurisée. Pour résoudre ce problème, nous allons : mettre en place un nouveau dispositif d'acquisition, à faible coût, des constantes de santé des personnes ; établir des techniques de traitement et d'analyse des mesures collectées sur des personnes ; élaborer un nouvel algorithme de sécurisation de la transmission de ces données médicales par téléphonie mobile.

Le test d'égalité des moyennes de *Student* a confirmé l'Hypothèse H0 avec une probabilité comprise entre 5% et 1% pour les constantes suivantes : La température, la saturation du sang en oxygène, la tension diastolique, la tension systolique, la glycémie et le rythme cardiaque. Cela prouve la fiabilité de notre nouvelle méthode d'e-santé. Notre algorithme de prédiction des pathologies risquées par les patients a donné un taux de 97,5 % de conformité de notre diagnostic avec celui de la fiche patient des malades de l'ICA. Pour l'ECG, en prenant ceux de l'ICA comme référentiels, notre méthode a montré sa fiabilité à 65% sur la morphologie et à 84% sur la fréquence. Notre modèle de classification de l'hypertension par réseau de neurones artificiels a donné une parfaite classification des types d'hypertension, avec une régression R^2 de 0.99, un RMSE de 0.03553, une sensitivité de 0.91, une spécificité de 0.93, et une performance de 0.94. Notre algorithme EMSRSA a amélioré les performances du RSA originel, au niveau du temps de génération de la clé privée.

Au terme de cette thèse, nous avons apporté une nouvelle application pour la collecte des constantes sur un smartphone ou une tablette; implémenté un nouvel algorithme d'évaluation de ces constantes collectées sur les appareils mobiles, et un algorithme de prédiction de pathologies à partir de ces constantes et des symptômes connus de cette pathologie. Notre modèle neuronal de classification de pathologies a donné de bonnes performances et nous avons établi un nouvel algorithme EMSRSA basé sur l'amélioration de RSA, pour la sécurisation des données transmises par téléphonie mobile.

Mots clés : E-santé, Réseaux de Neurones Artificiels, Hypertension artérielle, ECG, Algorithme RSA.

Abstract

In sub-Saharan Africa, there is a scarcity of health centers, specialists and medical examinations are unavailable in remote parts of our country, Côte d'Ivoire. This situation leads to late or missed diagnoses, which lead to unfortunate and irreversible situations. The problem is therefore to find out how to transmit several medical data acquired directly on individuals, analysed and interpreted, to specialists in a secure manner. To solve this problem, we are going to: set up a new low-cost device for acquiring people's health constants; establish techniques for processing and analysing the measurements collected from people; develop a new algorithm for securing the transmission of this medical data by mobile telephony.

Student's test of equality of averages confirmed Hypothesis H0 with a probability of between 5% and 1% for the following constants: Temperature, blood oxygen saturation, diastolic pressure, systolic pressure, blood sugar and heart rate. This proves the reliability of our new e-health method. Our algorithm for predicting patient risk pathologies gave a 97.5% compliance rate of our diagnosis with that of the ICA patient record. For the ECG, taking those of the ICA as a reference, our method has shown its reliability at 65% on morphology and 84% on frequency. Our model of hypertension classification by artificial neural network gave a perfect classification of the types of hypertension, with an R^2 regression of 0.99, an RMSE of 0.03553, a sensitivity of 0.91, a specificity of 0.93, and an accuracy of 0.94. Our EMSRSA algorithm improved the performance of the original RSA, in terms of private key generation time.

At the end of this thesis, we brought a new application for collecting constants on a smartphone or a tablet; implemented a new algorithm for evaluating these constants collected on mobile devices, and a pathology prediction algorithm based on these constants and the known symptoms of this pathology. Our neural model for pathology classification gave good performances and we established a new EMSRSA algorithm based on the improvement of RSA, for the security of data transmitted by mobile phones.

Keywords: e-health, Artificial Neuron Networks, Hypertension, ECG, RSA algorithm.

DEDICACE

À Dieu, notre Seigneur JESUS CHRIST, pour sa grâce sur ma vie.

À feu mon père, ACHI M'BEDE Julien, pour son soutien sans faille dans mes études.

À toute ma famille, spécialement à ma Mère, Madame ACHI, née AFFESSI Hélène, à mes petites sœurs ACHI Aguio Eléonore et ACHI Christelle Perpétue.

À ma précieuse épouse, Mme ACHI, née YAO Akissi Agnès et à nos merveilleux enfants : Emmanuella, Mickaëlla et Rebecca.

REMERCIEMENTS

Une thèse, c'est environ trois ou quatre ans de découverte, entremêlant de bonnes comme de mauvaises surprises, mais qui constituent toujours un défi à relever. C'est donc avec enthousiasme et dans un regard rétrospectif, que je me soumets à cet exercice de reconnaissance envers toutes ces personnes sans lesquelles ce mémoire ne serait pas rédigé aujourd'hui.

Mes remerciements vont tout d'abord, à l'endroit de Dieu, notre Seigneur JESUS CHRIST qui m'a donné la santé, le souffle de vie et l'énergie nécessaire pour arriver au bout de ce projet d'étude.

Cette thèse a été réalisée à l'Institut National Polytechnique FELIX HOUPHOUËT BOIGNY de Yamoussoukro (INP-HB), au sein du Laboratoire d'Instrumentation Image et Spectroscopie (L2IS) et du Laboratoire de Réseaux Informatiques et Télécoms (LARIT).

Je tiens à remercier Professeur YAO Benjamin, Professeur Titulaire et par ailleurs, Directeur de l'Ecole Doctorale (EDP) de l'INP-HB de Yamoussoukro, pour avoir bénéficié de tous ses encouragements et soutiens, tout au long de ces années de recherche.

Je remercie ici Professeur ZOUEU T. Jérémie, Professeur Titulaire, mon Directeur d'UMRI et co-directeur aussi de ma thèse, et Directeur du Laboratoire d'Instrumentation Imagerie et Spectroscopie (L2IS) à l'INP-HB de Yamoussoukro, pour ses sages conseils et son soutien sans faille à l'aboutissement de cette thèse.

Un remerciement spécial à mon Directeur de thèse, Professeur HABA Cissé Théodore, Maître de Conférences, pour sa guidance et sa direction inégalée qui m'ont permis d'aboutir à cette soutenance.

Je n'oublie pas ici aussi, Professeur OUMTANAGA Souleymane et Professeur BABRI Michel, Directeur du Laboratoire de Réseaux informatiques et Télécom (LARIT), pour l'accueil qu'ils m'ont offert dans la dernière phase de ma thèse, ainsi que tous les Docteurs et membres du LARIT pour leurs conseils et suggestions. Merci à Professeur LOUM Laussane Georges pour la présidence du jury de ma soutenance de thèse, et les bons

conseils et orientations, sur la suite de mes travaux. Merci également au Professeur BEDJA Koffi-Sa de l'Université de Lomé au Togo, pour son excellent rapport qui m'a permis d'améliorer ce manuscrit. J'adresse un vibrant hommage à Professeur KRE N'guessan Raymond de l'Université Nangui Abrogoua, qui m'a fait de judicieuses remarques et suggestions dans son rapport. Je dis grand merci à Professeur DIBY Kadjo Ambroise, dont l'examen de ma thèse a permis de restructurer certaines parties de ce document.

Je voudrais également dire un vibrant merci à toute l'administration de l'Institut de Cardiologie d'Abidjan, situé au sein du Centre Hospitalier Universitaire (CHU) de Treichville, et par la même occasion, affirmer ma grande reconnaissance à la Direction Médicale et Scientifique (DMS) qui a supervisé mes travaux. Je pense fortement à Professeur ANZOUAN KACOU Jean-Baptiste, Directeur du DMS, à Professeur HAUHOUOT Assepo Marie Laure, Directrice du service de biochimie, à Docteur KONAN Jean-Louis, mon tuteur au service de biochimie, au Docteur DON Célestin, chargé de la pharmacie, à Mlle Iness, assistante du Professeur ADOUBI Anicet. Professeur ADOUBI a été mon Directeur de stage au sein de l'ICA et du CHU de Bouaké, et c'est lui qui m'a aidé à établir tout le protocole de travail, et a aussi orienté l'interprétation et la certification des résultats.

Mes remerciements se tournent également vers toute l'équipe du Laboratoire d'Instrumentation Image et Spectroscopie de l'INP-HB, avec qui j'ai passé d'agréables moments d'échanges. Merci au Dr TOKOU Zan, au Dr BAGUI Kossan Olivier qui a supervisé tous mes articles scientifiques, au Dr KOUABENAN Kouakou Anicet, au Dr YALE Pavel, au Dr REGNIMA Guy-Oscar, au Dr AGNERO Marcel, au Dr Yébouet Marie Florence, au Dr KONIN Edoukoua, au Dr DIBY wilfried, à Mlle ASSOI Koko Eliane, aux Messieurs KOUAKOU Benoît, KOFFI N'guessan Thomas, KOFFI Yao, KOSSONOU Taky Alvarez et tous les autres membres du laboratoire. Votre soutien a été très précieux pour ces travaux.

Je remercie mes parents de m'avoir motivé, lors des moments difficiles, à continuer le travail jusqu'à son achèvement.

Que tous ceux qui ont contribué à quelques niveaux que ce soient, à l'aboutissement de ce travail et qui n'ont pas été cités par simple omission, trouvent ici l'expression de mes sincères remerciements. Merci à tous.

LISTE DES MATIERES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABREVIATIONS ET SYMBOLES

AC. Ur : Acide Urique dans le sang

AES : Advanced Encryption Standard

Ag: Age

BD : Base de Données

CAN: Convertisseur Analogique Numérique

CHb : Concentration Totale d'Hémoglobine dans le sang

$CHbO_2$: Concentration Sanguine en Oxyhémoglobine

D1 : Dérivation 1.

DES : Data Encryption Standard

DMS : Direction Médicale et Scientifique

ECG: Electrocardiogramme

EMSRSA: Enhanced, Modified and Secured River Shamir Algorithm

Gl : Glycémie ou Taux de sucre dans le sang

H0 : Hypothèse de *Student*

Hb : Hémoglobine

HDL: Bon Cholestérol

ICA : Institut de Cardiologie d'Abidjan

LDL : Mauvais Cholestérol

MRSA : Modified River Shamir Algorithm

MSE: Mean Square Error, moyenne des carrés des erreurs

NFHM : modèle hybride neuro-flou

NFS : Numération Formule Sanguine.

PAD : Pression Artérielle Diastolique (PAD)

PAS : Pression Artérielle Systolique

Pd : Poids

RC : Rythme Cardiaque ou pouls

RMSE: Root Mean Square Error, Racine carrée de MSE

S : Sexe (S)

SpO2 : Saturation « pulsée » en oxygène

T : Taille

T° : Température du patient en °C

TA : Tension Artérielle

TDNN: Time Delay Neuronal Network

Ye : couleur des yeux

INTRODUCTION GENERALE

Parler d'acquisition de constantes de santé, de leur traitement et de leur transmission par téléphonie mobile, est quelque chose de très important ; en effet, les constantes de santé sont des grandeurs physiques prélevées sur le corps humain par le biais de capteurs spéciaux.

Ces capteurs sont soit :

-Invasifs ; dans ce cas, le prélèvement se fait par intraveineuse ou accès au liquide du plasma ;

-Non-invasifs ; dans ce deuxième cas, le prélèvement se fait sans pénétration intraveineuse ou extraction de liquide plasmatique.

Ils sont multidimensionnels quand il s'agit de plusieurs constantes différentes. Ce sont elles qui sont transmises via le réseau de téléphonie mobile.

Dans un tel contexte, l'acquisition via trois mini multi-capteurs de constantes multidimensionnels, devient importante pour le patient et ses médecins traitants, car cela permet la télésurveillance ou l'observation des alertes de l'état du patient, la télé expertise et la téléassistance ou l'aide à distante de spécialistes aux agents traitants et proches du patient.

La problématique à résoudre découle de ces faits : les diagnostics tardifs ou non faits conduisent à des situations malheureuses et irréversibles. De plus, les examens médicaux ne sont pas toujours disponibles dans les endroits reculés du pays. Le problème est donc de trouver comment transmettre plusieurs données médicales acquises directement sur des personnes, analysées puis interprétées, à des spécialistes, de façon sécurisée. En d'autres termes, il s'agit d'atteindre les objectifs spécifiques suivants :

- La mise en place d'un nouveau dispositif d'acquisition, à faible coût, des constantes de santé des personnes ;
- L'établissement des techniques de traitement et d'analyse des mesures collectées sur des personnes, notamment la classification ;
- L'élaboration d'un nouvel algorithme de sécurisation de la transmission de ces données médicales par téléphonie mobile.

Devant ce problème d'ordre sanitaire de haute portée nationale et internationale, plusieurs travaux ont essayé de trouver une solution efficace. Nous avons la plateforme multi-capteurs pour la surveillance à distance du positionnement géographique et des signaux comportementaux [1]. Ensuite, les réseaux de capteurs pour application de suivi médical [2].

Il y a eu aussi la mesure télémétrique de signaux biologiques sélectionnés par technologie Bluetooth [3]. N'oublions pas le système sans fil de surveillance médicale à moindre coût, et de transmission à une station d'alarme médicale [4]. Cependant, toutes ces études, nous le verrons plus loin dans ce travail, ont montré, comme tant d'autres, leur insuffisance, notamment par un nombre limité de constantes acquises.

En vue d'y apporter notre contribution, nous proposons une nouvelle technique d'acquisition de 7 constantes non invasives qui sont :

- La pression artérielle systolique (PAS) ;
- La pression artérielle diastolique (PAD) ;
- La tension artérielle (TA) ;
- Le rythme cardiaque ou pouls (RC) ;
- La saturation « pulsée » en oxygène (SpO2) ;
- La température du patient (T°) ;
- L'électrocardiogramme (ECG).

Cinq constantes invasives également sont collectées :

- La glycémie ou Taux de sucre dans le sang (Gl) ;
- L'acide urique dans le sang (AC. Ur) ;
- L'hémoglobine (Hb) ;
- L'albumine ou les protéines dans l'urine ;
- Le PH du corps

Le poids (Pd), la taille (T), le sexe (S), l'âge (Ag), la couleur des yeux et le groupe sanguin y sont également renseignés manuellement.

Cela nous permet de déduire l'Indice de Masse corporelle (IMC) et le taux d'hématocrite (Ht) et complète à 14 le nombre de constantes collectées. Nous avons créé une librairie de symptômes en fonction des pathologies courantes sélectionnées par nos soins, collectés sur le client et renseignés manuellement dans notre application.

Notre démarche à suivre est la suivante : nos algorithmes de premier niveau procèdent d'abord aux tests des pathologies directement liées à ces valeurs physiques, en vue de déduire leur caractère normal, anormal ou critique. Ensuite, notre algorithme s'inspirant de la loi de Bayes, que nous imitons [7], permet d'affiner la prédiction de pathologies. Cette prédiction est consolidée par un apprentissage par réseaux de neurones artificiels de rétro-propagation. La transmission est, par la suite, sécurisée par un algorithme amélioré de RSA.

Les tests de pathologies et le diagnostic prédictif sont ainsi transmis à notre Mobile Cloud Computing, via la puce du réseau téléphonique embarquée dans nos terminaux mobiles, qui les transmet à son tour au médecin traitant, aux spécialistes. Il est possible que les données soient envoyées aux parents du patient.

Notre travail de recherche, intitulé : « Contribution à une technique d'acquisition et de traitement de constantes de santé, transmises par voie sécurisée avec l'algorithme RSA amélioré (EMRSA), à un médecin distant, par téléphonie mobile », est organisée en trois chapitres dont le premier parle de l'état de l'art et présente les généralités sur les capteurs et des constantes de santé.

Le deuxième chapitre présente les matériels et les méthodes utilisés. Le chapitre troisième expose les résultats et les discussions. Une conclusion et les perspectives de recherche sont données après ces trois parties.

Ainsi, le chapitre 1 présente le contexte et une revue bibliographique sur les techniques d'acquisition de constantes de patients, et leur transmission par des technologies telles que la téléphonie mobile. Il montre aussi des généralités sur les modes de fonctionnement des capteurs. Les principes des différentes constantes acquises dans notre recherche sont précisés.

Le chapitre suivant expose clairement les matériels que nous avons utilisés pour résoudre nos hypothèses, notamment notre échantillon biologique, le nouveau dispositif de collecte des constantes sur les patients. Nous y voyons également les méthodologies utilisées, à savoir :

- La nouvelle application mobile que nous avons développée, pour permettre la collecte des constantes sur un smartphone ou une tablette ;
- Le test statistique de *Student*, pour confirmer la fiabilité des constantes collectées par notre méthode ;
- Le nouvel algorithme d'évaluation de ces constantes collectées sur les appareils mobiles ;
- L'algorithme de prédiction de pathologies à partir de ces constantes et des symptômes ;
- Le modèle neuronal de classification de pathologie telle que l'hypertension artérielle ;
- Le nouvel algorithme basé sur l'amélioration de celui de RSA, pour la sécurisation des données transmises par téléphonie mobile.

Le troisième chapitre expose les résultats obtenus, notamment :

- Les résultats du test de *Student* sur la comparaison des constantes collectées par notre méthode et celle de l'Institut de Cardiologie d'Abidjan (ICA) ;

- Les résultats de la prédiction de pathologies ;

- Les résultats des électrocardiogrammes (ECG) acquis par les deux méthodes comparées;

- La classification des stades de l'hypertension artérielle par les réseaux de neurones artificiels ;

- L'algorithme RSA modifié et amélioré en EMSRSA.

Une analyse récapitulative des avantages économiques, des gains en efficacité et temps, est présentée à la fin de ce troisième chapitre.

CHAPITRE 1 : ETAT DE L'ART ET GENERALITES

1.1. Etat de l'art

L'acquisition, via trois multi-capteurs, de constantes de santé devient importante pour le patient et ses médecins traitants, car cela permet la télésurveillance ou l'observation des alertes de son état, la télé expertise et la téléassistance ou l'aide distante de spécialistes aux agents traitants proches du patient. Nous présentons, ici, quelques travaux qui ont tenté d'apporter une solution pertinente à ce problème.

1.1.1. Plate-forme multi-capteurs pour la surveillance du positionnement géographique et des signaux comportementaux

Dans cette étude, C. Axelle et *al*. [1] proposent une architecture multi-capteurs de mesure et de transmission des données physiologiques à distance, et qui soit la moins énergivore possible. Elle comprend 6 parties :

-La conception et la réalisation d'une architecture modulaire, possédant un certain nombre de capteurs et de modules capables de transmettre des données physiologiques à distance sur un serveur ;

-Une présentation contextuelle du champ de sa recherche ;

-L'état de l'art sur les systèmes multi-capteurs conçus ;

-La réalisation de la plateforme multi-capteurs ;

-Les stratégies et algorithmes pour économiser l'énergie de la pile ;

-Les résultats des tests et discussion.

Les Limites

Cette recherche traitant d'un véritable procédé multi-capteurs de signaux physiologiques élucide bien les technologies à implémenter pour transmettre à distance via tablette PC, PDA et Smartphone, des données vers un serveur distant. Cependant, l'étude est prédictive seulement pour des pathologies ciblées au sein d'une population européenne : obésité, diabète et maladies cardiovasculaires.

1.1.2. Réseaux de capteurs pour applications de surveillance médicale

B. Gavilanes et *al*. [2] Ont mis en place un système de réseaux de capteurs capables de surveiller les caractéristiques physiologiques des personnes âgées et de transmettre ces

données à un centre de soins ou de logistique. Ces travaux comprennent trois parties :
-La comparaison des schémas de distribution Unicast et Multicast, pour la transmission de données physiologiques ;
-L'hétérogénéité des nœuds avec des patients équipés de capteurs géographiquement rapprochés ;
-L'agrégation des données physiologiques dans ce contexte de nœuds hétérogènes.

Limites

Comme les précédentes, cette étude vise la mise en place de meilleurs procédés pour acquérir des constantes sur des patients, mais s'attarde beaucoup plus sur les technologies de transmission optimale, à partir d'échantillons de patients géographiquement identifiés.

1.1.3. Mesure télémétrique de signaux biologiques sélectionnés

M.Cerny et *al*. [3] ont proposé une architecture de transmission de données médicales à partir d'un mobile doté de la technologie Bluetooth, dans le même élan que C. Axelle et al. Cette étude, cependant, présente un nombre limité de constantes de santés collectées et transmises à un serveur distant.

1.1.4. Système de surveillance médicale sans fil à moindre coût et transmission à une station d'alarme

A. VEYSEL et *al*. [4] ont travaillé sur une architecture de surveillance médicale de personnes à domicile, grâce à des capteurs sensoriels autour des personnes. Là encore, le nombre de constantes est limité.

1.1.5. Utiliser des téléphones intelligents et des capteurs corporels pour offrir des soins de santé personnels mobiles omniprésents

M. C. Silva Bruno et *al*. [5] proposent une architecture de transmission de données physiologiques, notamment l'ECG, via un téléphone mobile à un serveur distant. Il montre

surtout que le stockage de ces données sur le téléphone mobile avant sa transmission, permet d'économiser plus d'énergie que le fait de transmettre en continu vers le serveur distant.

1.1.6. Mobile-health : un état des lieux en 2015

Cette revue de littérature [6], en matière d'état de l'art en application de m-health ou application mobile d'é-santé, montre les dernières technologies émergentes,

Limites :

Au vu de toutes ces technologies, nous constatons qu'elles sont certes performantes, mais très peu d'entre-elles proposent l'acquisition de plusieurs constantes sur une tablette en vue de leur transmission par le réseau mobile vers une centrale spécialisée, puis vers des spécialistes.

1.1.7. La conception d'un système de surveillance m-health basé sur une plateforme de cloud computing

Cet article [7] parle d'un système de santé basé sur un mobile cloud utilisant le stockage cloud et l'accès multi-utilisateurs, pour la télésurveillance de la prise de médicaments par les patients distants. Il ne traite pas, cependant, d'acquisition de constantes de santé.

1.1.8. Systèmes mobiles de soins de santé dans les cloud utilisant le concept de point de service

Cette thèse de doctorat [8] parle de la mise en place d'un système cloud mobile qui permettrait aux patients, à domicile ou en hospitalisation et ayant besoin de secours, de pouvoir joindre les agents de santé ou spécialistes qui pourraient leur indiquer la marche à suivre. Elle ne traite pas spécifiquement de l'acquisition de constantes de santé.

1.1.9. Le Télé-ECG au service du dépistage des maladies cardiaques en Côte d'Ivoire

Au cours de cet atelier qui s'est tenu en Côte d'Ivoire, précisément dans la ville de Bouaké, les experts en cardiologie ont dégagé les grands axes de mise en place d'une

plateforme automatisée de partage de données médicales, notamment l'ECG. Nous notons que ce travail était centré autour de la seule constante de santé qu'est l'ECG [9].

1.1.10. La télémédecine basée sur les appareils mobiles et l'informatique en cloud mobile

Dans cet article [10], l'auteur expose la conception d'un Mobile Cloud Computing (MCC), pour le stockage sécurisé des données médicales. Une application mobile a été développée. Cependant, il n'y est pas précisé le nombre de constantes collectées.

1.1.11. Conception rentable de la télésurveillance en temps réel des soins de santé à domicile basée sur le Mobile Cloud Computing

Ce papier traite du développement d'une application médicale pour smartphone [11], en vue de collecter des constantes de santé. Il a l'avantage d'être moins cher, mais le nombre de constantes collectées est limité.

1.2. Le problème

La revue de littérature ci-dessus des travaux existants révèle que les auteurs ont fait d'excellents travaux dans le champ qui cerne la collecte des constantes de santé. Cependant, très peu d'entre eux ont orienté leurs travaux vers la conception d'un outil novateur d'acquisition par Bluetooth de plusieurs constantes de santé, en vue de leur affichage sur un terminal mobile, pour des tests prédictifs sous forme de bilan de santé, et leur transfert sur un cloud computing, via le réseau de téléphonie mobile.

Ceci dit, aucun de ces travaux n'a pu exposer une acquisition d'un aussi grand nombre de constantes, par technologie Bluetooth et par saisie directe, au travers de trois mini multi-capteurs, capables d'acquérir automatiquement 12 signaux physiologiques et d'en déduire 2 autres paramètres physiologiques. Du moins, les travaux qui ont abordé l'acquisition par Bluetooth de signaux physiologiques multidimensionnels, se limitent au maximum à trois valeurs physiques, et donc, ils sont insuffisants pour établir un bilan de santé ; même le CARDIOPAD d'Arthur ZANG du Cameroun ne traite spécifiquement que des maladies cardiaques [12].

D'un autre côté, le bilan de santé classique nécessite de nombreux examens différents, avec des matériels lourds, couteux et difficiles à déplacer en temps réel. Ainsi, nous avons proposé notre plateforme multi-capteurs pour l'acquisition et la transmission des 14 constantes de santé et d'autres valeurs déduites. Ceci, en vue de réduire le temps des résultats à pratiquement 3 minutes maximum, avec un matériel accessible, moins coûteux et mobile. Par la suite, nous proposons leur modélisation dans notre application mobile. A ce stade, nos algorithmes de premiers niveaux procèdent d'abord aux tests des pathologies directement liées à ces valeurs physiques, en vue de déduire leur caractère normal, anormal ou critique. Ensuite, nos algorithmes avancés, font agir les symptômes de la personne en vue d'affiner un diagnostic prédictif de pathologies, avant leur transmission sécurisée par l'algorithme RSA amélioré, via le réseau de téléphonie mobile vers notre mobile cloud computing.

1.3. Mode de fonctionnement des capteurs et schéma synoptique d'un capteur Biomédical

1.3.1. Chaîne de mesure par un capteur

Les capteurs sont des éléments qui réagissent à des grandeurs physiques qu'ils transforment en grandeur électrique (en général une tension). On les incorpore très souvent à une chaîne d'acquisition permettant à la grandeur mesurée d'être conditionnée afin que la mesure (ou signal de sortie) donne une estimation optimisée du mesurande [13]. Les figures 1 et 2 montrent la chaine d'acquisition d'un signal par le capteur.

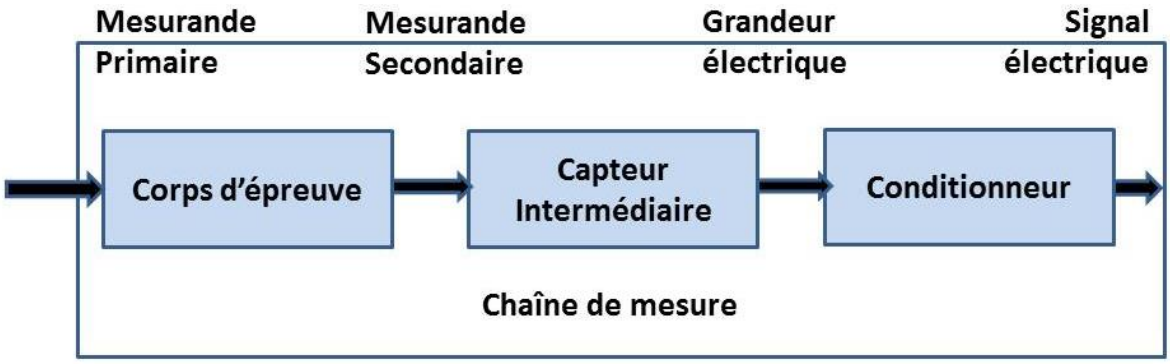


Figure 1: Chaine d'acquisition d'une mesure [13]

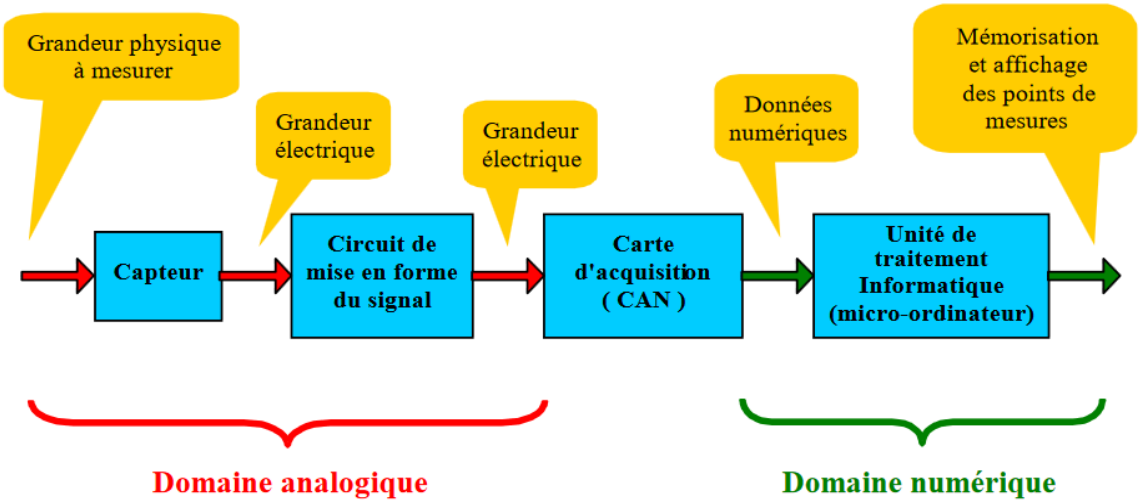


Figure 2: Chaîne de mesure informatisée [14]

Une mesure est une illustration numérique d'une grandeur physique (température, pression, champ magnétique, etc). On définit la terminologie suivante :

-Mesurande : grandeur physique soumise à un mesurage (pression, température, ...) ;

-Mesurage : toutes les opérations permettant d'obtenir la valeur d'une grandeur physique (mesurande) ;

-Mesure : valeur numérique représentant le mesurande (6 MPa, 20°C, 2 m.s, etc.).

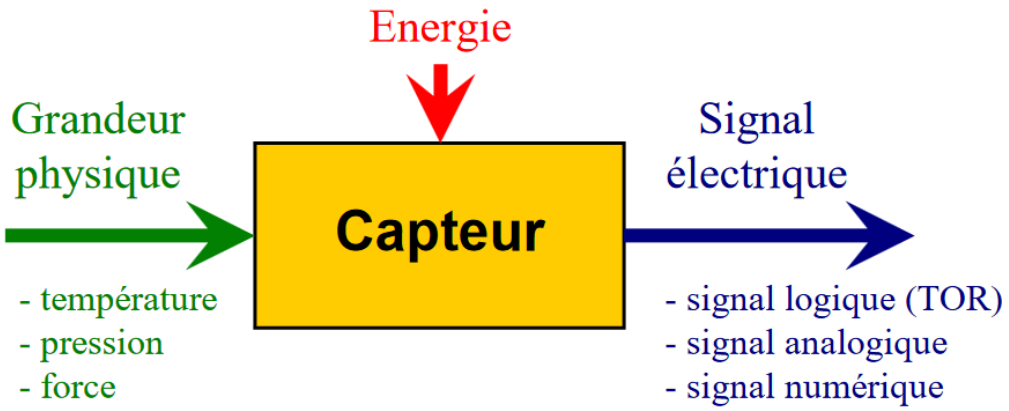


Figure 3: Schéma synoptique d'un capteur [14]

1.3.2. Caractéristiques déterminantes dans le choix d'un capteur

Pour une application donnée, il est fréquent que plusieurs technologies de capteur puissent convenir. Leur choix dépendra des performances visées en termes de caractéristiques de mesure, dont les principales sont définies ci-après.

Etendue de mesure : (E.M.) différence entre la valeur minimale m_{min} et maximale m_{max} du mesurande à obtenir : $E.M. = m_{max} - m_{min}$. L'étendue de mesure est définie par la courbe d'étalonnage du capteur (figure 4) qui, à chaque valeur du mesurande *m* fait correspondre un signal de sortie *s* unique [15].

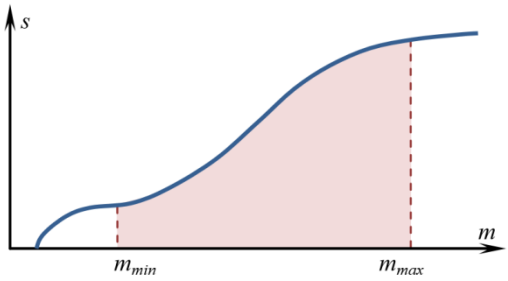


Figure 4: Etendue de mesure d'un capteur [15]

Dynamique de mesure : C'est la différence entre les valeurs extrêmes mesurables par le capteur pour une marge d'erreur fixée. Les mesures ne sont pas entachées d'une erreur supérieure à celle tolérée, elles sont données avec la notion de précision [15].

Résolution : c'est la plus petite valeur identifiable par le capteur. La résolution dépend du niveau de bruit.

Sensibilité : Facteur de proportionnalité entre le signal de sortie du capteur *s* et la grandeur mesurée. Pour une valeur donnée *m* du mesurande, la sensibilité *S(m)* du capteur est égale au rapport entre la variation de la sortie électrique et la variation du mesurande [15] :

$$S(m) = \left(\frac{\Delta s}{\Delta m}\right) \tag{1.1}$$

Si *S(m)* est, dans l'étendue de mesure, une fonction linéaire du mesurande *m*, le capteur est dit linéaire. Sa sensibilité *S(m)* est alors constante sur l'étendue de mesure (figure 5).

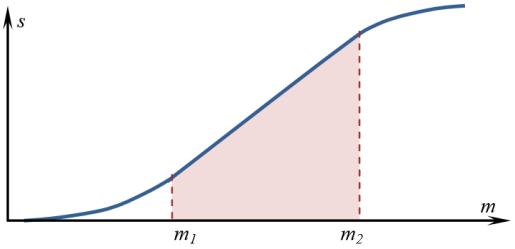


Figure 5: Sensibilité de mesure d'un capteur [15]

Précision : L'incertitude sur chaque résultat de mesure M doit être quantifiée par une estimation de l'erreur possible exprimée par ± δM. Nous savons alors que $m = M \pm \delta M$. L'erreur de précision est une erreur relative ε_p ramenée à l'étendue de mesure :

$$\varepsilon_p = \left(\frac{\delta M}{E.M}\right) \tag{1.2}$$

Bande passante : Gamme de fréquence dans laquelle fonctionne le capteur. Elle caractérise la rapidité du capteur. En effet, la rapidité est la capacité de réponses aux variations du mesurande dans le temps.

Dérives et paramètres d'influence : Diverses grandeurs physiques (g_i) autres que le mesurande *m*, sont susceptibles d'influencer la mesure *M* faite par le capteur :

M = f(m,g_1,g_2, ...). Il peut s'agir, par exemple, de la température ambiante, de vibrations, d'humidité mais aussi de perturbations électromagnétiques, etc. Il est possible d'en tenir compte dans le mesurage, en réalisant en parallèle une mesure de certaines grandeurs d'influence, ou de s'en protéger (suspension antivibratoire, blindage électromagnétique …) ou encore de les compenser par la chaîne d'acquisition avec une électronique adaptée.

D'autres caractéristiques sont importantes dans le choix d'un capteur, notamment le coût, l'encombrement, sa facilité de mise en œuvre [15].

1.3.3. Caractéristiques liées aux erreurs de mesure

Les mesures faites par un capteur sont généralement sujettes à une imprécision. La différence entre la valeur réelle du mesurande et la mesure est appelée erreur de mesure. On peut distinguer deux types d'erreurs : les erreurs systématiques et les erreurs accidentelles (figure 6).

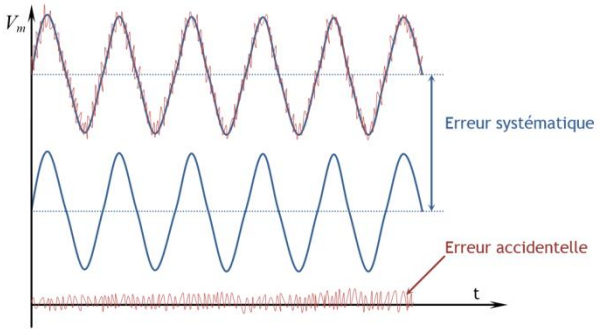


Figure 6: Erreur systématique et erreur accidentelle de mesure d'un capteur [15]

Les erreurs systématiques ont plusieurs origines possibles. Elles proviennent d'une erreur dans la courbe d'étalonnage, d'une valeur erronée d'une grandeur de référence, d'une correction erronée apportée aux mesures ou encore, d'un écart à la linéarité du capteur supposé linéaire. Les erreurs systématiques introduisent un même décalage que l'on peut éventuellement réduire par réétalonnage.

Les erreurs accidentelles peuvent être dues à une lecture erronée d'un appareil à déviation, d'une erreur de mobilité (capteur insensible à certaine variation du mesurande), aux bruits de l'environnement (thermique, amplificateurs de l'électronique de conditionnement), aux fluctuations des tensions d'alimentation, etc. Leur réduction passe par une amélioration des dispositifs de la chaîne d'acquisition, ou le post-traitement du signal.

Trois caractéristiques métrologiques, ou qualité de mesure d'un capteur, définissent les erreurs de mesure : la justesse, la fidélité et la précision (confère figure 7).

En effet, La justesse est la qualité d'un capteur dont les erreurs systématiques sont faibles. Un capteur juste est un capteur dont la valeur moyenne de mesures répétées (V_{moy}) correspond à la valeur vraie du mesurande (V_m) [15].

La fidélité est la qualité d'un capteur dont les erreurs accidentelles sont faibles. Il donne des résultats peu dispersés autour de la valeur moyenne (V_{moy}). On dit également que les mesures sont reproductibles. Enfin, la précision est la qualité d'un appareil dont chaque mesure est proche de la valeur réelle du mesurande. Il est donc à la fois fidèle et juste.

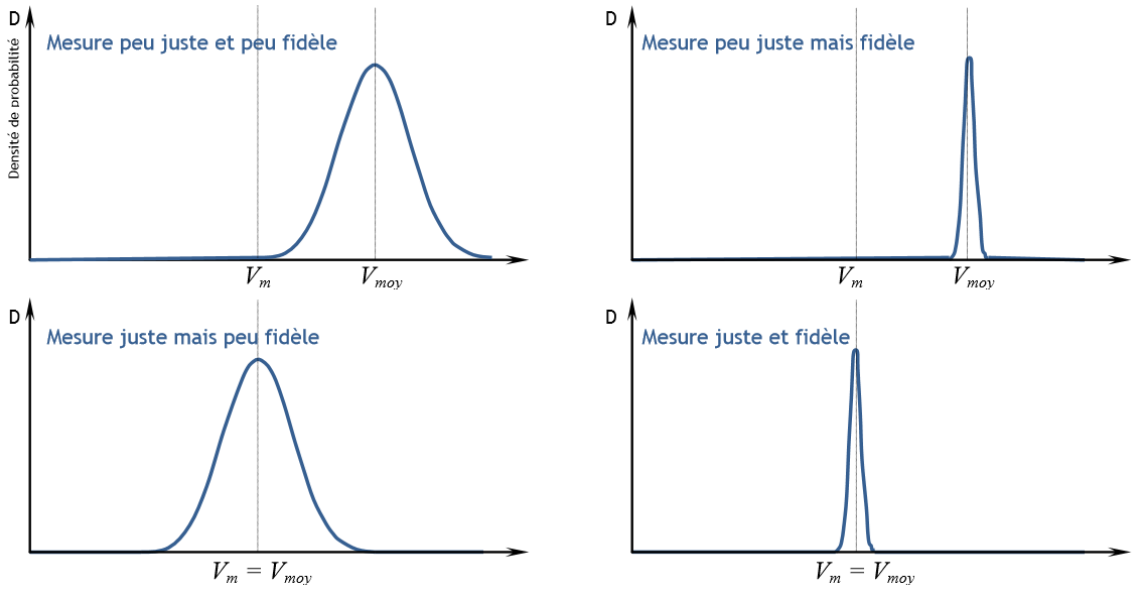


Figure 7: Notion de fidélité et de justesse [15].

1.3.4. Conditionnement des signaux

Le conditionnement permet de mettre en forme le signal mesuré en vue d'un traitement et d'une transmission éventuelle. Il ne s'agit pas ici de faire un bilan exhaustif des conditionnements associés aux capteurs, mais d'en donner plutôt quelques exemples.

1.3.5. Amplification

Lorsque les signaux électriques issus des capteurs sont de faibles amplitudes, il peut être nécessaire de les amplifier pour les adapter à la chaîne de transmission. Il faut savoir que l'amplification (en tension ou en puissance) du signal électrique issu du capteur est un phénomène bruyant : elle s'accompagne d'une dégradation du rapport signal sur bruit. Cela signifie que si l'amplitude du signal utile issue du capteur se trouve augmentée, les parasites (bruit) le sont également mais dans des proportions plus grandes encore [15]. Les amplificateurs d'instrumentation sont conçus de manière à optimiser le rapport signal sur bruit, c'est-à-dire à « peu » le dégrader. Ils sont caractérisés par un gain d'amplification (en tension ou en puissance) ratio du signal électrique de sortie de l'amplificateur sur le signal d'entrée, ainsi que par un facteur bruit F >1 qui quantifie la dégradation du rapport signal sur bruit entre l'entrée et la sortie.

1.3.6. Filtrage

Le filtrage peut avoir différentes applications. Il peut en particulier être pratiqué afin de réduire le bruit (signal parasite « large bande » ou haute fréquence) entachant le signal utile. Ainsi, un filtrage passe-bas éliminera le bruit haute fréquence et produira un effet de lissage utile [15]. Placé avant l'échantillonnage de la conversion analogique/numérique, le filtre d'entrée appelé filtre anti-repliement, contraint le signal à avoir un spectre limité tel que $f_{max}<fe/2$. Placé en sortie de la conversion analogique/numérique, le filtrage lisse le signal de sortie pour restituer le signal utile [15].

1.3.7. Conversion analogique/numérique

La conversion analogique/numérique consiste à transformer la tension analogique (issue du capteur) en un code binaire (numérique) adapté à son exploitation dans un processus

de régulation, de contrôle, de calculs ou encore de stockage. La conversion analogique/numérique n'est pas systématique ; un stockage ou une régulation pouvant également être réalisé à partir de données analogiques [15].

Le Convertisseur Analogique Numérique (CAN) transforme le signal analogique, signal continuellement variable pouvant prendre une infinité de valeurs, en un signal numérique, signal discontinu pouvant être représenté aux moyens de données binaires (0 et 1). La conversion analogique/numérique comporte deux étapes, l'échantillonnage et la conversion proprement dite. En effet, l'échantillonnage est une opération qui doit satisfaire un juste équilibre entre précision et rapidité [15].

La rapidité à laquelle sont prélevés les échantillons, doit permettre une reconstruction fidèle du signal, elle est représentée par la fréquence d'échantillonnage f_e qui doit être suffisamment grande pour retranscrire les variations rapides du signal (figure 8). Le théorème d'échantillonnage aussi dénommé théorème de Shannon-Nyquist [16], permet de déterminer la fréquence d'échantillonnage d'un signal donné. Il énonce que la reconstruction d'un signal de sortie fidèle au signal d'entrée, requiert de choisir une fréquence d'échantillonnage qui soit au moins, deux fois supérieure à la fréquence maximale contenue dans le signal d'entrée, soit : $f_e \geq 2.f_{max}$.

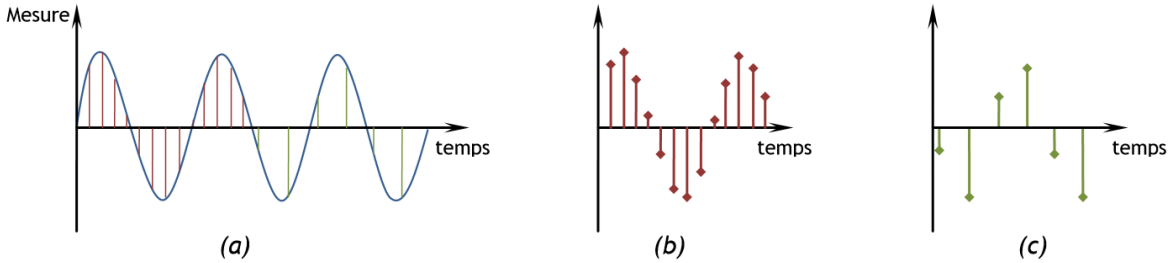


Figure 8: Echantillonnages d'un signal de mesure (a) avec une fréquence d'échantillonnage plus élevée dans le cas (b) que le cas (c), $fe_b > fe_c$ [15]

1.4. Principe des différentes constantes acquises dans notre recherche

1.4.1. Electrocardiogramme (ECG)

L'électrocardiographie est une technique relativement peu coûteuse permettant, à l'aide d'un simple examen et sans danger, de surveiller le bon fonctionnement de l'appareil cardiovasculaire. L'enregistrement graphique de cette activité électrique du cœur est appelé signal électrocardiogramme ECG. Les positions des électrodes utilisées pour le recueil du

signal ECG sont connues par dérivations électrocardiographiques. L'ECG standard est enregistré sur 12 dérivations (six dérivations périphériques et six précordiales) [17].

L'électrocardiogramme est, rappelons-le, indolore, non invasif et rapidement exécuté. L'ECG conventionnel comporte 12 dérivations et est réalisé au moyen de 10 électrodes. L'activité électrique instantanée du cœur peut se résumer à un vecteur résultant principal (dipôle). Ce dernier est enregistré par les dérivations électrocardiographiques qui sont des lignes de tension reliant 2 points distincts (figure 9).

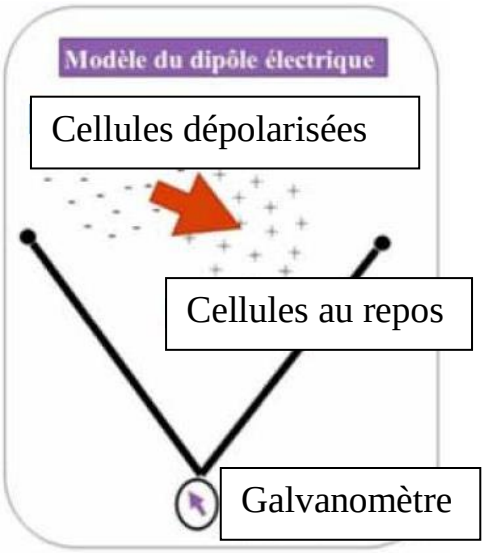


Figure 9: Enregistrement d'un dipôle électrique par un galvanomètre [17]

Une dérivation correspond donc à la mesure d'une différence de potentiel via un galvanomètre entre deux électrodes placées au niveau de deux points différents du corps. Au total, six électrodes sont fixées sur le thorax et quatre au niveau des membres. Le patient doit être allongé, partiellement dénudé dans une pièce de température agréable pour éviter les tremblements musculaires. Il doit respirer normalement, et être confortable pour éviter les artefacts. Les électrodes sont fixées à l'aide de petites ventouses ou de pastilles adhésives.

Disposition des électrodes

Les électrodes des membres sont appelées périphériques (éloignées du cœur) et explorent le cœur dans le plan frontal : on a 3 dérivations bipolaires ou standards obtenues grâce à 3 électrodes : une est posée au niveau du bras droit, une sur le bras gauche et la dernière sur la jambe gauche. L'électrode sur la jambe droite est indifférente. Elles sont annotées DI (connexion bras gauche-bras droit), DII (bras droit-jambe gauche), DIII (bras gauche-jambe gauche). Selon l'hypothèse avancée par Einthoven [18-19], on suppose que ces dérivations décrivent un triangle équilatéral dont le centre est occupé par le cœur. Des 3

électrodes sur les membres, on obtient également 3 dérivations unipolaires amplifiées et désignées comme suit : aVR pour le bras droit, aVL pour le bras gauche, aVF pour la jambe gauche [18].

Ces dérivations unipolaires sont obtenues par l'enregistrement de différences de potentiels entre l'électrode exploratrice (positive) qui détecte les différences de potentiel là où elle se trouve et une électrode neutre obtenue par l'artifice du Central Terminal de Wilson [19]. Dérivations uni et bipolaires dans le plan frontal déterminent ensemble un double triaxe (6 axes au total) au centre duquel se trouve le cœur [20]. A la figure 10, la position de chaque électrode est facilement repérée sur un cercle qui permet de déterminer les angles de ces axes par rapport à la ligne horizontale (0°, position de DI).

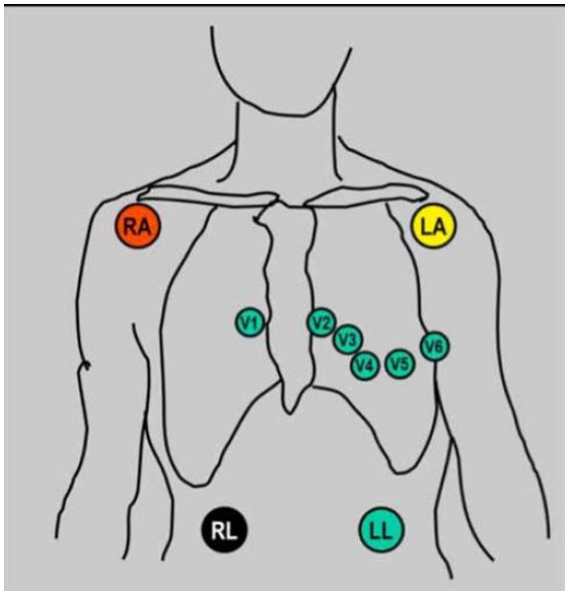


Figure 10: Disposition des électrodes périphériques et précordiales. RA: épaule droite; LA: épaule gauche; RL: jambe droite; LL: jambe gauche. [20]

Les électrodes sur le thorax sont les « précordiales » [21] et sont notées de V1 à V6. Ces électrodes unipolaires analysent l'activité électrique dans le plan horizontal. La disposition des précordiales est la suivante :

- V1 : 4ème espace intercostal, côté droit du sternum ;

- V2 : 4ème espace intercostal, côté gauche du sternum ;

- V3 : équidistance de V2 et V4 ;

- V4 : $5^{ème}$ espace intercostal, ligne médio-claviculaire ;

- V5 : idem, ligne axillaire antérieure ;

- V6 : idem, ligne axillaire moyenne.

Le résumé de la disposition des 12 dérivations est schématisé sur la figure 10.

1.4.2. L'oxymétrie pour la mesure du taux de saturation en oxygène dans le sang (SpO2)

L'oxymètre permet de mesurer la quantité d'oxygène dont le sang est saturé. Cette mesure permet de surveiller l'état des patients sujets à des troubles respiratoires ou souffrant d'affections de l'appareil respiratoire [22].

Physiologie :

Le principe utilisé pour le fonctionnement des oxymètres de pouls est basé sur la capacité d'absorption du sang des lumières rouge et infrarouge, selon leur saturation en oxygène. Le calcul du taux de saturation sanguin en oxygène noté SpO_2 (en %) est basé sur le rapport entre la $CHbO_2$ sur la CHb [22].

$$SpO_2 = \frac{CHbo_2}{\mathrm{CHb}} \qquad (1.3)$$

La $CHbO_2$ étant la concentration sanguine en oxyhémoglobine, et la CHb, quant à elle, est la concentration totale d'hémoglobine dans le sang. L'hémoglobine est une molécule du sang contenant des atomes de fer et qui présente une grande affinité avec l'oxygène. Les globules rouges du sang sont composés à près de 33 % d'hémoglobine. C'est ce qui leur confère cette capacité à transporter l'oxygène capté au niveau des poumons vers les différents tissus de l'organisme. Lorsque l'hémoglobine capte l'oxygène au niveau des poumons, il devient de l'oxyhémoglobine et se colore en rouge vif ; et lorsque cet oxygène est libéré au niveau des tissus, il devient la désoxyhémoglobine (figure 11). Ces deux types d'hémoglobines possèdent un taux d'absorption différent de la lumière rouge et de la lumière infrarouge. L'oxyhémoglobine absorbe mieux la lumière infrarouge et la désoxyhémoglobine absorbe mieux la lumière rouge [22].

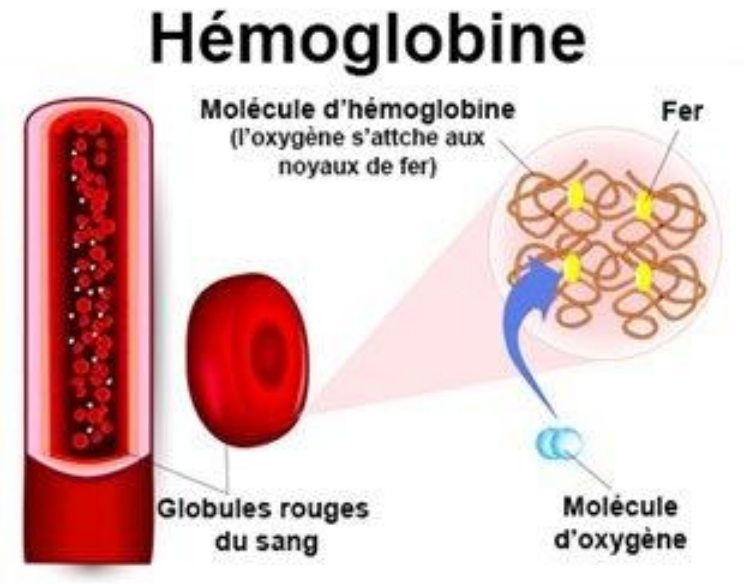


Figure 11: Présence de l'oxygène dans le sang [22]

Fonctionnement :

Le principe d'absorbance va permettre de déterminer le taux de saturation en oxygène d'un milieu. En effet, la quantité de lumière absorbée par un milieu, est proportionnelle à sa concentration en une espèce chimique donnée, selon la loi de Beer-Lambert. Le capteur qui se place à l'extrémité du doigt, est équipé d'un émetteur et d'un récepteur de lumière. L'émetteur permet l'émission d'une lumière infrarouge et d'une lumière rouge grâce à deux Leds (figure 12). La lumière rouge a une longueur d'onde de 660 nm, la lumière infrarouge a une longueur d'onde de 950 nm. Ces deux lumières vont traverser la peau et vont être captées par un récepteur, constitué d'une photodiode, qui va les quantifier [22].

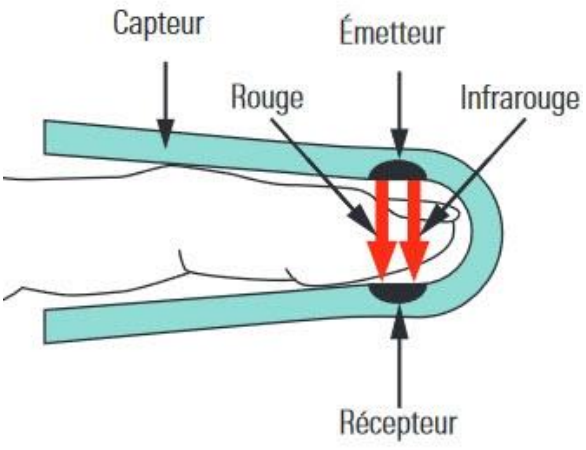


Figure 12: Disposition pour l'acquisition de la saturation en oxygène dans le sang [22].

Un calcul sur la quantité de lumière absorbée va permettre de déterminer la saturation sanguine en oxygène. La saturation du sang (SpO2) s'exprime en pourcentage et va permettre d'avoir une estimation de l'état d'un patient. La valeur normale est située entre **90 % et 100 %**. L'oxymètre va, en outre, permettre de mesurer la fréquence cardiaque, par la mesure de la variation des différents flux de sang au niveau des extrémités.

En plus du capteur qui se place aux extrémités, l'oxymètre est composé d'un moniteur et d'un câble lorsqu'il n'est pas compact. Le câble sert à relier le capteur au moniteur, qui dispose d'un calculateur qui va analyser et traduire les données reçues du capteur.

En effet, le capteur possède la forme d'un doigtier ou d'un pince-doigt et se place au niveau des doigts, des oreilles et des ailes du nez chez l'adulte, ou au niveau des orteils et du pied pour les modèles pédiatriques. Pour l'oxymétrie, la saturation « pulsée » en oxygène (SpO2) est normale entre 96% et 100%. Pour 76%< SpO2<96%, elle est considérée comme anormale alors que SpO2<60% est critique ; la marge critique étant ± 20%.

1.4.3. Acquisition de la température (par infrarouge)

La température (T° en degré Celsius), a pour valeur normale un chiffre situé entre (32-37° C) ; la marge critique étant ± 3° C ; en exemple, une température de 40 °C est anormale. Sous l'aisselle, lors d'une prise de température axillaire, la sonde du thermomètre est calée contre l'aisselle et recouverte par le bras plaqué contre le thorax. La mise en place est donc très simple. Cependant, cet emplacement n'est pas recommandé pour des mesures fiables et rapides (une prise de mesure prend entre 6 et 15 minutes).

La température mesurée, même par infrarouge comme c'est le cas avec le module infrarouge de notre « 6 in 1 health monitor », est celle de la surface de la peau et non la température centrale du corps. Pour obtenir la température rectale équivalente, il faut ajouter au moins 0.5 à 0.8°C.

1.4.4. Le rythme cardiaque

Le Rythme cardiaque (RC, ou Battements cardiaques par minute, Bpm), a pour valeurs normales (60-100 Bpm). Nous considérons qu'il est critique s'il est au moins supérieur ou

inférieur aux valeurs normales de ±20 Bpm (40<RC<60 ou 100<RC<120 est anormale alors que RC<40 ou RC>120 est critique) ; la marge critique est arrêtée par nous à ±20 Bpm.

1.4.5. La pression artérielle

Ainsi, avec la pression artérielle systolique (PAS) en mmHg et la Pression artérielle diastolique (PAD), la Tension artérielle (TA) est :

$$\boldsymbol{TA\ (en\ mmHg)=PAS/PAD}. \tag{1.4}$$

Une hypertension s'annonce au-delà de 14/9 (140/90). En particulier, on parle d'hypertension artérielle quand la diastolique est supérieure à 90 de façon permanente. Toute valeur de PAS>140 mmHg et PAD>90 mmHg est anormale.

Nous considérons toute valeur PAS ou PAD au-delà déjà de ce seuil de ±10mmHg comme critique (Ex : 140 mmHg <PAS<150 mmHg est anormale alors que 150 mmHg <PAS est critique). Le tableau 1 nous indique les différents stades de l'hypertension artérielle.

1.4.6. Données corporelles

Au niveau des données corporelles : le poids (Pd en kg) permet d'envisager l'indice de Masse corporelle (IMC), connaissant la taille du patient. L'indice de masse corporelle est :

$$IMC\ (en\ kg/m^2) = (poids\ en\ kg) / (taille\ en\ m)^2 \tag{1.5}$$

Il permet de surveiller une alerte au diabète et au surpoids. Si l'IMC<18.5 kg/m^2 alors c'est la maigreur. Si l'IMC est compris entre [18.5, 24.9], il est normal ; entre [25- 29,9], nous avons un surpoids, et si l'IMC > 30 kg/m^2, nous avons l'obésité.

La Taille (T) est en mètre (m). Le sexe (S) prend la valeur M ou F. L'âge (Ag) est en année.

La couleur des yeux (Ye) blanchâtre indique un état normal, jaune ou rouge signifie potentiellement la possibilité de pathologie.

Tableau 1: Classification de l'Union Européenne des stades de l'hypertension [23].

Catégorie	**Systolique** *mmHg*		**Diastolique** *mmHg*
Optimale	<120	et	<80
Normale	120 - 129	et/ou	80 - 84
Normale Haute	130 - 139	et/ou	85 - 89
Hypertension Stade 1	140 - 159	et/ou	90 - 99
Hypertension Stade 2	160 - 179	et/ou	100 - 109
Hypertension Stade 3	>180	et/ou	>110
Hypertension de systolique isolée	>140	et/ou	<90

1.4.7. Le taux d'hémoglobine et d'hématocrite dans le sang

Au niveau des variables de la Numération Fonction Sanguine (NFS) : l'hémoglobine (Hb) est entre 12 et 14.5 g/100ml chez l'homme et 11 et 13 g/100ml chez la femme ; la marge critique est arrêtée à ±2 g/100ml. Le taux d'hématocrite (Ht en g/100ml) est 3 fois Hb [24].

$$Ht\ (g/100ml) = 3 \times (Hb) \tag{1.6}$$

1.4.8. Le taux de Cholestérol LDL (Mauvais cholestérol)

Le taux limite statistique du cholestérol total est, chez l'adulte, de 2 g/l. Le rapport LDL-C/HDL-C ou CT/HDL-C est moins fréquemment évalué, où TC désigne le taux de cholestérol total en mmol/l. Le bilan lipidique prend en compte le rapport du taux des Apo lipoprotéines B (représentatives du LDL-C) et du taux des Apo lipoprotéines Al (représentatives du HDL-C) : apoB/apoAl < 0,90.

Un taux de cholestérol LDL est généralement considéré comme normal lorsqu'il est compris entre 0,9 et 1,6 g/L chez l'adulte.

Le LDL-C est calculé selon la formule de Friedevvald (en g/l) (si TG < 4 g/l, la limite étant de 1,5 g/1), où TG le taux sanguin de triglycérides dans la même unité :

$$LDL\text{-}C = CT - (HDL\text{-}C + 1/5\ TG)\ (\text{en g/l}) \quad (1.7)$$

$$LDL\text{-}C = CT - (HDL\text{-}C + 1/2{,}2\ TG)\ (\text{en mmol}) \quad (1.8)$$

1.4.9. L'acide urique dans le sang

On dose l'acide urique (Ur) par une prise de sang. Sa valeur normale est entre 150 et 300 µmol/l chez la femme et (300-400 µmol/l) chez l'homme. La marge critique étant ± 20 µmol/l. On parle d'hypo-urémie quand le taux est inférieur à 25 mg/L et d'hyper-urémie quand le taux est supérieur à 70 mg/L.

1.4.10. La glycémie ou taux de sucre dans le sang

Pour la Glycémie, le taux normal de sucre dans le sang (Gl) est compris entre 0,6 et 1,10 g/l. (1,26 g/l < Gl est anormale alors que 1,40 g/l < Gl est critique) ; la marge critique étant ± 0,20 g/l.

1.4.11. Généralités sur l'hypertension artérielle

L'hypertension, également connue sous le nom d'hypertension artérielle élevée, est un état dans lequel les vaisseaux sanguins connaissent une augmentation continue de la pression. Le sang est transporté du cœur à toutes les parties du corps, dans les vaisseaux sanguins. Chaque fois que le cœur bat, il pompe le sang dans les vaisseaux. La tension artérielle est créée par la force du sang qui pousse contre les parois des vaisseaux sanguins (artères), lorsqu'il est pompé par le cœur. Plus la pression est élevée, plus le cœur doit pomper fort [25].

Selon l'Organisation Mondiale de la Santé (OMS), l'hypertension - ou l'hypertension artérielle - est un trouble médical grave qui augmente considérablement les risques de maladies cardiaques, cérébrales, rénales et autres. On estime que 1,13 milliard de personnes dans le monde souffrent d'hypertension, la plupart (les deux tiers) vivant dans des pays à revenu faible ou moyen [26]. En 2015, 1 homme sur 4 et 1 femme sur 5 souffraient d'hypertension. L'hypertension artérielle est une cause majeure de décès prématuré dans le monde. Sur les 17 millions de décès prématurés (de moins de 70 ans) dus à des maladies non

transmissibles en 2015, 82 % se produisent dans les pays à revenu faible ou intermédiaire et 37 % sont dus à des maladies cardiovasculaires. Les personnes atteintes d'une maladie cardiovasculaire ou qui présentent un risque cardiovasculaire élevé (en raison de la présence d'un ou de plusieurs facteurs de risque comme l'hypertension et la tachycardie), doivent être dépistées et prises en charge rapidement [27].

Dans ce contexte, la détection précoce de l'hypertension aux urgences d'un Institut de Cardiologie ou tout autre centre sanitaire d'accueil, est plus que cruciale. La classification automatique des stades de l'hypertension est également très utile pour limiter le risque de maladie cardiaque et de décès. La principale contribution de ces travaux est de proposer un modèle de détection et de classification automatique de l'hypertension artérielle. Ce modèle basé sur le RNA, nous aide à classer les niveaux d'hypertension, selon la norme européenne (Tableau 1 de la page 36), afin d'aider le praticien à prescrire le meilleur traitement pour le patient.

De nombreuses études ont utilisé des réseaux neuronaux artificiels, souvent avec retro propagation, pour classer les niveaux d'hypertension artérielle. M. Pulido et *al*. [28] ont écrit un article sur la classification de la pression artérielle, en utilisant la méthode des réseaux neuronaux modulaires (MNN). Ils ont pu classer, grâce à ce MNN, les différents niveaux d'hypertension artérielle de 40 personnes. T. H. WU et *al*. [29] ont produit un travail sur l'application biomédicale de la prédiction de la tension artérielle systolique à l'aide de réseaux neuronaux. La prédiction de la tension artérielle systolique par des facteurs corrélés (sexe, cholestérol sérique, glycémie à jeun et signal électrocardiographique) est composée de deux algorithmes de réseau neuronal. H. D. Masethe et *al*. [30], ont élaboré un travail sur la prédiction des maladies cardiaques à l'aide d'algorithmes de classification. Des algorithmes d'exploration de données tels que J48 (une méthode à base d'arbre de décision, qui établit une fonction de classement représentable par un arbre qui est construit enpartant de la racine et en allant vers les feuilles), Naïve Bayes, REPTREE (une variante rapide de l'algorithme C4.5), CART (dont l'acronyme signifie « Classification And Regression Trees », s'attelle à construire un arbre de décision en classifiant un ensemble d'enregistrements), et Bayes Net ont été utilisés dans cette recherche, pour prédire les crises cardiaques. S. Radhimeenakshi et al. [31] ont rédigé un article sur la prédiction des maladies cardiaques à l'aide d'un réseau neuronal avec rétrodiffusion. I. P. Adebayo [32] a produit un article sur le modèle prédictif pour la classification du risque d'hypertension à l'aide de l'algorithme ''Decision Trees'', axé sur l'élaboration d'un modèle prédictif pour la classification du risque d'hypertension chez les

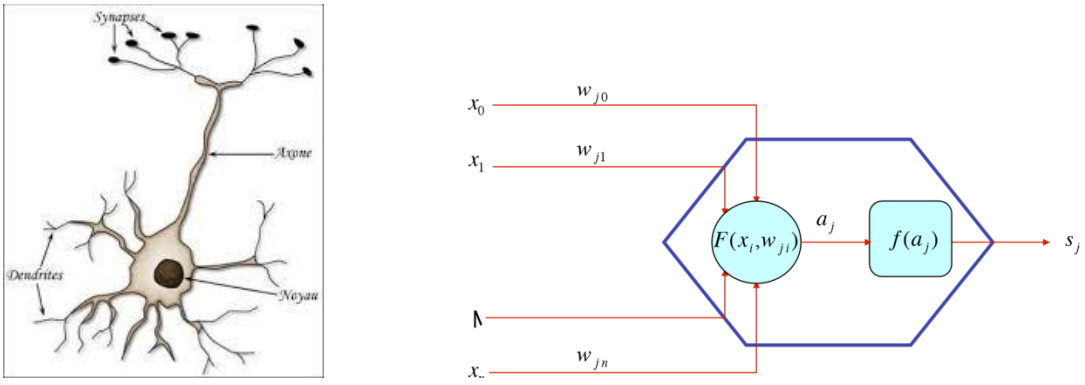
Nigérians, en utilisant des algorithmes basés sur l'information historique obtenue auprès de répondants sélectionnés au sud-ouest du Nigeria. L'ID3 (un algorithme de classification supervisé, c'est-à-dire qu'il se base sur des exemples déjà classés dans un ensemble de classes pour déterminer un modèle de classification), avec une précision de 100 %, a surpassé la C4.5 (une amélioration de l'ID3, se base sur une mesure de l'entropie dans l'échantillon d'apprentissage pour produire le modèle ou graphe d'induction) , qui a affiché une précision de 86,36 %. S. Nimmala et *al*. [33] ont produit un article sur la prédiction de l'hypertension artérielle basée sur l'utilisation d'algorithmes d'apprentissage machine AAA+++, lorsque J. C. Guzman et *al*. [34] ont conçu un Fuzzy optimisé et Classifié pour le diagnostic de la tension artérielle, avec une nouvelle méthode informatique pour l'optimisation des règles expertes. Un modèle hybride neuro-flou (NFHM) a été proposé et a montré un bon avantage. Saloni et *al*. [35] ont effectué une classification des personnes souffrant d'hypertension artérielle par rapport aux personnes ayant une tension artérielle normale, à l'aide de l'analyse vocale, avec diverses caractéristiques extraites du signal vocal des personnes en bonne santé et des personnes souffrant d'hypertension artérielle ; la classification a donné une efficacité de 79%. T. J. Niiranen et *al*. [36] ont travaillé à l'étude: Prediction of Blood Pressure and Blood Pressure Change With a Genetic Risk Score, où ils ont cherché à savoir si un score de risque génétique (SGR), constitué de 32 polymorphismes nucléotidiques simples, pouvait prédire l'hypertension et la tension artérielle incidente. Les résultats ont montré que la SGR est fortement associée à la TA, mais faiblement associée à l'augmentation de la TA et à l'hypertension incidente dans une population d'âge moyen tardif. P. Melin et *al*. [37] ont construit un modèle hybride basé sur un réseau neuronal modulaire et des systèmes flous pour la classification et le diagnostic des risques d'hypertension et de pression artérielle.

1.4.12. Généralités sur les réseaux de neurones

Les modèles connexionnistes, ou réseaux de neurones artificiels (RNA), s'inspirent des propriétés du cerveau pour simuler des processus cognitifs [38]. Mise au point dans les années 1890 par le célèbre psychologue américain, W. James, sur le concept de mémoire associative, cette discipline a connu une période dite obscure. Cette période d'ombre était liée à l'incapacité de cette nouvelle technique à résoudre des problèmes non linéairement séparables. Avec l'avènement des ordinateurs puissants et rapides, Rummelhart et *al*. [39] ont levé cette équivoque, ce qui va susciter à nouveau un intérêt pour les RNA. Elle s'applique de nos jours, dans plusieurs domaines de recherche [40], vu son efficacité à résoudre des

problèmes réalistes et complexes. Comme le cerveau, un réseau de neurones artificiels est composé d'unités (ou neurones) regroupées en couches et reliées les unes aux autres par des connexions (synapses) d'intensité variable. Chaque unité reçoit de l'information des unités auxquelles elle est connectée, calcule son niveau d'activité en intégrant ces informations puis, si son niveau d'activité dépasse un certain seuil, transmet l'information aux unités auxquelles elle est connectée [41]. Ainsi, on a une couche d'entrée recevant les informations externes, une ou plusieurs couche(s) intermédiaire(s) appelées aussi couches cachées, car elles ne sont pas en contact avec l'extérieur et enfin une couche de sortie. Rappelons qu'il n'y a pas d'interconnexions au niveau d'une couche, car chaque neurone reçoit ses entrées de la couche inférieure. L'apprentissage se traduit par la modification du poids des connexions reliant entres elles les différentes unités. Les stimuli à apprendre sont présentés à la couche d'entrée, la réponse du modèle est donnée par la couche de sortie. Les réseaux de neurones formels sont donc des modèles théoriques de traitement de l'information inspirés du fonctionnement des neurones biologiques. [42]

La figure 13 présente les différentes parties d'un neurone biologique d'une part, et d'un réseau de neurone artificiel d'autre part.



(A) (B)

Figure 13: Schéma du neurone biologique (A) et du neurone formel (B)

1.4.12.1. Principe du RNA

Le fonctionnement du RNA peut se résumer en quatre grandes étapes :

- préparation des échantillons ;
- élaboration de la structure du RNA ;
- apprentissage ;
- validation et test.

Préparation des échantillons : Comme dans les cas d'analyse de données, cette préparation est cruciale et aide le concepteur dans le choix du type de réseau approprié pour résoudre son problème. La façon dont se présente l'échantillon, conditionne : le type de réseau, le nombre de cellules d'entrée, le nombre de cellules de sortie et la façon dont il faut mener l'apprentissage, les tests et la validation [43].

Elaboration de la structure du réseau :

Cette phase dépend étroitement du type des échantillons. Elle consiste à choisir d'abord le type de réseau parmi un ensemble de modèle (le perceptron standard, le réseau de Hopfield, le réseau à décalage temporel (TDNN), le réseau de Kohonen, etc...). Dans le cas du perceptron (cas de notre exemple), il faut aussi choisir le nombre de neurones dans la couche cachée [43].

Apprentissage :

L'apprentissage est une phase du développement d'un réseau de neurones durant laquelle le comportement du réseau est modifié. On distingue deux grandes classes d'algorithmes d'apprentissage :

- l'apprentissage supervisé qui consiste à estimer une fonction qui traduit la relation entre les objets et leurs groupes.

- l'apprentissage non supervisé ; on ne cherche pas ici à estimer une fonction mais à regrouper des objets présentant des propriétés identiques. Dans le cadre de notre travail, nous utilisons le premier algorithme supervisé [43]. Il consiste tout d'abord à calculer les pondérations optimales des différentes liaisons, en utilisant un échantillon. On entre des valeurs (observations) dans les cellules d'entrée et qui évoluent pour arriver dans un état S, qui est ensuite comparé à la réponse désirée Y. En fonction de l'erreur obtenue (écart entre S et Y) en sortie, on corrige les poids accordés aux pondérations. C'est un cycle qui est répété jusqu'à ce que la courbe d'erreurs du réseau ne soit plus croissante. Il faut faire attention à ne pas surentraîner un réseau de neurones qui devient alors moins performant. Ce processus est basé sur la minimisation d'une fonction de coût par un algorithme adaptatif de type gradient. La fonction de coût souvent utilisée est l'erreur moyenne quadratique E définie par :

$$E = \frac{1}{N}\sum_{i=1}^{N} E_i = \frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{J}(Y_j^{(i)} - S_j^{(i)})^2 \qquad (2.5)$$

Avec *N* le nombre d'observations de la base d'apprentissage, *J* le nombre de neurones de la couche de sortie, $S^{(i)}$ la valeur de sortie du neurone *j* de la dernière couche obtenue lors de la présentation *i* et $Y_j^{(i)}$ la valeur désirée de la présentation numéro *i* à la sortie du neurone *j*.

Validation et Tests :

Alors que les tests concernent la vérification des performances d'un réseau de neurones hors échantillon et sa capacité de généralisation, la validation est parfois utilisée lors de l'apprentissage (ex: cas du early stopping). Une fois le réseau calculé ou le modèle établi, il faut toujours procéder à des tests afin de s'assurer que notre réseau réagit correctement. Toutes les étapes décrites plus haut peuvent se résumer en un organigramme suivant (figure 14) [43] :

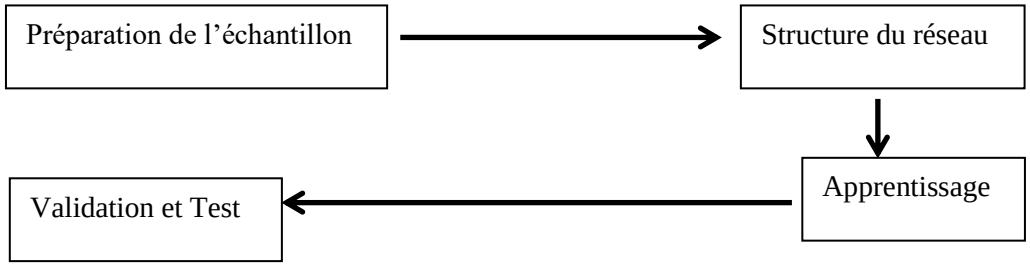


Figure 14: Organigramme de la mise en place d'un modèle à partir d'un réseau de neurones artificiels

Pour mettre en place un réseau de neurones artificiels, on prépare, dans un premier temps l'échantillon qui va constituer notre base de données d'étude. A ce niveau, des méthodes de filtrage peuvent être appliquées pour assainir la base. Par la suite, l'on définit le modèle ou la structure de notre algorithme neuronal, avant de passer à l'apprentissage et à la validation des tests de performance de notre réseau de neurones artificiels.

1.4.13. Généralités sur la cryptographie par l'algorithme RSA

La transmission de données médicales par téléphonie mobile est une innovation que constitue le m-Heath ou plus généralement l'e-santé. Cette télémédecine manipule des données personnelles de patients qui méritent d'être protégées, lors de leur transmission via le réseau opérateur ou privé, afin que des personnes mal intentionnées n'aient pas accès à celles-ci. C'est ici que la cryptographie intervient pour sécuriser les données médicales transmises, en préservant leur confidentialité, leur intégrité et leur authenticité. Dans ce champ de la sécurité des données personnelles, la cryptographie à clé publique ou cryptographie

asymétrique est de plus en plus prépondérante, car elle fournit une clé publique pour encrypter le message transmis et une seconde clé privée, liée à la première par des formelles mathématiques, que seul le destinataire final possède pour décrypter le message. L'algorithme RSA de River et Shamir [44], fournit cette cryptographie asymétrique en se basant sur une clé publique et une clé privée, sur deux nombres premiers. Cependant, la factorisation de ces deux nombres premiers pour donner la variable 'N' de RSA peut être découverte par un hacker et rendre ainsi vulnérable la sécurisation des données médicales. Dans cette partie de notre travail, nous proposons un algorithme de RSA renforcé au niveau de sa sécurité avec 'n' nombres premiers et un stockage hors ligne des paramètres essentiels de l'algorithme RSA, en vue de le rendre plus sécurisé. Nous avons opéré un triple cryptage-décryptage avec ces 'n' nombres premiers, ce qui a rendu plus difficile la tâche consistant à casser la factorisation de la variable 'N'. Ainsi, la génération de clé pour le cryptage et le décryptage prend plus de temps que celle du RSA traditionnel.

1.4.13.1. Justification de notre démarche

Transmettre des données médicales via les technologies d'interconnexion comme la téléphonie mobile est une opération qui exige la plus grande sécurité, en vue de préserver leur caractère privé et personnel. Ce sujet a fait l'objet de plusieurs travaux dans la littérature et continue de passionner plusieurs chercheurs. D. Sathya et *al*. [45] ont travaillé sur un système sécurisé de surveillance à distance, en combinant un algorithme symétrique et un cryptage basé sur l'attribut, pour sécuriser la transmission de données et le système de contrôle d'accès au réseau des capteurs médicaux. J. Heurix et *al*. [46] ont travaillé sur un stockage qui préserve la vie privée et l'accès aux données médicales par pseudonymisation et cryptage. M. Layouni et *al*. [47] ont travaillé sur la supervision distante de l'e-santé qui préserve la vie privée, par un processus d'approbation préalable du patient, avant toute transmission au centre de santé. M. Milutinovic et *al*. [48] ont parlé de la gestion de données préservant la vie privée dans un système d'e-santé, en développant un nouveau protocole basé sur une nouvelle architecture d'e-santé.

Nous constatons par ces travaux, que le cryptage des données vise à rendre inaccessibles les données médicales à des personnes non autorisées. Ainsi, la confidentialité, l'intégrité et la disponibilité de ces données sont préservées [49]. Il existe principalement deux types de cryptographie. La cryptographie à clé symétrique, avec une clé publique unique

qui est partagée entre l'émetteur qui envoi le message crypté et le récepteur qui reçoit ce dernier. Il décrypte le plein texte. Parmi les algorithmes symétriques, on peut citer : DES (Data Encryption Standard), 3DES, AES (un algorithme de chiffrement par blocs, les données sont traitées par blocs de 128 bits pour le texte clair et le chiffré, destiné à remplacer DES). Il y'a également IDEA et BLOWFISH (un algorithme de chiffrement symétrique (c'est-à-dire « à clef secrète ») par blocs conçu par Bruce Schneier en 1993. Il utilise une taille de bloc de 64 bits et la clé de longueur variable peut aller de 32 à 448 bits [50]. Nous avons également la cryptographie asymétrique avec deux clés distinctes: une clé publique qu'utilise l'envoyeur pour crypter son message et une autre clé privée, liée mathématiquement à la première, qui sert à décrypter le message d'origine. On peut citer ici, l'algorithme RSA qui factorise deux nombres premier pour donner un grand nombre entier 'N' [51]. Le principe simple qui conduit RSA est de pouvoir opérer des calculs mathématiques faciles, mais dont l'opération inverse est difficile, en l'absence d'information supplémentaire, selon Muhammad Ariful Islam et *al*. [52], dont nous nous inspirons des travaux dans cette partie de notre recherche.

En général, RSA utilise deux nombres premiers ''p'' et ''q'' pour obtenir la factorisation du grand nombre entier ''N''. L'attaque concernant RSA peut intervenir à ce niveau, quand le hacker réussi à découvrir la factorisation du grand nombre N, empêchant ainsi la génération de la clé privée à partir de la clé publique. Notre travail, dans cette partie, est une amélioration des travaux de MUHAMMAD Ariful Islam, par l'accentuation du temps de génération de la clé, lors de la factorisation du grand nombre N. Nous utilisons, comme lui, quatre nombre premiers, au lieu de deux dans le modèle de RSA original; ce qui rend plus corsé la factorisation, avec un grand nombre de l'exposant servant au cryptage. Au lieu du double cryptage-décryptage qu'il a opéré, nous faisons un triple cryptage-décryptage pour rendre encore plus fort RSA, donc plus sécurisé que RSA original et MSRSA de Muhammad. Pour accélérer le cryptage-décryptage, nous faisons un stockage hors ligne des paramètres essentiels de génération de la clé qui sert à la factorisation.

Plusieurs travaux de recherche dans les thèses de doctorat et dans les journaux scientifiques ont montré qu'il était possible d'améliorer la sécurité du cryptage et du décryptage des données personnelles et privées. Concernant l'algorithme RSA, ces travaux foisonnent, et dans la présente revue de littérature, nous montrons un tableau non exhaustif de ces travaux. A.Hamza et *al*. [53] ont proposé une modification de RSA qu'ils ont appelé : Timing Attack Prospect for RSA Cryptanalysts Using Genetic Algorithm Technique. Cet

article propose l'utilisation d'un Algorithme génétique pour mesurer le temps nécessaire dans l'attaque du crypto système RSA. B. Kumar et *al*. [54] ont proposé une hybridation de l'algorithme AES et RSA concernant les clouds. Akashdeep Bhardwaja et *al*. [55] ont exposé des algorithmes de sécurité pour le Cloud Computing. B. Swamia et *al*. [56] ont proposé un algorithme basé sur un double modulo au niveau de l'algorithme RSA, en utilisant la fonction de Jordan-Totient. Dr. P. Mahajan et *al*. [57] ont fait une revue de littérature sur le cryptage basé sur les algorithms AES, DES et RSA pour la sécurité des données. D. Preuveneersa et al. [58] ont écrit un article sur l'avenir du développement d'application d'e-santé basé sur la téléphonie mobile, en examinant HTML5 pour la gestion du diabète dans un environnement intelligent. M. Kethari et *al*. [59] ont produit une revue de littérature sur la transmission de données médicales pour la e-santé au niveau de la sécurité des plateformes web. V. Kapoor et *al*. [60] ont produit une nouvelle technique de cryptographie hybride pour consolider la sécurité réseau. K. G. Kadam et *al*. [61] ont produit également un algorithme hybrid utilisant à la fois le cryptage RSA-AES pour les services web. K. Rege et *al*. [62] ont également utilisé l'hybridation des algorithms AES et RSA pour sécuriser la communication Bluetooth. R. Raj et *al*. [63] ont travaillé sur la modification du crypto système RSA. S. Patel et *al*. [64] ont mis en place une nouvelle méthode de cryptage utilisant une modification de l'algorithme RSA et le théorème du rappel chinois. A. Gupta et *al*. [65] ont examiné une double modification du modulo de l'algorithme RSA et testé celui-ci par une attaque de brute force. B. Yüksel et *al*. [66] ont produit une recherche sur la protection de la vie privée et la sécurité des services électroniques. S. Bhuyan et *al*. [67] ont écrit un article sur les questions relatives à la protection de la vie privée et à la sécurité dans le domaine de la santé mobile : Recherches actuelles et orientations futures. H. S. G. Pussewalage et *al*. [68] ont fait une publication sur les mécanismes de protection de la vie privée pour faire respecter les exigences en matière de sécurité et de protection de la vie privée dans les solutions de cybersanté. Y. Li et *al*. [69] ont travaillé sur la conception et la mise en œuvre d'un algorithme RSA amélioré. S. Sharma et *al*. [70] ont produit une nouvelle variante du cryptosystème de sous-ensemble-somme de RSA. A. A. Ayele1 et *al*. [71] ont mis en place une technique de chiffrement RSA modifiée basée sur des clés publiques multiples. H. Huang et *al*. [72] ont écrit un article sur la transmission et l'analyse de données médicales privées et sécurisées pour un système sans fil de soins de santé avec detection. B.P. U. Ivy et *al*. [73] ont publié un article sur un système de chiffrement RSA modifié basé sur 'n' nombres premiers.

Tous ces travaux ont démontré qu'il était possible d'améliorer la sécurité de l'Algorithme RSA en le modifiant et en renforçant sa sécurité, et plus encore en le rendant plus rapide. En effet l'une des faiblesses de RSA, est le temps relativement long pour l'exécution de l'algorithme. Notre recherche consiste à renforcer la génération de la clé privée, en utilisant plusieurs nombres premiers, et en procédant par un triple cryptage-décryptage. Cela renforce la sécurité, car la génération de la clé privée prends plus de temps et rend plus difficile la factorisation du grand nombre 'N', que le Hacker aura du mal à casser facilement. Pour rendre l'exécution de l'algorithme plus rapide, en plus de ce triple cryptage-décryptage, nous stockons dans une base de données, les paramètres essentiels pour la génération de la clé privée.

Conclusion partielle

Ce premier chapitre a présenté le contexte de notre recherche et une revue bibliographique sur les techniques d'acquisition de constantes de patients, et leur transmission par des technologies telles que la téléphonie mobile. Il a présenté aussi les généralités sur les modes de fonctionnement des capteurs. Les principes des 14 constantes acquises dans notre travail ont été précisés. Ces constantes collectées sont 7 constantes non invasives qui sont : la pression artérielle systolique (PAS), la pression artérielle diastolique (PAD), la tension artérielle (TA), le rythme cardiaque ou pouls (RC), la saturation « pulsée » en oxygène (SpO2), la température du patient (T°), L'ECG; 6 constantes invasives également sont collectées : la glycémie ou Taux de sucre dans le sang (Gl), l'acide urique dans le sang (AC. Ur), l'hémoglobine (Hb), l'albumine ou les protéines dans l'urine, la présence de sang dans les urines et le PH. Le poids (Pd), la taille (T), le sexe (S), l'âge (Ag), la couleur des yeux et le groupe sanguin y sont également renseignés manuellement. Cela nous a permis de déduire l'Indice de Masse corporelle (IMC) et le taux d'hématocrite (Ht) et complète à 14 le nombre de constantes collectées que nous résumons dans un tableau en annexe 10. Enfin, nous avons exposé les généralités sur l'hypertension artérielle, les réseaux de neurones et l'algorithme RSA amélioré.

CHAPITRE 2 : MATERIEL ET METHODES

Les lignes suivantes présentent, en premier lieu le matériel de l'étude. D'abord sont exposés l'échantillon de personnes sur lesquelles les constantes ont été collectées, la taille de l'échantillon ainsi que les critères de validité des constantes prélevées. Nous précisons également les constantes effectives qui ont fait l'objet de nos relevés sur les fiches que nous avons constituées, en accord avec nos Professeurs superviseurs de l'ICA. Nous décrivons ensuite les équipements classiques tels que le thermomètre numérique, le saturomètre et le tensiomètre utilisés au sein du service des urgences. Par la suite, nous donnons une description précise de nos trois multi-capteurs : le multi-capteur « 6 in 1 health monitor», les Mini-multi capteurs « 3 in 1 EasyMate GHb» et « 3 in 1 EasyMate GCU ». Nous n'oublions pas de mentionner les bandelettes de test d'urine 10 paramètres pour l'acquisition du PH et de la détection de l'albumine dans le sang.

En ce qui concerne les méthodes de travail, nous décrivons l'architecture de l'application URGENCYPAD que nous avons développé, puis la théorie du test statistique de ***Student***. Viennent ensuite successivement : l'algorithme d'évaluation des constantes acquises par nos multi- capteurs, l'algorithme de prédiction de pathologies à partir des signaux acquis et des symptômes renseignés sur notre application mobile, puis la détection et la classification de l'hypertension artérielle par réseaux de neurones artificiels (RNA). Cet ensemble est bouclé par l'algorithme EMSRSA de sécurisation de transmission de données médicales par téléphonie mobile.

2.1. Matériel et expérimentation

2.1.1. Echantillon d'étude

A l'Institut de Cardiologie d'Abidjan (ICA), situé au sein du Centre Hospitalier Universitaire (CHU) de Treichville, nous avons eu l'opportunité d'acquérir les données médicales directement sur des personnes. Pour ce faire, nous avons utilisé les critères de sélection des patients présentant l'hypertension artérielle, le diabète, des tachycardies, des anémies, etc. ; et qui viennent à l'ICA pour faire un bilan biologique. En annexe 14, nous avons un exemple de fiche patient de l'ICA, qui mentionne la provenance du patient. Cela nous a permis d'établir une cartographie de provenance des différents patients.

2.1.2. Taille de l'échantillon

Nous avons collecté les constantes de 120 personnes (45 personnes saines et 75 malades), pour l'entraînement et la validation de nos algorithmes de prédiction ; La plupart des malades ont été prescrits au Catopril 25 mg, 1 comprimé sublinguale par jour. Entre 40 et 60 patients ont également été collectés au sein du service d'urgence de l'ICA pour les tests de performance. Dans cette dernière catégorie de personnes admises aux urgences pour des symptômes d'hypertension, spécifiquement avec une poussée HTA, la médication majeure à l'accueil était Loxen 30 mg, 3 ampoules, ou le Tropil 25 mg.

2.1.3. Paramètres étudiés

Les constantes collectées directement sur les patients de notre échantillon ont été comparées aux valeurs normales de celles acquises par les méthodes de l'ICA. Les constantes collectées étaient: la glycémie, la présence d'albumine dans l'urine (en prévision de l'urée), l'acide urique, l'hémoglobine, le taux d'hématocrite, la saturation en oxygène dans le sang (SpO2), la température, la tension artérielle, les pressions artérielles systoliques et diastoliques, le rythme cardiaque ou pouls, et l'ECG.

2.1.4. Critères de validité

Il s'agissait pour nous, d'observer ici les valeurs ou constantes qui ne s'éloignaient pas des données de référence en médecine.

2.1.5. Ethique de la recherche

Nous certifions que les données collectées ont été acquises de façon confidentielle, et nous avons obtenu au préalable le consentement des patients. Nous leur avons présenté les avantages de faire notre examen, car les résultats étaient rapidement disponibles et fiables également. Des outils statistiques ont été utilisés pour évaluer les écarts.

2.1.6. Matériels pour la collecte

Il nous a été fourni par Docteur KONAN Jean-Louis, en charge de la supervision des examens de Biochimie de l'ICA, une blouse de médecine qui a facilité notre approche avec les malades. Le Major du service des urgences a mis à notre disposition un saturomètre ; un

tube de prélèvement supplémentaire de sang, de couleur verte a été préparé pour nous ; ce qui nous a permis d'éviter de piquer un quelconque malade. Les autres données non invasives furent recueillies par le multi capteur « 6 in 1 health monitor » directement sur le patient ; les données ont été stockées dans l'application installée sur une tablette de type T9 MAX CCIT 10'', 3 Go de Ram, 32 Go de disque dure, Quad Core. Les constantes invasives ont été acquises au laboratoire de biochimie de l'ICA par nos deux autres multi capteurs **EasyMate GCU** (pour le Glucose dans le sang, le Cholestérol et l'Acide Urique) et le **EasyMate GHb** (pour le Glucose dans le sang et l'hémoglobine).

Concernant l'albumine (protéine) dans l'urine, le PH et la présence de sang dans les urines, nous avons utilisé des bols urinaires et des bandelettes 10 paramètres de type Insight Expert de la Société Acon. Ces dispositifs sont présentés à la figure 15.

(A) (B) (C)

(D) (E)

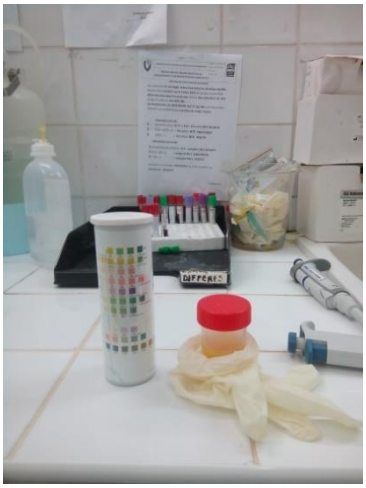


Figure 15: Le multi capteur « 6 in 1 Health Monitor » (A) sur un patient pour la prise de la tension artérielle, EasyMate GHb (B) et EasyMate GhCU (C), Bandelette d'urine et boîte à urine au laboratoire (D) et (E),

Nous avons utilisé un thermomètre numérique pour la température. A la température marquée, on ajoutait +0,5 °C, selon les pratiques médicales ; et cette valeur était comparée à la température fournie par le multi-capteur. Au total, 40 patients cliniques de l'ICA ont été examinés. Nous avions aussi un carnet de note pour recueillir, en temps réel, les constantes, et en prenant soin de marquer la date et l'heure de chaque prise. En outre, les glycémies de 15 autres patients (diabétiques ou non) ont été relevées au Centre de diabète du CHU de Treichville ; 5 ECG supplémentaires ont été réalisés par notre multi-capteur. Les résultats de ces collectes sont dans les annexes 1 à 3.

Cependant, nous avions à exprimer quelques contraintes : souvent les patients n'étaient pas dans les conditions idéales de prises de mesures, notamment pour la glycémie, car certains se présentaient aux urgences après avoir mangé. D'autres patients n'urinaient pas forcement avant leur évacuation en hospitalisation, aux soins intensifs ou au bloc opératoire. Certains, enfin, très affaiblis par la maladie, n'arrivaient pas à se tenir dans la position idéale exigée par la notice du multi-capteur, pour une prise idéale de la tension artérielle ou de l'ECG.

2.1.7. Plateforme multi-capteurs et notre Mobile Cloud Computing (MCC)

Nous présentons ici les modules de notre plateforme multi-capteur pour la mise en œuvre de notre MCC représenté dans la figure 16. Nous avons utilisé un multi-capteur miniaturisé et économique, utilisant une batterie à faible consommation d'énergie. Ce « 6 in 1 health monitor » permet d'acquérir simultanément : la pression artérielle systolique (PAS) en millimètre par mercure (mmHg), la pression artérielle diastolique (PAD) en millimètre par mercure (mmHg), la tension artérielle (TA), le rythme cardiaque ou pouls (RC) qui est le nombre de battements cardiaques par minute (Bpm), la saturation « pulsée » en oxygène (SpO2) qui se mesure en %, la température du corps en degré Celsius (T°), la glycémie (Gl) et l'ECG. Les spécifications techniques de ce multi-capteur sont mentionnées en annexe 11. Ce multi-capteur, ainsi que les deux autres dont nous parlerons plus loin dans ce document, ont été choisi à cause de leur coût d'achat relativement bas et surtout qu'ils sont faciles à déplacer sur les sites. Leur consommation en énergie est relativement plus faible que certains autres dispositifs en Europe. (Confère annexe 13, pour d'autres équipements similaires et un tableau comparatif avec un autre dispositif européen de la société Ihealth).

2.1.7.1. Multi-capteur « 6 in 1 health monitor»

La figure 16.A présente une description des composants de l'architecture du multi-capteur " 6 in 1 health monitor''. La figure 16.B présente les constantes acquises via ce multi-capteur.

(A)

(B)

Figure 16: Architecture de notre mini multi-capteur principal « 6 in 1 Health Monitor » en entier (A) et par module (B) [74].

2.1.7.2. Multi-capteur « 3 in 1 health monitor»

Notre deuxième multi-capteur économique « 3 in 1 EasyMate GCU », à la figure 17, à droite, nous acquiert : la glycémie ou Taux de sucre dans le sang (Gl), le cholestérol total

(CHL), l'acide urique dans le sang (Ac.Ur) en µmol/l. (Confère annexe 12 pour spécifications).

Figure 17: Mini-multi capteurs « 3 in 1 EasyMate GHb» et « 3 in 1 EasyMate GCU ».

Notre troisième multi-capteur « 3 in 1 EasyMate GHb » également à la même figure 15, à gauche, nous donne : la glycémie ou Taux de sucre dans le sang (Gl), l'hémoglobine (Hb) en g/dL. De la valeur de l'hémoglobine, nous tirons un autre paramètre de la Numération Formule Sanguine (NFS) qui est l'hématocrite (Ht). (Confère annexe 12 pour spécifications)

2.2. Déroulement de l'enquête

2.2.1. Cadre de référence

Après l'approbation du comité d'éthique de l'ICA, nous avons été confié au Professeur ANZOUAN Kacou Jean-Baptiste, Chef de la Direction Médicale et Scientifique (DMS) (Confère annexe 4) qui, à son tour, nous a confié au Laboratoire de Biologie de l'ICA, sous la responsabilité de son Chef de service, Madame le Professeur HAUHOUOT Marie-France. Celle-ci nous a confié à son assistant chef de clinique, Docteur KONAN Jean-Louis. Professeur ANZOUAN nous a présenté au personnel de l'ICA et nous a conduit lui-même aux urgences de l'ICA, en nous présentant à son assistante, Docteur TRAORE, qui à son tour, nous a mis en contact avec le major, aux infirmières chargées des soins et aux médecins en formation. De là, nous avons commencé les collectes de constantes, directement sur les patients, en salles d'urgence.

Nous avons établi quatre fiches de travail (Confère annexes 5-8), après la validation de notre protocole d'essai clinique par la DMS (Confère annexe 9), afin d'être efficace dans la collecte des constantes, en vue de leur traitement : Il s'est agi d'une fiche de consentement du patient, une fiche de collecte des constantes non invasives, une fiche de collecte de constantes invasives, et enfin une fiche de collecte des symptômes du patient en fonction des constantes

relevées sur le patient par notre capteur et du diagnostic des médecins. La figure 18 présente le schéma synoptique de notre Mobile Cloud Computing.

2.2.2. Schéma synoptique de notre Mobile Cloud Computing

Les constantes de santé invasives et non invasives sont collectées par l'agent de santé distant, directement sur les patients et insérées dans l'application mobile installée sur la tablette ou le smartphone. Les données sont alors transférées via le réseau de téléphonie mobile vers un serveur cloud, qui va faire un aiguillage automatique des données en vue d'accéder à des spécialistes disponibles. Une fois un spécialiste contacté, ce dernier peut alors apprécier les données et faire des recommandations précises à l'agent de santé distant, via le réseau de téléphonie mobile et l'aiguillage du même serveur cloud.

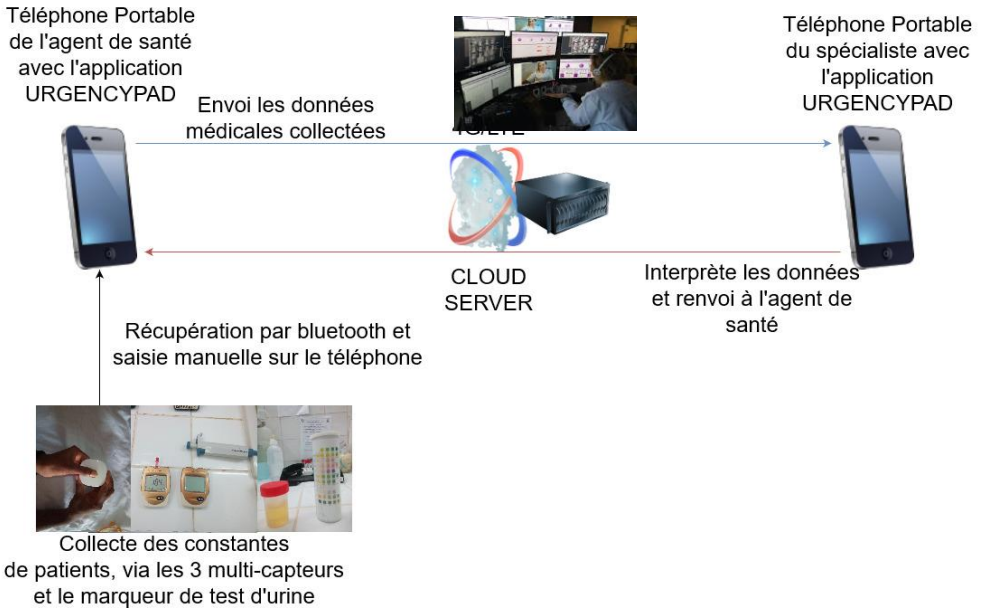


***Figure 18**:* Schéma synoptique de notre Mobile Cloud Computing.

2.3. Méthodes de notre recherche

2.3.1. Présentation des interfaces de notre application mobile pour l'acquisition des données médicales

2.3.1.1. Architecture de notre application mobile et Cloud URGENCYPAD

Pour mener à bien nos collectes de santé, nous avons développé une application mobile, avec une base de données hébergée sur un serveur web, dans une architecture N/3 selon la figure qui suit. La figure 19 présente l'architecture de notre application mobile.

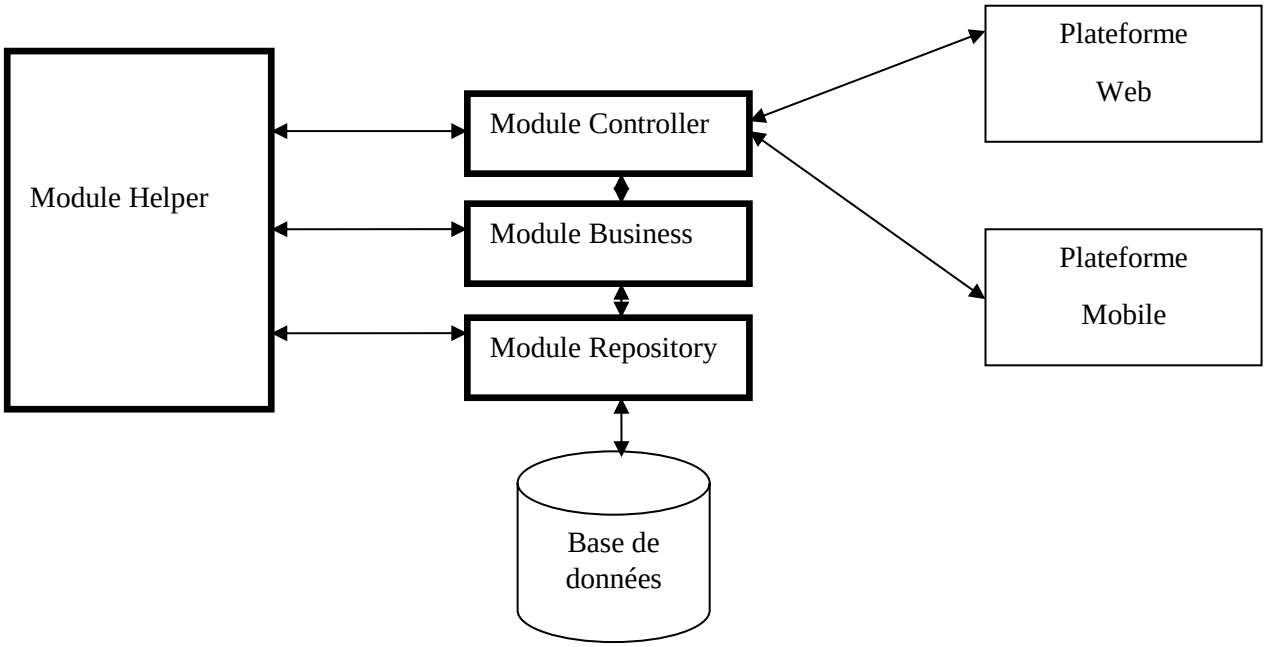


Figure 19: Schéma synoptique de notre application URGENCYPAD.

- Base de données : La source de données de notre projet (Oracle). C'est l'entrepôt de données ou datawarehouse, qui stocke toutes les données enregistrées sur le système.
- Module Repository : Il permet d'accéder aux tables de la base de données via les classes JAVA. Par exemple, il permet les transactions en BD (ajout, suppression…).
- Module Business : C'est La logique métier de notre application
- Module Controller : Il permet d'accéder aux services du cloud, notamment l'interface web et l'interface mobile.
- Module Helper: La couche transverse à toutes les autres. Elle contient toutes les fonctions utilisables sur notre mobile cloud computing.

2.3.1.2. Interfaces de l'application mobile cloud URGENCYPAD

Les figures 20 et 21 nous présentent quelques interfaces de notre application mobile dénommée URGENCYPAD. Les autres interfaces sont présentées en annexe 8. Quant à la

figure 20, il s'agit de l'interface de l'application web sur le serveur cloud, avec un serveur Apache Tomcat 8. Les autres interfaces web sont en annexe 15.

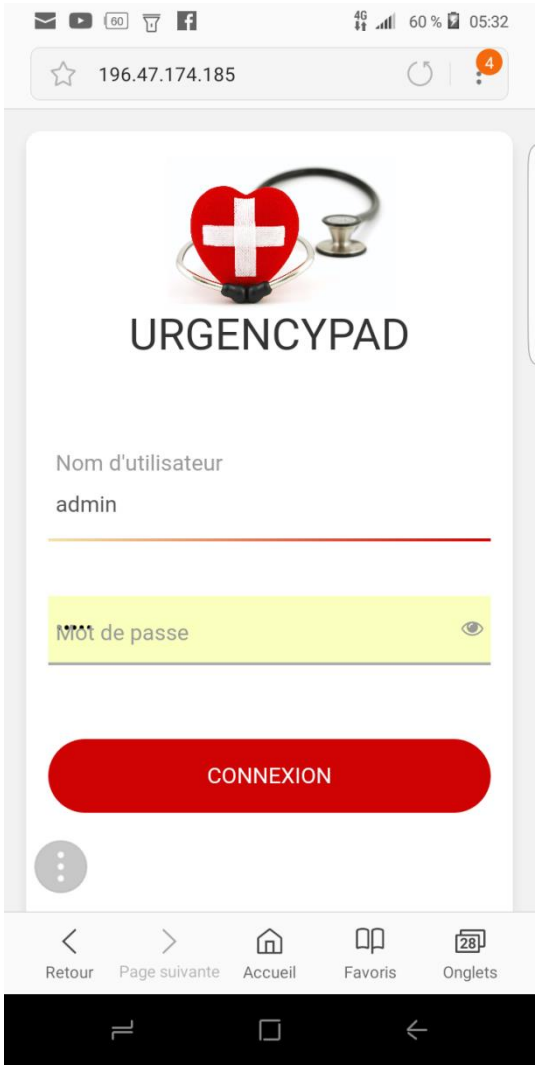


Figure 20: Interface de connexion de l'application mobile URGENCYPAD

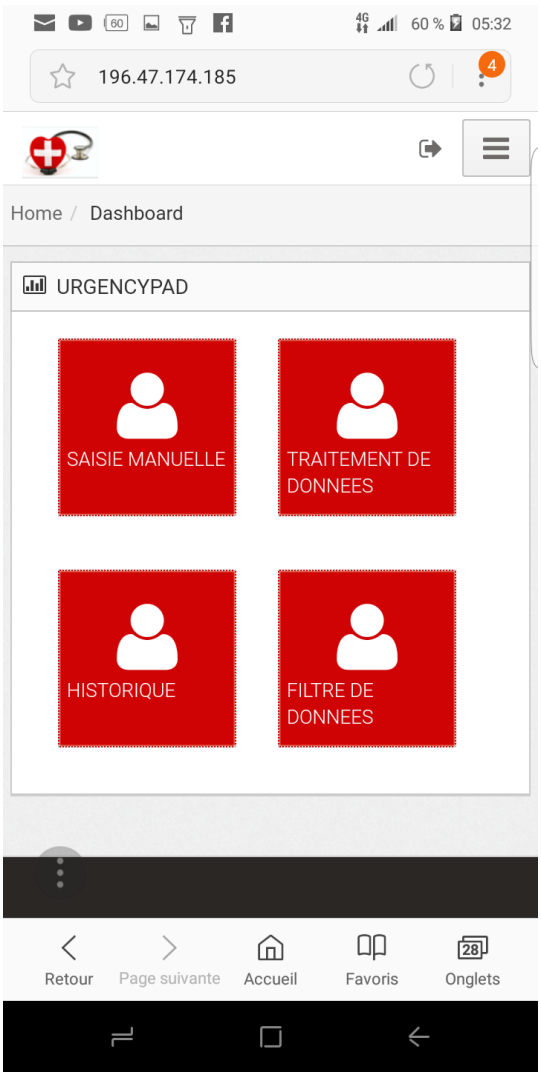


Figure 21: Tableau de bord de l'application

Avec l'écran de gauche, l'agent de santé peut se connecter en entrant un login et un mot de passe. Celui de la droite lui permet d'accéder à la saisie manuelle des constantes de santé sur l'application.

Cette application innovante a été développée exclusivement en environnement JAVA, car cela offre plus de librairies pour le développement. Elle est responsive, c'est-à-dire que son affichage s'adapte aussi bien sur les smartphones que sur les tablettes pc. Elle est évolutive car nous avons utilisé les Web services et sa base de données repose sur un serveur Cloud. A l'échelle nationale, ce serveur cloud sera un Data center capable de supporter un volume important de données ou Big Data.

Comme le montre la figure 22, l'administrateur de l'application web peut se connecter avec un login et un mot de passe sécurisés (Confère annexe 16, pour les autres interfaces).

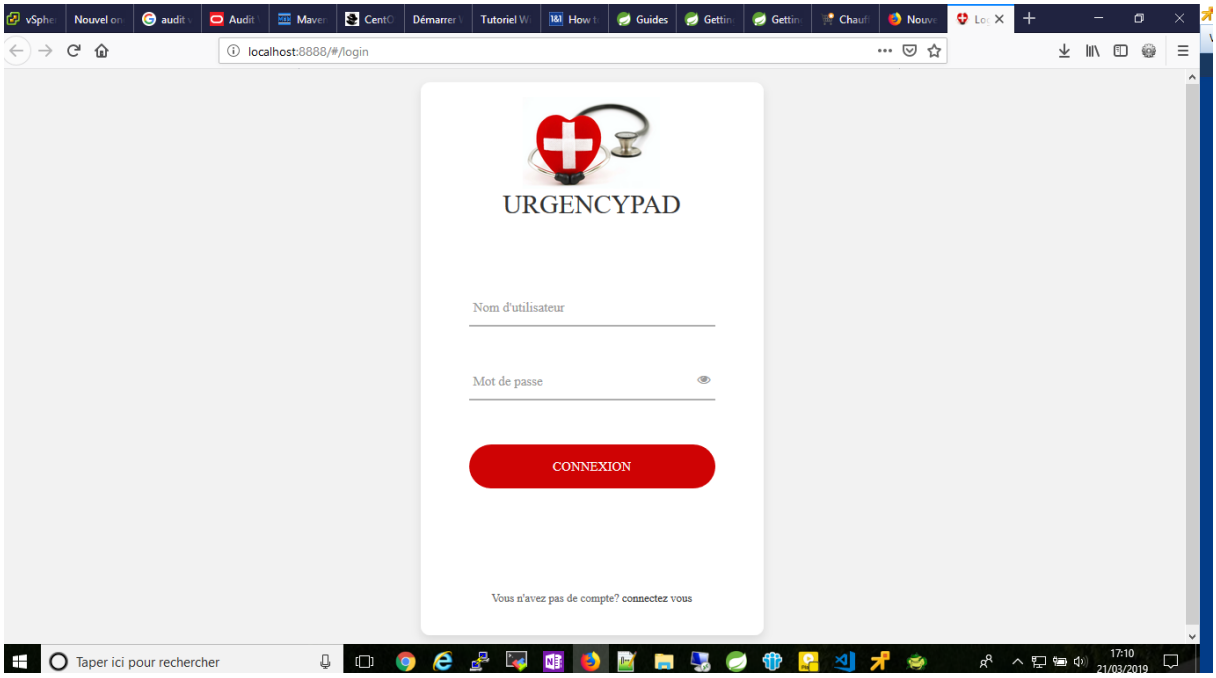


Figure 22 : Interface de connexion à l'application web sur le serveur cloud

La figure 23 nous montre, code à l'appui, l'environnement de développement JAVA que nous avons utilisé pour implémenter notre application URGENCYPAD (Confère annexe 17, pour les autres interfaces).

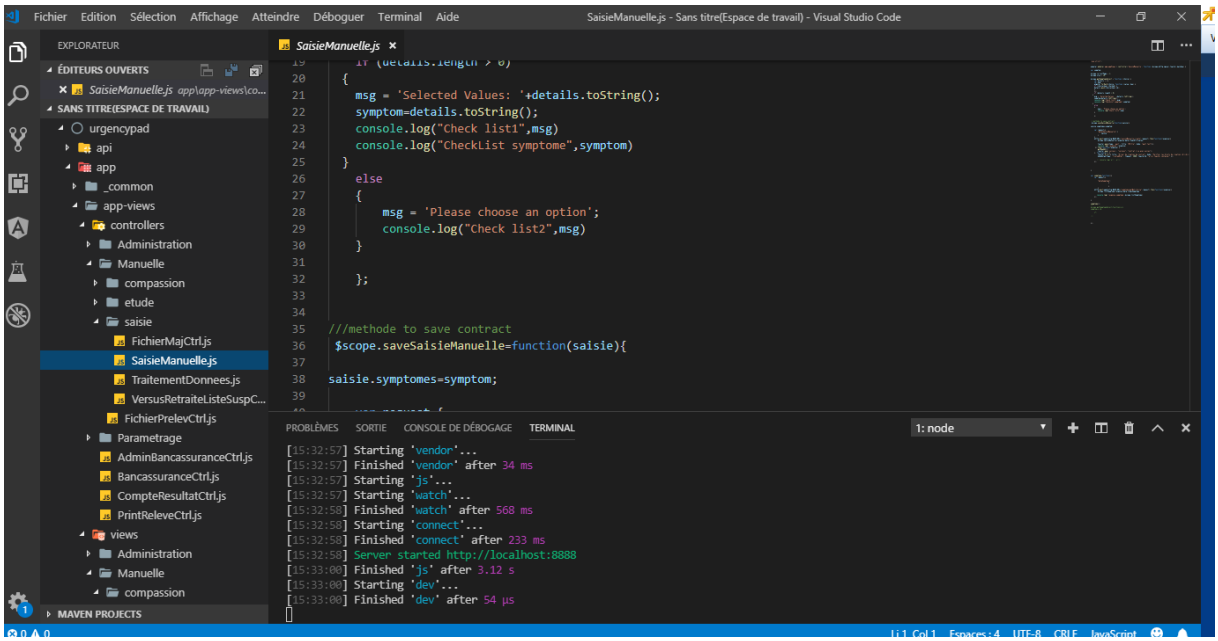


Figure 23: Quelques bytes codes de l'application URGENCPAD en environnement JAVA et Apache Tomcat

2.3.2. Test de *Student* pour la comparaison de notre méthode de collecte des constantes et la méthode de l'Institut de Cardiologie d'Abidjan

A la lumière de la revue de littérature, pour comparer la convergence de deux méthodes de mesure sur une population donnée, plusieurs solutions s'offrent au chercheur ; à savoir : la famille des analyses décisionnelles, les méthodes de comparaison de distributions et les tests de comparaison de moyennes. En effet, soit un échantillon de moyenne μ. Pour comparer cette moyenne à une valeur de référence, deux tests paramétriques sont possibles :
-**Le test t de *Student*** : si on ne connaît pas la vraie variance de la population dont est extrait l'échantillon ; on utilise alors comme estimateur de la variance, la variance de l'échantillon s^2.
-**Le test z :** si on connaît la vraie variance σ^2 de la population. Les **tests t et z** pour un échantillon permettent de déterminer si la moyenne d'un échantillon est significativement différent d'une valeur D donnée (**test t** de ***Student*** si la variance de l'échantillon est estimée, **test z** si elle est connue). Pour notre problématique, qui soulevait la question de savoir si les deux méthodes de mesure donnent statistiquement la même mesure sur les patients, nous avons choisi la méthode de comparaison de moyennes.

En effet, avec la comparaison des moyennes, nous pouvons confirmer ou infirmer qu'en moyenne, les deux méthodes donnent la même mesure sur les constantes considérées, avec une erreur de première espèce bien définie. Nous avons choisi le test d'égalité de moyenne de ***Student*** [75]. L'hypothèse H0 du test est qu'il n'y ait pas une différence significative entre les deux moyennes, pour la constante considérée au seuil de 5%. Cette hypothèse sera rejetée si la probabilité est inférieure à 0,05 ou la statistique est supérieure à 1,96. Ces données ont été introduites dans le logiciel métier de traitement statistique **STATA** et un test d'égalité de moyenne sur les constantes a été réalisé. Ces données pouvaient aussi être traitées dans le **logiciel 'R'**.

2.3.3. Algorithme d'évaluation des constantes acquises par nos multi-capteurs

Voici l'exemple de l'algorithme du RC (Rythme Cardiaque) que nous généralisons pour les autres constantes collectées. Il nous permet d'obtenir, dans l'application URGENCYPAD, un jeu de couleur pour chaque constante collectée. Le Rythme cardiaque (RC, ou Battements cardiaques par minute, a pour valeurs normales (60-100 Bpm). Nous considérons qu'il est critique s'il est au moins supérieur ou inférieur aux valeurs

normales de ±20 Bpm. Une valeur comprise entre (40 Bpm<RC<60 Bpm ou 100 Bpm<RC<120 Bpm) est anormale alors qu'une valeur RC<40 Bpm ou RC>120 Bpm est critique) ; la marge critique que nous avons définie étant à ± 20 Bpm. La figure 24 illustre cette classification des valeurs de constantes.

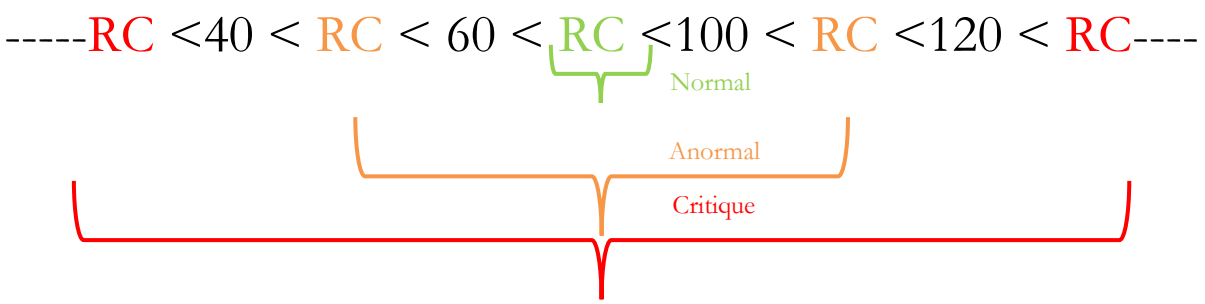


Figure 24: Classification des valeurs de constantes avec un jeu de couleurs.

L'algorithme suivant nous a permis de déterminer automatiquement sur l'application mobile, si la constante collectée était normale, anormale ou critique.

Algorithme :

```
Variables :

RC_min, RC_max, RC : entier
Couleur= {rouge, vert, orange}
Debut
   Ecrire ('entrez la valeur du RC') ;
   Lire (RC) ;
   Si (RC_min <RC<RC_max) alors
      Couleur= vert ;
   Sinon
      Si ((RC_min -20 < RC<RC_min) ou (RC_max < RC<RC_max + 20)) alors
         Couleur = orange ;
      Sinon
         Couleur =rouge ;
      Fin si
   Fin si
   Ecrire ('La couleur est : ' Couleur ') ;
Fin
```

2.3.4. Algorithme de prédiction de pathologies à partir des signaux acquis et des symptômes renseignés sur notre application mobile

Notre deuxième algorithme consiste à tester les constantes collectées, en les comparant aux valeurs normales, selon l'enchaînement suivant (figure 25) :

1-Comparer la valeur collectée avec la valeur normale ;

2-Si la valeur est normale, la classer parmi les signaux normaux. Si la valeur est anormale ou critique, passer à l'instruction suivante ;

3-Dénombrer les symptômes observés sur le patient et faire le ratio avec les symptômes connus de la pathologie que la valeur physiologique adresse ;

4-Sélectionner les trois pathologies qui obtiennent le meilleur score par ordre décroissant (voir figure 23) ;

5-Afficher, en suggérant, les trois pathologies que risque le patient par ordre de chance d'élection (% des symptômes).

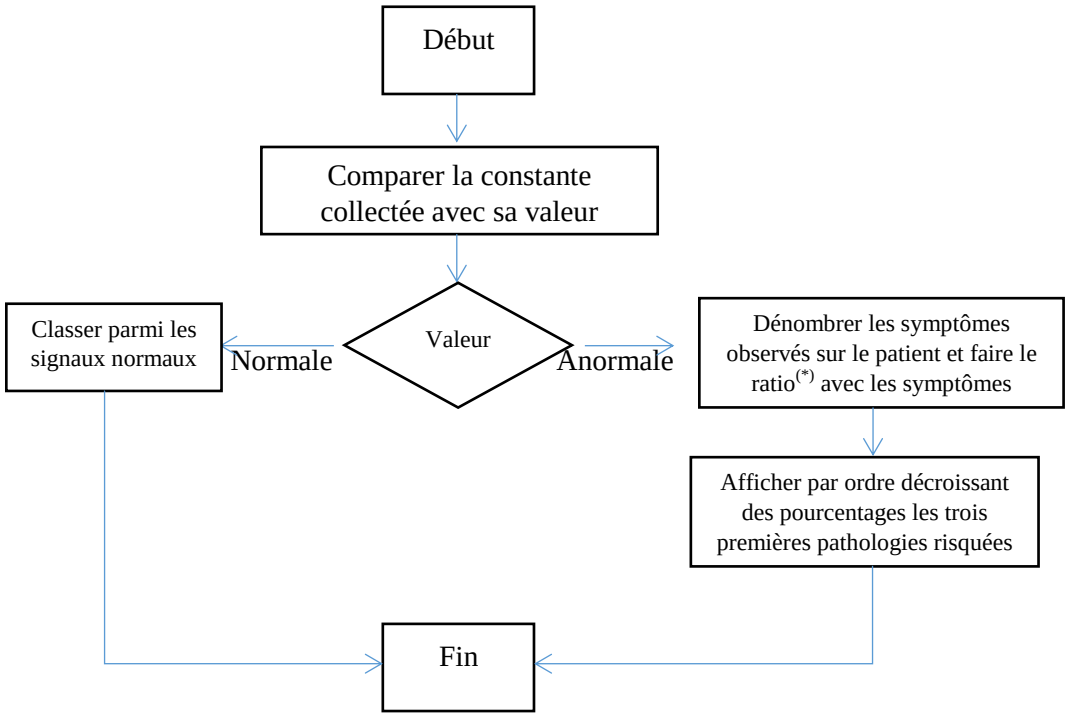


***Figure 25*:** Algorithme de prédiction des trois pathologies risquées par le patient collecté.

(*) Ce ratio est inspiré de la loi de Bayes [76] :

$$p(A/B)=\frac{p(A\cap B)}{p(B)} \tag{2.1}$$

Avec

$$p(A\cap B)=p(A)\cdot p(B/A) \tag{2.2}$$

$$p(B)=p(A\cap B)+p(A^{\bullet}\cap B)=p(A)\cdot p(B/A)+p(A^{\bullet})\cdot p(B/A^{\bullet}) \tag{2.3}$$

La loi généralisée de la loi de Bayes donne :

$$p(A/B)=\frac{p(A)\cdot p(B/A)}{p(A)\cdot p(B/A)+p(A^{\bullet})\cdot p(B/A^{\bullet})} \quad (2.4)$$

Le terme *P(A)* est la probabilité a priori de A. Elle est « antérieure » au sens qu'elle précède toute information sur B. P(A) est aussi appelée la probabilité marginale de A. Le terme *P(A|B)* est appelée la probabilité conditionnelle de A sachant B (ou encore de A sous condition B). Elle est « postérieure », au sens qu'elle dépend directement de B. Le terme *P(B|A)*, pour un A connu, est appelé la fonction de vraisemblance de B. De même, le terme P(B) est appelé la probabilité marginale ou a priori de B.

Nous avons considéré le nombre de symptômes collectés comme p(A∩B) et le nombre classique connu de symptômes d'une pathologie normale comme p(B), la probabilité à priori. Cet algorithme, de la figure 25, nous a donc permis d'obtenir les résultats contenu dans le tableau 5 de prédiction, à la page 59.

2.3.5. Détection et classification de l'hypertension artérielle par réseaux de neurones artificiels (RNA)

Dans cette partie de notre travail, nous avons mis au point une nouvelle technique de cybersanté, pour détecter l'hypertension et classifier ses différents stades, afin d'aider les médecins, à distance, dans leur diagnostic. Basé sur le réseau neuronal artificiel (RNA), notre algorithme de Levenberg-Marquardt (***trainlm***) aide à détecter l'hypertension tôt chez les patients reçus aux urgences, en particulier dans les centres médicaux des régions les plus reculées du pays. Il nous fournit surtout une classification des stades de l'hypertension.

Pour notre réseau de neurones artificiels, de septembre 2016 à décembre 2018, les constantes non invasives de 120 patients ont été recueillies. Leur tension artérielle a été mesurée à l'aide d'un multi capteur appelé "6 en 1 Health Monitor" (Figure 16 de la page 40), pendant deux jours consécutifs, tôt le matin. Un prélèvement similaire a été effectué à l'aide d'un tensiomètre conventionnel dans les mêmes conditions. Pour le test de notre algorithme de détection, de janvier à mars 2019, à l'Institut de Cardiologie d'Abidjan, 40 patients ont été prélevés deux fois de suite par notre méthode et par la méthode de la médecine conventionnelle, dans un intervalle de temps allant de une à deux heures, après leur arrivée aux urgences. Leur fréquence cardiaque a également été recueillie. On note, enfin, qu'aucune étude n'a encore été menée sur la classification de l'hypertension avec réseau neuronal artificiel à l'Institut de Cardiologie d'Abidjan en Côte d'Ivoire. Le tableau 2 présente notre

codification avec une base binaire à 7 chiffres, pour chaque stade de la classification européenne de l'hypertension. La classification aide à mieux gérer l'hypertension et ses aggravations [77], avec une performance satisfaisante [78].

Tableau 2: Codification de l'hypertension artérielle pour la classification automatique

Catégorie	Systolique		Diastolique	Code
Optimale	<120	et	<80	0000001
Normale	120 - 129	et/ou	80 - 84	0000011
Normal haut	130 - 139	et/ou	85 - 89	0000111
Hypertension stade 1	140 - 159	et/ou	90 - 99	0001111
Hypertension stade 2	160 - 179	et/ou	100 - 109	0011111
Hypertension stade 3	>180	et/ou	>110	0111111
Hypertension systolique isolée	>140	et/ou	<90	1111111

2.3.5.1. Méthodologie et Matériel de notre RNA

Notre base d'entrainement est composée de 120 patients prélevés pour la tension artérielle. Elle a été divisée en trois groupes : 84 ont été utilisés pour l'entraînement, 18 pour la validation et 18 pour les tests, ce qui représente une distribution de 70%, 15% et 15%.

Le but de l'application de la méthode RNA est de construire des équations mathématiques pour prédire et classifier la tension artérielle. Nous avons reconstruit une base de données de 120 échantillons et 4 informations sur la tension artérielle comme entrée du réseau et une base de données de (120 x 7) pour la sortie du réseau. Les données d'entraînement sont présentées au réseau pendant l'entraînement, et le réseau est ajusté en fonction de son erreur. Les données de validation sont utilisées pour mesurer la généralisation du réseau et pour arrêter la formation, lorsque la généralisation cesse de s'améliorer. Les données d'essai n'ont aucun effet sur l'entraînement et fournissent ainsi une mesure indépendante de la performance du réseau, pendant et après l'entraînement. Le modèle de classification mis au point utilise un réseau en aval à deux couches, avec une fonction de

transfert hyperbolique tangente (***Tanh***) dans la couche cachée, et une fonction de transfert linéaire dans la couche de sortie. Le nombre de neurones cachés par défaut est de 10.

2.3.6. Algorithme de sécurisation de transmission de données médicales par téléphonie mobile

2.3.6.1. Méthodologie et Matériels de notre Algorithme RSA modifié

2.3.6.1.1. Fonctionnement de RSA original

Génération de la clé privée

a) Sélectionner *p* et *q*, tous deux des nombres premiers, *p* étant différent de *q*.

b) Calculer n = *p* x *q*.

c) Calculer la valeur phi d'Euler de *n*, ø (*n*) = (*p* -1) x (*q*-1).

d) Sélectionner au hasard un entier *e* qui satisfait aux conditions suivantes :

PGCD (Ø (*n*), *e*) = 1; avec 1 < *e* <Ø(*n*).

e) Calculer un nombre pris au hasard *d* tel que d = ɵ-1 (mod Ø (*n*)), ou encore :

d∗e≡1 (mod Ø (*n*))

f) Clé publique CPU = {*e*, *n*}.

g) Clé privée CPR = {*d*, *n*}.

Le cryptage

Le cryptage est fait grâce à la clé publique : {*e*, *n*}

a) Le texte plein - Message (M)

b) Le texte crypté - C = M^e mod *n*.

Le décryptage

Le décryptage s'opère par la clé privée : {*d*, *n*}

a) Texte crypté - C

b) Texte plein - M = C^d mod *n*. Où M est le message d'origine, *p* et q étant des nombres premiers. 'n' est leur modulo commun, *e* et *d* étant respectivement la clé publique et privée.

2.3.6.1.2. Fonctionnement de MRSA de Muhammad

Génération de la clé privée

a) Sélectionner *p* et *q*, *r*, *s*, tous quatre des nombres premiers, *p*, *q*, *r*, *s* étant différents.

b) Calculer n = $p * q * r * s$.

c) Calculer la valeur phi d'Euler de n, Ø (*n*) = (*p* -1) x (*q*-1) x (*r*-1) x (*s*-1).

d) Sélectionner au hasard un entier *e* et *f* qui satisfait aux conditions suivantes :

PGCD (Ø (*n*), *e*) = 1; 1 < *e* <Ø(*n*) ;

PGCD (Ø (*n*), *f*) = 1; 1 < *f* <Ø(*n*);

e) Calculer un nombre pris au hasard *d* tel que *d* = e-1 (mod Ø (*n*)),

ou encore : $d * e \equiv 1$ (mod Ø (*n*))

Calculer $f * g \equiv 1 (\text{mod } Ø (n))$

f) Clé publique CPU = {*e*, *f*, *n*}.

g) Clé privée CPR = {*d*, *g*, *n*}.

Le cryptage

Le cryptage s'opère par la clé publique : {*e*, *f*, *n*}

a) Texte crypté - C

b) Texte plein - M = $((M^e \text{ mod } n)^f) \text{mod } n)$. Où M est le message d'origine, *p* et *q*, *r*, *s* étant des nombres premiers. 'n' est leur modulo commun, *e*, *f*, *n* et *d*, *g*, *n* étant respectivement la clé publique et privée.

Le décryptage

Le décryptage s'opère par la clé privée : {*d*, *g*, *n*}

a) Texte crypté - C

b) Texte plein - M = $((C^g \text{ mod } n)^d) \text{ mod } n)$. Où M est le message d'origine, *p* et *q*, *r*, *s* étant des nombres premiers. 'n' est leur modulo commun.

2.3.6.1.3. Fonctionnement d'EMSRSA proposé

Génération de la clé privée

a) Sélectionner *p* et *q*, *r*, *s*, tous quatre des nombres premiers, *p*, *q*, *r*, *s* étant différents.

b) Calculer n = $p * q * r * s$.

c) Calculer la valeur phi d'Euler de n, Ø (*n*) = (*p* -1) x (*q*-1) x (*r*-1) x (*s*-1).

d) Sélectionner au hasard un entier *e* et *f*, *h*, *i* qui satisfait aux conditions suivantes :

PGCD (Ø (*n*), *e*) = 1; 1 < *e* <Ø(*n*) ; PGCD (Ø (*n*), *f*) = 1; 1 < *f* <Ø(*n*);

PGCD (Ø (*n*), *h*) = 1; 1 < g <Ø(*n*);

e) Calculer un nombre pris au hasard *d* tel que d = e-1 (mod Ø (*n*)),

ou encore $d*e \equiv 1 \pmod{Ø(n)}$

Calculer $f*g*h*i \equiv 1 \pmod{Ø(n)}$

f) Clé publique CPU = {*e*, *f*, *h*, n}.

g) Clé privée CPR = {*d*, *g*, *i*, *n*}.

Le cryptage

Le cryptage s'opère par la clé publique : {*e*, *f*, *h*, *n*}

a) Texte crypté - C

b) Texte plein - M = $((((M^e \bmod n)^f) \bmod n)^g) \bmod n)$. Où M est le message d'origine, p et q, r, s étant des nombres premiers. 'n' est leur modulo commun, *e*, *f*, *h*, *n* et *d*, *g*, *i*, *n* étant respectivement la clé publique et privée.

Le décryptage

Le décryptage s'opère par la clé privée :{*d*, *g*, *i*, *n*}

a) Texte crypté - C

b) Texte plein - M = $((((C^h \bmod n)^d) \bmod n)^i) \bmod n)$. Où M est le message d'origine, *p* et *q*, *r*, *s* étant des nombres premiers. 'n' est leur modulo commun. Nous avons programmé en environnement JAVA Eclipse version Oxygen, une interface pour tester les différents algorithmes RSA original, MRSA de Muhammad et EMSRSA que nous avons établi.

La figure 26 représente l'interface JAVA qui a servi à tester les algorithmes RSA original, MRSA de Muhammad et EMSRSA que nous avons établi. (Voir annexe 18, pour les

autres interfaces). La figure 27 représente le diagramme de flux de notre algorithme EMSRSA.

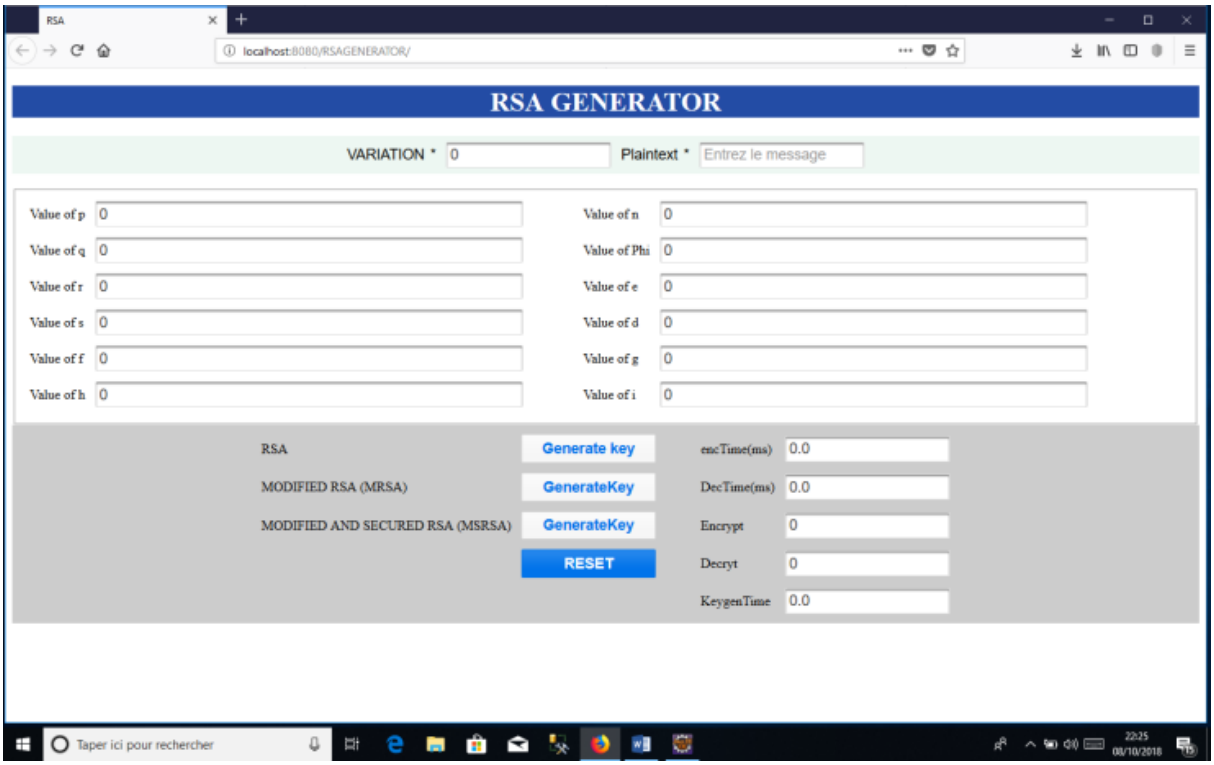


Figure 26: Interface java 'RSA GENERATOR' pour une taille de bit à 0.

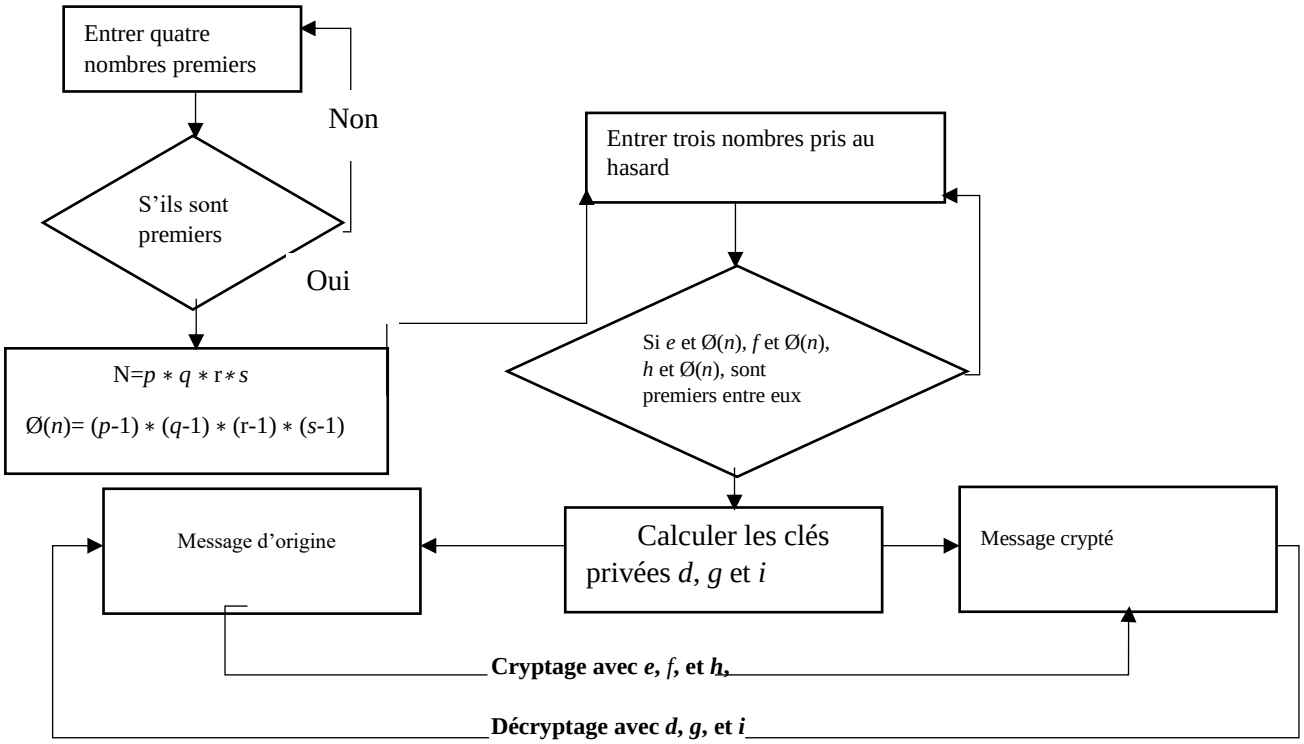


Figure 27: Diagramme de flux de notre Algorithme (EMSRSA), inspiré de (MRSA) de Muhammad et *al*.

2.3.6.2. Implémentation

Notre implémentation de l'algorithme s'est fait en environnement JAVA version OXYGEN sur un ordinateur Lenovo, Intel® Core TM i5 CPU M520 (2.40 GHz)*(2.40 GHz), avec 8 Go de RAM. Le défi de sécurité de l'algorithme RSA et d'autres algorithmes modifiés tels que celui de Muhammad, est de consolider la factorisation du nombre 'n', afin d'augmenter la difficulté de détection de la clé par un hacker. Nous avons choisi l'environnement JAVA pour développer nos applications, car elle nous offrait plus de librairies, surtout pour les grands nombres et fonctions mathématiques, contrairement aux autres environnements de développement comme Visual studio de Microsoft avec C#.

Conclusion partielle

Ce deuxième chapitre nous a permis de présenter clairement les matériels que nous avons utilisés pour résoudre nos hypothèses, notamment notre échantillon biologique composé de 120 patients collectés pour l'entrainement et la validation de notre algorithme de classification par réseaux de neurones, et 40-60 autres patients dont les données de santé ont été collectés pour les tests. Il a présenté le nouveau dispositif de collecte des constantes sur les patients, composé de trois multi-capteurs qui sont : « 6 in 1 Health Monitor », « 3 in 1 EasyMate GCU » et « 2 in 1 EasyMate Ghb ». Il a présenté également les méthodologies utilisées, à savoir :

- La nouvelle application mobile que nous avons développée en environnement JAVA, pour permettre la collecte des constantes sur un smartphone ou une tablette ;
- Le test statistique de *Student*, pour confirmer la fiabilité des constantes collectées par notre méthode ;
- Le nouvel algorithme d'évaluation de ces constantes collectées sur les appareils mobiles ;
- L'algorithme de prédiction de pathologies à partir de ces constantes et des symptômes ;
- Le modèle neuronal de classification de pathologie telle que l'hypertension artérielle ;
- Le nouvel algorithme basé sur l'amélioration de celui de RSA, pour la sécurisation des données transmises par téléphonie mobile.

CHAPITRE 3 : RESULTATS ET DISCUSSION

Les méthodes et méthodologies que nous avons utilisées nous ont permis d'obtenir les résultats que nous présentons et analysons dans les paragraphes qui suivent :

3.1. Résultat du test de *Student* pour la comparaison des constantes collectées par notre méthode et celle de l'Institut de Cardiologie d'Abidjan (ICA)

Ce tableau 3 présente le test de *Student* appliqué sur les constantes d'un échantillon de 40 patients.

Tableau 3: Résultats de test d'égalité de moyenne sur les constantes

variables	obs	MoyVM	MoyNM	écart-type	t-stat	DF	Prob
HB (g/100ml)	40	11,22	11,04	0,36	-12,88	-0,18	0,00
TC (°C)	40	36,19	36,14	0,19	-0,63	-0,05	0,54
HT (g/100ml)	40	32,89	97,97	17,88	3,61	65,08	0,00
SPO2 (%)	40	97,88	97,9	0,23	1,00	0,03	0,32
DIA (mmHg)	40	88,82	88,79	4,87	-1,00	-0,03	0,32
GL	44	1,26	1,26	0,07	0,04	0,00	0,97
SYS (mmHg)	40	142,43	142,43	7,18	2,00	0,00	1,00
RC (Bpm)	40	93,925	93,95	2,86109	1,00	0,03	0,32

Le test d'égalité des moyennes a donné une probabilité supérieure comprise entre 0,05 et 0.01 pour les constantes suivantes : La température (TC), la saturation du sang en oxygène (SPo2), la tension diastolique (DIA), la tension systolique (SYS), la glycémie (GL) et le rythme cardiaque (RC). L'hypothèse H0 est donc confirmée pour ces constantes et prouve que notre nouvelle méthode donne des résultats semblables aux valeurs collectées par les outils de l'ICA. En revanche, nous avons rejeté cette hypothèse pour le taux d'hémoglobine et le taux d'hématocrite dans le sang, car la probabilité a donné une valeur inférieure à 0.05, qui est le seuil d'acceptation. Cependant, il nous appartiendra de demander à nos fournisseurs d'équipement d'améliorer certains paramètres de mesure notamment l'hémoglobine, le taux d'hématocrite et le taux de bon cholestérol dans le sang.

Les graphiques suivants viennent illustrer la vérification de l'hypothèse H0 du test de *Student* par les constantes collectées par notre nouvelle méthode.

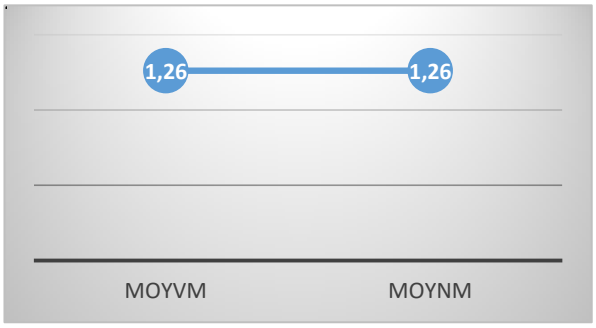


Figure 28: Graphique du test de *Student* pour la Glycémie (GL)

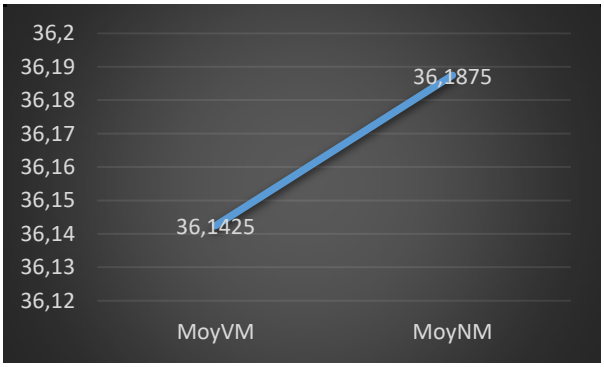


Figure 29: Graphique du test de *Student* pour la Température (TC)

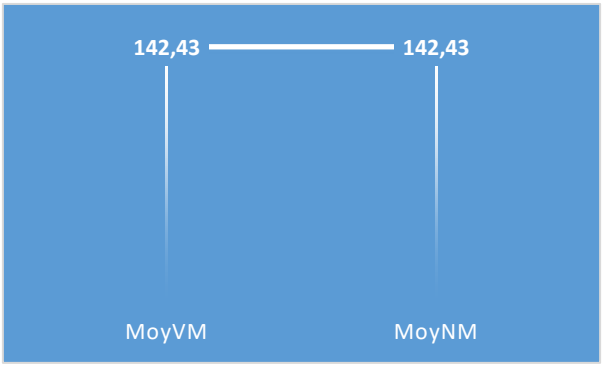


Figure 30: Graphique du test de *Student* pour la diastolique (DIA)

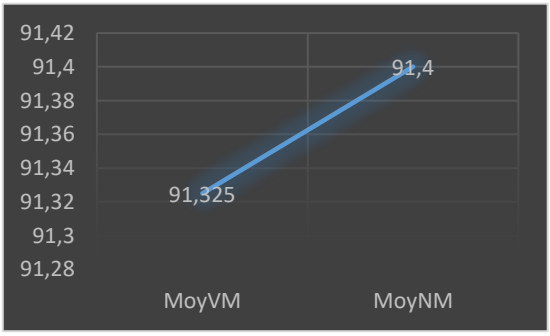


Figure 31: Graphique du test de *Student* pour la pression systolique (SYS)

Les graphiques ci-dessus s'interprètent comme suit : ils donnent les deux moyennes obtenues par les deux différentes méthodes utilisées. A cet effet, l'abréviation MoyVM est mise pour la méthode de l'hôpital et MoyNM est mise pour la nouvelle méthode proposée. Ainsi, avec l'ancienne, on a obtenu une moyenne de 91,325 contre 91,4 pour notre nouvelle méthode proposée. Sur quarante personnes enquêtées, nous avons une différence de 0,075 de moyenne entre les deux méthodes. Ce qui est bien supérieur au seuil de 0,05 de l'hypothèse H0. Le tableau 4 présente l'interface de calcul des probabilités du test de *Student*, dans le logiciel de statistique STATA.

Tableau 4: Traitement statistique des données du Rythme cardiaque dans STATA

Variable	Obs	Mean	Std. Err.	Std. Dev.	[95% Conf.	Interval]
RC1	40	91.325	3.100742	19.61081	85.05316	97.59684
RC2	40	91.4	3.091925	19.55505	85.14599	97.65401
diff	40	-.075	.0659011	.4167949	-.2082975	.0582975

```
    mean(diff) = mean(RC1 - RC2)                                  t =  -1.1381
Ho: mean(diff) = 0                              degrees of freedom =       39

Ha: mean(diff) < 0           Ha: mean(diff) != 0           Ha: mean(diff) > 0
Pr(T < t) = 0.1310         Pr(|T| > |t|) = 0.2620          Pr(T > t) = 0.8690
```

3.2. Résultat de la prédiction de pathologies à partir des signaux acquis et des symptômes renseignés sur notre application mobile

Le Tableau 5 indique que, globalement, notre algorithme de prédiction des trois pathologies les plus prabables pour le patient, donne des valeurs convergentes vers les diagnostics de l'ICA.

Tableau 5: Prédiction des trois premières pathologies des 40 patients collectés à l'ICA avec notre deuxième algorithme de prédiction.

Patient N°	Pathologie 1ère	Pathologie 2ème	Pathologie 3ème	Diagnostic ICA	Résultat
1	Dyspnée 100%	CMD 75%	Anémie 36%	Dyspnée	Convergent
2	Dyspnée 100%	Anémie 45%	Asthénie 36%	Dyspnée, OMI	Convergent
3	Dyspnée 100%	CMD 50%	Péricardite 50%	Dyspnée	Convergent
4	Dyspnée 100%	Hypertension 67%	Hypoxie 25%	Dyspnée	Convergent
5	Dyspnée 100%	Anémie 45%	Asthénie 36%	Dyspnée, OMI	Convergent
6	Dyspnée 100%	Tachycardie 56%	Anémie 27%	Dyspnée, OMI	Convergent
7	Dyspnée 100%	Anémie 91%	Tachycardie 56%	Dyspnée	Convergent
8	Dyspnée 100%	Anémie 55%	Hypertension 23%	Dyspnée	Convergent

9	Tachycardie 89%	Anémie 34%	0bésité 22%	Syncope	Néant
10	Tachycardie 77,78%	Anémie 54,54%	Asthénie 36,36%	Tachycardie	Convergent
11	Hypertension 66,67%	Tachycardie 55,56%	Hypoxie 5,56 %	Hypertension	Convergent
12	Dyspnée 100%	CMD 75%	Anémie 27%	Dyspnée	Convergent
13	Dyspnée 100%	Asthénie 36%	Hypertension 33%	Dyspnée	Convergent
14	Dyspnée 100%	Hypertension 27%	Anémie 19%	Dyspnée	Convergent
15	Péricardite 100%	CMD 63%	Anémie 55%	Péricardite	Convergent
16	Dyspnée 100%	CMD 87,5%	Anémie 27,27%	Dyspnée	Convergent
17	Dyspnée 100%	CMD 37,5%	Tachycardie 22,22%	Dyspnée	Convergent
18	Dyspnée 100%	Tachycardie 78%	CMD 38%	Dyspnée	Convergent
19	Dyspnée 100%	CMD 75%	Anémie 37%	Dyspnée	Convergent
20	Tachycardie 78%	CMD 75%	Dyspnée 50%	Tachycardie	Convergent
21	Asthénie 64%	CMD 63%	Tachycardie 56%	Fatigue, Vertiges	Convergent
22	CMD 50%	Tachycardie 33,33%	0bésité 20%	CMD	Convergent
23	Hypertension 78%	Asthénie 17%	Hypoxie 6 %	Hypertension	Convergent
24	Hypertension 77,77%	Dyspnée 50%	Tachycardie 33,33%	Hypertension	Convergent
25	Dyspnée 100%	Anémie 54%	Hypoxie 31 %	Dyspnée	Convergent
26	CMD 63%	Dyspnée 50%	Hypertension 22%	CMD	Convergent
27	Dyspnée 100%	Anémie 55%	Asthénie 25%	Dyspnée	Convergent
28	Tachycardie 78%	Asthénie 25%	Anémie 18%	Tachycardie	Convergent
29	Dyspnée 100%	Tachycardie 67%	CMD 63%	Dyspnée	Convergent
30	Dyspnée 100%	CMD 75%	Anémie 45%	Dyspnée	Convergent
31	Hypertension 78%	Précordialgie 67%	Anémie 27%	Hypertension	Convergent
32	Dyspnée 100%	CMD 63%	Anémie 45%	Dyspnée	Convergent
33	Dyspnée 100%	Anémie 37%	Hypertension 23%	Dyspnée	Convergent
34	Hypertension 78%	Asthénie 37%	Asthénie 36,36%	Hypertension	Convergent
35	Hypertension 78%	Asthénie 37%	Asthénie 36,36%	Hypertension	Convergent
36	Hypertension 78%	Asthénie 37%	Hypoxie 12 %	Hypertension	Convergent
37	Dyspnée 100%	Hypertension 55,56%	Anémie 27,27%	Dyspnée	Convergent
38	Anémie 37%	Hypertension 23%	Hypoxie 17 %	Anémie aigue	Convergent
39	Dyspnée 100%	Anémie 63,63%	CMD 62,5%	Dyspnée	Convergent
40	Dyspnée 100%	Anémie 28%	Hypertension 23%	Dyspnée	Convergent

Pour le patient N°1, par exemple, notre algorithme prédit la dyspnée, ce qui est conforme au diagnostic des médecins qui ont ausculté le même patient avec leurs outils classiques. (Ce résultat a été certifié par Dr Jean Louis Konan). Le tableau 6 et la figure 32 ne font que démontrer les statistiques concernant cette convergeance.

Tableau 6:: Tableau de performance de notre algorithme de prédiction des trois pathologies risquées par le patient, en fonction des symptômes collectés.

Pathologies convergentes (en %)	97,5
Pathologies non convergentes (en %)	2,5

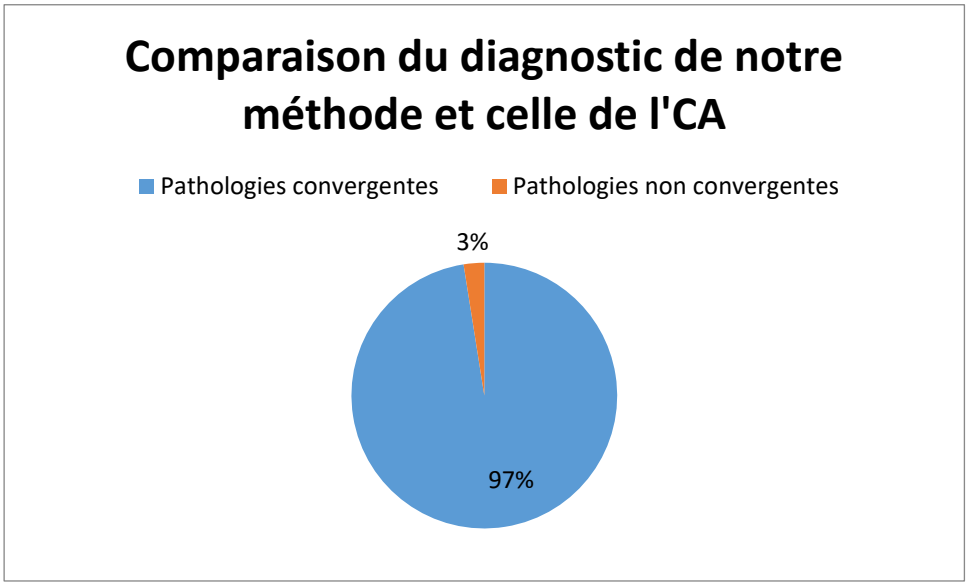


Figure 32: Courbe de performance de notre algorithme de prédiction.

Au vu du taux de 97,5 % de conformité de notre diagnostic avec celui de la fiche patient des malades de l'ICA, nous affirmons que notre nouvelle méthode d'acquisition des constantes de santé est performante.

Le tableau 7 et la figure 33 nous indiquent bien que la dyspnée, l'hypertension artérielle et la tachycardie arrivent en tête des pathologies aux urgences de Cardiologie. Ce résultat est conforme aux statistiques des causes d'entrées en cardiologie [9].

Tableau 7: Simulation d'analyse Big Data du taux de prévalence des pathologies au sein des 40 patients étudiés.

Pathologie	Taux de prévalence
Dyspnée	0,6
Anémie	0,025
Asthénie	0,025
CMD	0,05
Hypertension artérielle	0,175
Péricardite	0,025
Tachycardie	0,1

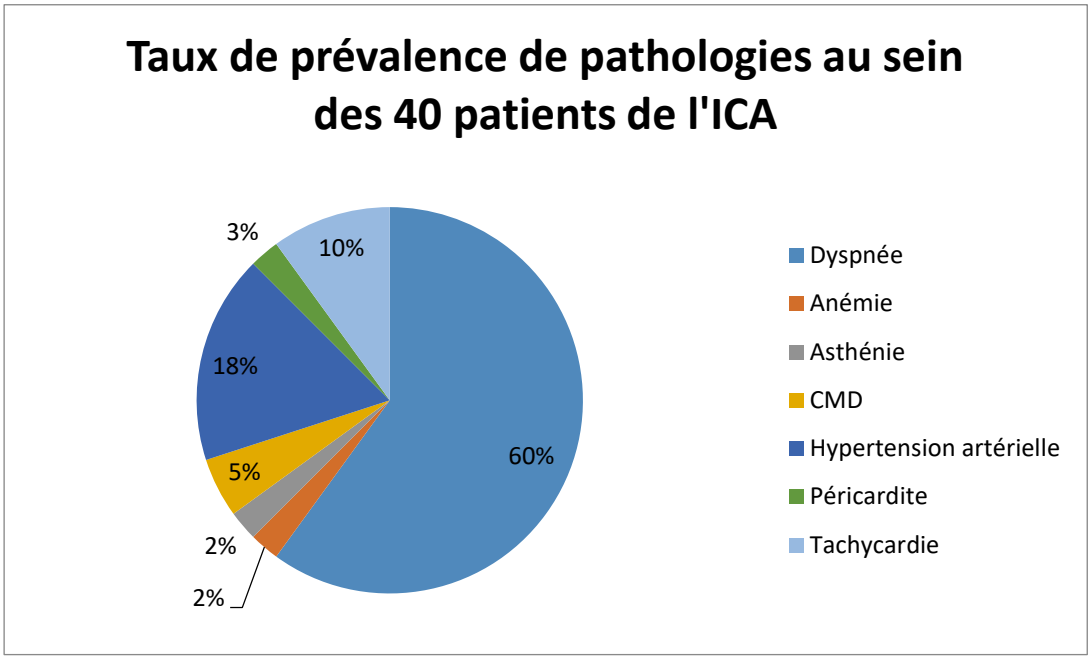


Figure 33: Taux de prévalence de chaque pathologie au sein du service des urgences de l'ICA

3.3. Résultat des ECG obtenus avec notre méthode et celle de l'ICA

Nous avons réalisé une quarantaine de prises d'ECG simultanément par notre dispositif « 6 in 1 Health Monitor » et l'équipement d'ECG de l'ICA. Nous avons pu comparer les ECG des deux méthodes, au niveau de la dérivation D1, et avons obtenu les résultats suivants (figure 34 et 35) :

Figure 34: ECG 9 obtenu avec notre méthode

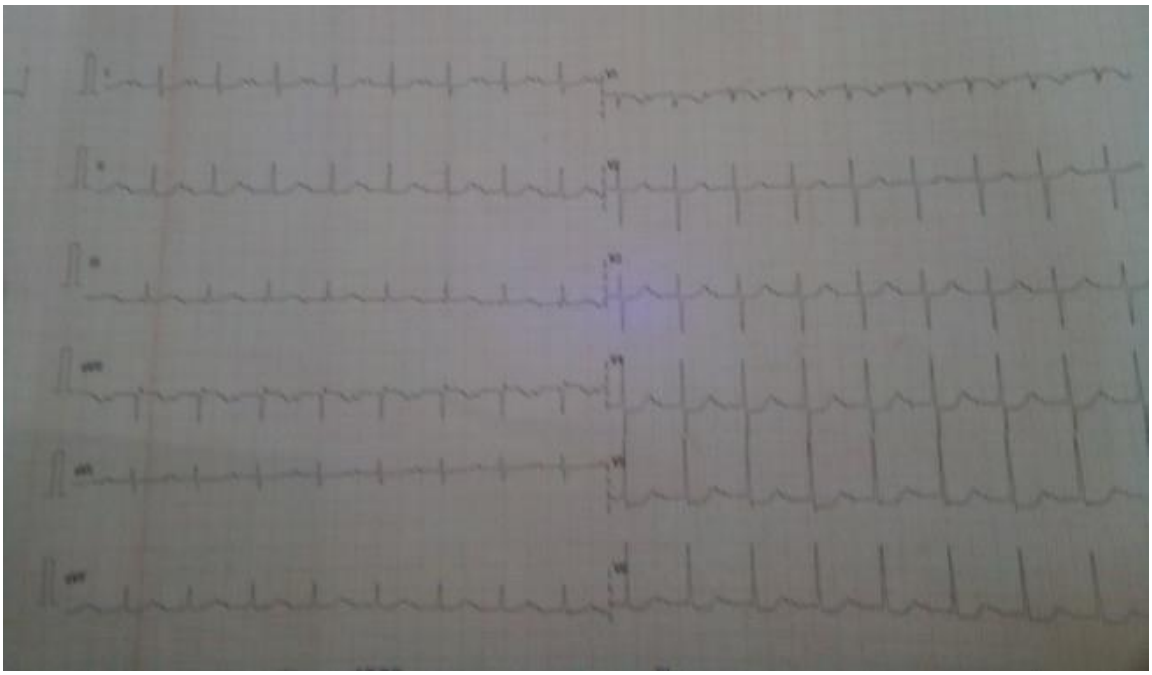


Figure 35: Le même ECG obtenu avec la méthode de l'ICA

Les autres ECG comparés sont confinés en annexe 20.

Tableau 8: Interprétation des ECG des deux méthodes par un Cardiologue de l'ICA.

Numéros ECG	**MORPHOLOGIE CONVERGENTE**	**FREQUENCE CONVERGENTE**			**REMARQUES**
		ECG	**APP**		
1	X	123	133	X	
2	N	231	111	N	
3	N	107	113	X	FA/Artefacts
4	N	98	128	N	
5	N	80	76	N	Onde P
6	N	105		N	FA/RS /axe Confusion
7	X	112	103	X	
8	X	101	94	X	
9	X	104	94	X	
10	X	98	98	X	
11	X	98	91	X	
12	X	104	90	X	
13	N	92	90	X	Voltage/ressemble à D2
14	X	114	104	X	
15	X	89	93	X	+/- artefacts
16	X	61	65	X	+/- artefacts
17	X	78	65	X	
18	X	98	69	N	
19	N	100	98	X	QRS OK/P non

20	X	114	105	X	Voltage
21	X	77	69	X	
22	X	113	112	X	
23	X	105	105	X	
24	N	103	103	X	Axe QRS
25	N	80	83	X	
26	N	97	101	X	Plusieurs morphologies QRS
27	X	94	104	X	
28	X	112	103	X	
29	X	73	187	N	
30	X	41	48	X	
31	N	89	98	N	Echec du tracé
32	N	102	101	X	Onde P et repolarisation incorrectes
33	N	60	55	X	Onde P et repolarisation incorrectes
34	X	63	65	X	
35	X	50	57	X	
36	X	84	92	X	
37	X	51	53	X	

3.3.1. Traitement des résultats

Le tableau ci-dessus (où X signifie convergent, alors que N veut dire non convergent) a été dressé par l'un des éminents cardiologues de l'Institut de Cardiologie d'Abidjan, en la personne de Professeur Adoubi Anicet. Sur les 37 ECG, 24 par notre méthode ont donné un résultat convergent avec celui de la méthode de l'ICA, au niveau de la morphologie. 31 ECG par notre méthode ont donné un résultat convergent avec celui de la méthode de l'ICA, au niveau de la fréquence. C'est-à-dire que les complexes de l'ECG se répètent selon le même intervalle, sur le graphe de l'ECG. Le tableau 9 illustre le taux de conformité de nos ECG avec ceux de l'ICA, au niveau de la morphologie et de la fréquence.

Tableau 9: Taux de conformité de nos ECG avec ceux de l'ICA au niveau de la morphologie et de la fréquence.

ECG conformes morphologie	ECG non conformes morphologie	ECG conformes Fréquence	ECG non conformes fréquence
24	13	31	6
64,9%	35,1%	83,7 %	16,3%

3.3.2. Interprétation du tableau des résultats de comparaison d'ECG

Nous pouvons conclure, au vu de ces résultats, en se basant sur les ECG de l'ICA comme référentiels, que notre méthode est fiable à 65% sur la morphologie et à 84% sur la fréquence. Ces résultats sont encourageants, quand on prend en compte la contrainte de la position des patients qui a pu influencer certains ECG de notre méthode, et qui aurait pu améliorer la morphologie et la fréquence de nos ECG. Toujours est-il que ces résultats donnent une idée assez claire au praticien à distance, qui peut demander alors des ECG plus classiques pour conforter son diagnostic.

3.4. Résultat de la détection et de la classification de l'hypertension artérielle par réseaux de neurones artificiels

Nous avons subdivisé chaque échantillon de personnes en deux groupes : les personnes en bonne santé et les personnes malades. Le tableau 10 présente les résultats des paramètres de régression pour l'entraînement, la validation et les tests d'hypertension artérielle.

Tableau 10: Paramètres de régression linéaire.

	Samples	**MSE**	**R-square**
Entrainement	84	$4.51271.10^{-2}$	$9.06817.10^{-1}$
Validation	18	$7.16553.10^{-2}$	$8.5395.10^{-1}$
Test	18	$2.14478.10^{-1}$	$6.69882.10^{-1}$

La sortie du RNA représente la valeur prévue. Les valeurs prévues ont été comparées aux valeurs expérimentales. L'objectif de cette comparaison est de vérifier le modèle. Avant la comparaison, une approximation a été faite en utilisant la valeur de sortie du RNA pour améliorer la prédiction du réseau par rapport au code cible. Voici l'algorithme de cette approximation :

3.4.1. Approximation de notre RNA

Si la valeur de la sortie est inférieure à 0.5, le réseau considère cette valeur comme 0.

Si la valeur de la sortie est supérieure ou égale à 0.5, le réseau considère cette valeur comme 1.

Algorithme d'approximation dans Matlab :

```
% Verification test
Predict_value_approximation=zeros(40,7);
For i=1:length (y3)
For j=1:7
if Predict_value (i,j)<0,5
Predict_value_approximation(i,j)=0;
Else if  Predict_value (i,j)>=0,5
Predict_value_approximation (i,j)=1;
End
End
End.
```

Le Tableau 11 montre que le modèle est efficace pour prédire la valeur expérimentale, car le taux d'erreur (RMSE) est de 0.035, le coefficient de regression et sa valeur ajustée tendent vers 1. Pour valider le modèle, nous avons utilisé une autre base de 40 patients.

Tableau 11: Efficacité de l'approximation

SSE	0,3509
R-square	0,9949
Adjusted R-square	0,9949
RMSE	0,03553

L'équation de regression est ainsi définie par le modèle linéaire polynomial de degré 1:

$$F(x) = p1*x + p2 \quad (3.1)$$

Avec

$$p1 = 0{,}9916\ (0.9301, 1.008) \quad (3.2)$$

$$p2 = -3.587e\text{-}17\ (-0.005953, 0.005953) \quad (3.3)$$

(Confiance à une limite de 95%).

Ce modèle polynomial est efficace si:

p1 tend vers 1; p2 tends vers 0;

Le coefficient de regression (R^2) tends vers 1;

La valeur calculée F(x) est égale à la valeur cible. Ceci refère à une bonne corrélation.

Les paramètres ajustés de regresseion linéaire nous donnent un coefficient de regression R^2 et sa valeur ajustée qui sont à 1, et une coefficient d'erreur au carré qui tend vers 0. Notre modèle est idéal pour classifier l'hypertension artérielle dans ses différents stades.

Tableau 12: Paramètres d'ajustement de régression.

SSE	$9.593.10^{-28}$
R-square	1
Adjusted R-square	1
RMSE	$1.07.10^{-15}$

Nous rappellons que la fonction d'activation utilisée pour les neurones cachés est la tangente hyperbolique (*Tanh*). Ainsi, la relation entre les valeurs prédites et les entrées du réseau, peut être écrite dans le formulaire :

$$N_j = (\sum_{i=1}^{4} IW_i \times input_i) + B_1 \quad (3.4)$$

où :

IW : est le poids des connexions entre la couche d'entrée et la couche cachée.

B1 : biais de la couche d'entrée,

Les poids et biais d'entrée (Tableau 13) permettent le calcul des entrées de l'ensemble des neurones de la couche cachée.

Tableau 13: Poids et biais d'entrée.

	IW1	IW2	IW3	IW4	B1
N1	2,58042329	-1,35575113	0,48398956	-2,29304598	-1,39332009
N2	-0,25224723	-1,76459358	1,8926405	-0,76885063	-2,17620989
N3	0,43261613	0,05132772	1,1435582	-2,08309689	1,30465012
N4	-1,13468874	0,03976861	0,79564137	6,36849645	0,91035239
N5	1,04985401	-1,7174662	-2,14923188	0,42546313	0,46146386
N6	0,02747253	0,43429435	4,13636914	6,30580653	0,32382958

N7	0,5797267	2,98904285	-2,52587991	0,50965214	-2,06056146
N8	2,99450082	3,09033927	-0,77888844	1,18668366	3,80473198
N9	-4,06064766	-0,5484279	0,2505943	-4,1263983	-2,54189067
N10	-1,40645935	-1,71344066	-0,36666111	-1,09185684	-2,79219743

Pour obtenir la valeur de la sortie du neurone nous avons appliqué la fonction d'activation. Dans le cas de la sortie du neurone, N_i a été calculé par la formule suivante :

$$\text{output} = (\sum_{i=1}^{10} \text{LW}_i \times \tanh(\text{N}_i)) + \text{B}_2 \quad (3.5)$$

où :

B2 : biais de la couche de sortie,

LW : poids des connexions entre la couche cachée et la couche de sortie.

Les poids et les biais de sortie (Tableau 14) sont utilisés pour le calcul. Le résultat est un vecteur dont les différentes valeurs correspondent respectivement à différents niveaux de tension artérielle.

Tableau 14: Poids et biais de sortie.

LW1	**LW2**	**LW3**	**LW4**	**LW5**	**LW6**	**LW7**	**LW8**	**LW9**	**LW10**	**B2**
1,91387076	1,03169866	0,86975114	-0,48223712	-0,39481719	-0,73355056	-0,85828691	-0,98861556	-1,29483258	-1,08461972	0,03964006
2,36225872	1,11867008	0,73338295	-0,50297172	-1,89173404	-0,94655414	-1,6379994	-1,15757379	-1,19189306	-1,17661125	0,93432576
2,56200843	1,3300524	0,14846728	-0,75513659	-1,62218245	-0,64780742	-1,87654655	-1,55088595	-1,37530522	-1,58225787	1,54852402
1,81775416	0,29993342	0,5881185	-0,6632305	-0,02011126	0,69844097	-1,08029539	-0,88130346	-1,21553042	-1,05508666	0,22284475
1,88541269	-1,07232858	-0,80085177	0,64690657	0,26954714	-0,12622869	-0,29655459	-1,1519814	-0,889569	-1,30982887	0,76773846
1,60895856	0,40603662	0,38341057	1,0114281	-0,17617575	-0,73372657	-0,1877084	-0,56721097	-0,76752932	-0,88474504	1,03219083

Le Tableau 15 et la figure 36 montrent que notre modèle a été capable de classer correctement les différents degrés d'hypertension artérielle.

Tableau 15: Classification des stades de l'hypertension artérielle avec notre RNA.

N° Personne	Systolique1	Diastolique 1	Systolique 2	Diastolique 2	Pouls	Sortie RNA avec Approximation	Classification
Personne 1	106	98	106	97	107	0001111	Hypertension stade I
Personne 2	205	119	205	119	77	0111111	Hypertension stade III
Personne 3	118	132	117	133	98	1111111	Hypertension systolique isolée

Personne 4	111	103	111	103	85	0011111	Hypertension stade II
Personne 5	108	98	106	96	81	0001111	Hypertension stade I
Personne 6	99	90	99	92	87	0000111	Normale Haute
Personne 7	122	94	122	92	83	0001111	Hypertension stade I
Personne 8	220	108	220	106	81	0001111	Hypertension stade I
Personne 9	148	140	148	139	61	0111111	Hypertension stade III
Personne 10	130	126	130	125	115	0111111	Hypertension stade III
Personne 11	140	103	140	101	133	0001111	Hypertension stade I
Personne 12	231	100	231	98	98	0001111	Hypertension stade I
Personne 13	177	144	177	142	116	0111111	Hypertension stade III
Personne 14	180	98	180	98	69	0001111	Hypertension stade I
Personne 15	150	108	150	106	95	0011111	Hypertension stade III
Personne 16	189	100	189	99	50	0111111	Hypertension stade III
Personne 17	126	90	126	91	129	0000111	Normale Haute
Personne 18	127	76	127	77	76	0000001	Optimale
Personne 19	138	87	137	86	115	0000111	Normale Haute
Personne 20	128	54	128	53	81	0000001	Optimale
Personne 21	128	85	127	85	43	0000111	Normal Haute
Personne 22	92	54	92	53	110	0000001	Optimale
Personne 23	128	73	128	71	94	0000001	Optimale
Personne 24	154	72	153	72	91	1111111	Hypertension systolique isolée
Personne 25	108	70	107	71	72	0000001	Optimale
Personne 26	240	61	241	61	102	1111111	Hypertension systolique isolée
Personne 27	21	69	21	69	101	0000001	Optimal
Person ne 28	102	11	102	10	89	1111111	Hypertension systolique isolée
Personne 29	111	87	111	85	103	0000111	Normal Haute
Personne 30	118	76	118	77	91	0000001	Optimale
Personne 31	204	74	204	71	115	1111111	Hypertension systolique isolée
Personne 32	208	17	208	16	98	1111111	Hypertension systolique isolée
Personne 33	104	84	104	84	110	0000111	Normale Haute
Personne 34	128	83	128	82	89	0000011	Normale

Personne 35	126	87	126	87	96	0000111	Normale Haute
Personne 36	215	84	215	82	90	1111111	Hypertension systolique isolée
Personne 37	187	89	187	88	55	1111111	Hypertension systolique isolée
Personne 38	112	68	110	66	89	0000001	Optimale
Personne 39	139	82	139	80	92	0000011	Normale
Personne 40	119	89	118	89	86	0000111	Normale Haute

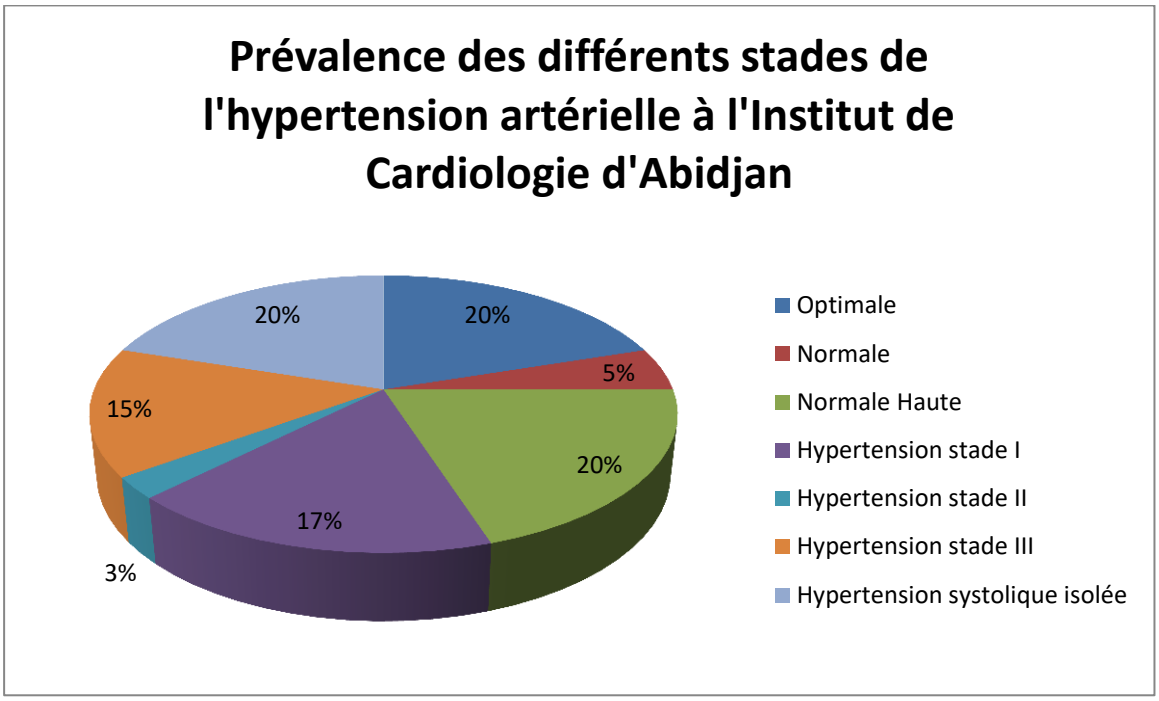


Figure 36: Taux de prévalence de chaque stade de l'hypertension au sein de l'ICA.

De plus, parmi notre population d'essai de 40 personnes, nous avons trouvé 4 personnes à la fois hypertendues et tachycardiques, 6 patients tachycardiques et non-hypertensifs, et 2 patients souffrant d'hypertension systolique isolée et de tachycardie. Nous concluons que la détection de l'hypertension combinée à la fréquence cardiaque pourrait apporter plus d'efficacité dans le diagnostic médical et le traitement.

D'autre part, lorsqu'un nouveau test ou examen est en cours de développement, il est impératif de mesurer sa validité intrinsèque (sensibilité et spécificité). En utilisant un groupe de personnes dont on sait déjà si elles sont atteintes ou non de la maladie, on mesure la capacité du test ou de l'examen à prédire si la maladie est présente.

Vp (Vrai positif) représente le nombre de personnes malades avec un test positif,

Fp (faux positif) représente le nombre de personnes non malades dont le test est positif,
Fn (faux négatif) représente le nombre de personnes malades dont le test est négatif,
Vn (vrais négatif) représente le nombre de personnes non malades dont le test est négatif.

$$\text{Sensitivité} = \frac{Vp}{Vp+Fn} \text{ ; Sensitivité = 91\%} \quad (3.6)$$

$$\text{Specificité} = \frac{Vn}{Vn+Fp} \text{ ; Spécificité = 93\%} \quad (3.7)$$

$$\text{Performance} = \frac{Vp+Vn}{Vp+Vn+Fp+Fn} \text{ ; Performance = 94\%} \quad (3.8)$$

Ces statistiques nous montrent que notre modèle neuronal a été capable de classifier les vrais malades (sensitivité) et les personnes non malades (spécificité).

3.5. Performance de l'algorithme RSA modifié pour le cryptage lors de la transmission de données médicales par téléphonie mobile

Le tableau 16 nous indique que notre méthode proposée EMSRSA a un temps de génération de la clé privée plus élevé que celui de MRSA de Muhammad et celui de RSA original.

Tableau 16: Tableau comparé des performances des algorithmes RSA, MRSA et le notre (EMSRSA).

Taille des bits p, q, r, s	100	128	256	512	1024	2048	4096	Algorihtme
Temps clé privée (en ms)	0,487619	0,397367	0,536381	0,583859	1,022289	1,878189	6,547785	RSA
	1,150182	0,948718	2,089063	3,352168	3,724298	11,668641	43,781358	MRSA
	2,262297	1,846109	3,756807	7,11368	12,052748	21,220416	65,98343	EMSRSA
Temps de cryptage (en ms)	0,059883	0,0586	0,102229	0,151419	0,962406	2,863266	10,178836	RSA
	0,155696	0,169812	0,506868	1,804191	4,027991	16,20906	87,732529	MRSA
	0,71603	0,747683	10,668167	33,898088	199,573975	1285,051478	10237,78236	EMSRSA
Temps de décryptage (en ms)	4,845822	0,257925	0,873438	3,477494	24,465223	167,77436	1464,092836	RSA
	1,250701	1,941494	15,558901	53,716385	337,387986	2809,571451	20253,26726	MRSA
	1,193811	1,176702	14,275265	51,301388	377,112268	2699,154794	20158,48051	EMSRSA

Notre méthode [79] est donc plus sécurisée que RSA, car le hacker mettra plus de temps pour craquer notre algorithme, au niveau de la factorisation du grand nombre 'N'. Pour les entrées, par exemple, de nombres premiers pour le bit de taille 2048, le temps de generation de la clé donne 21 ms contre 11,6 ms pour MRSA de Muhammad et 1,8 ms pour RSA. Notre temps de décryptage est également plus court que ce lui de MRSA: 2699 ms contre 2809 ms. Les figures 37, 38 et 39 présentent une comparaison des performances des trois algorithmes (RSA, MRSA et EMSRSA).

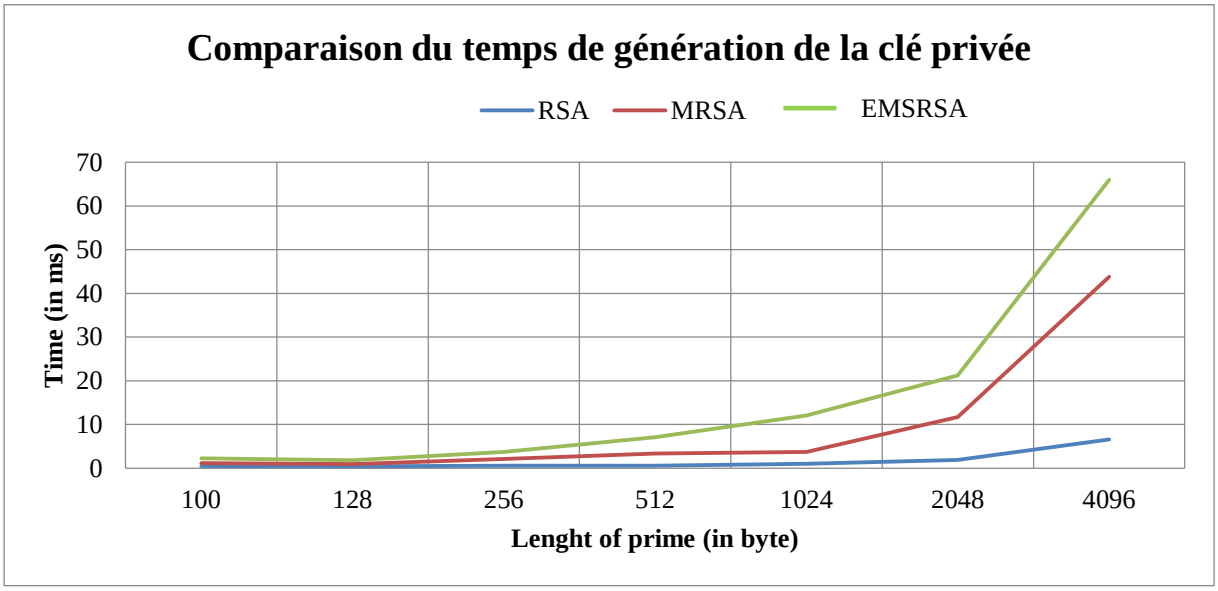


Figure 37: Comparaison du temps de génération de la clé privée.

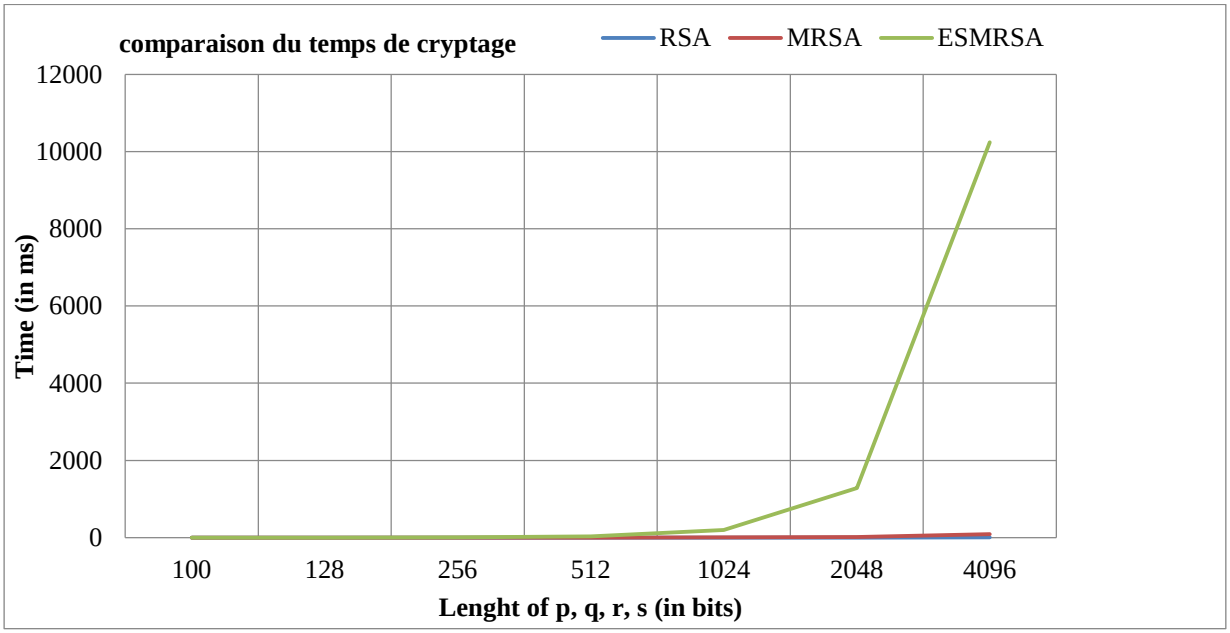


Figure 38: Comparaison du temps de cryptage.

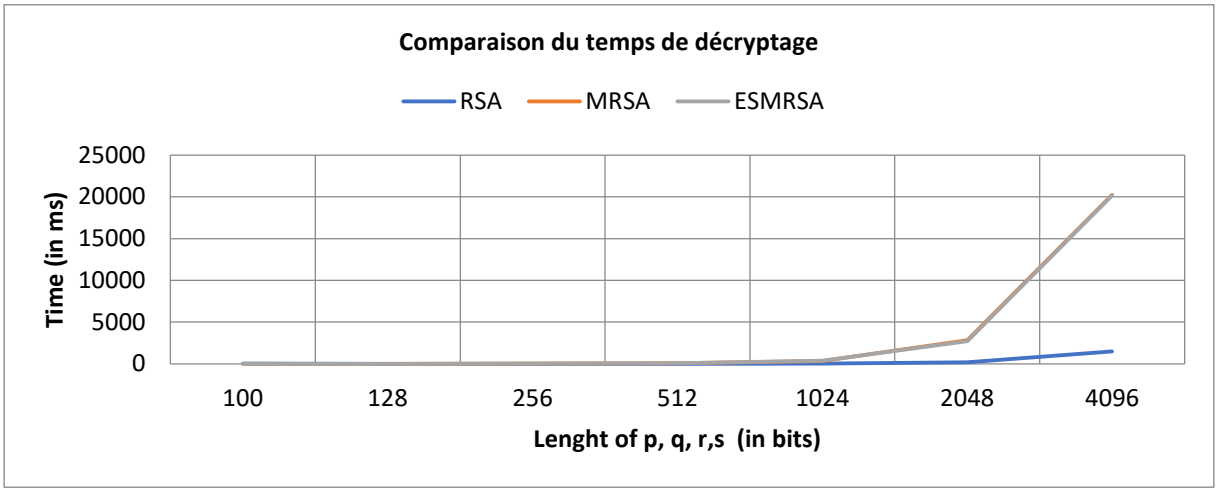


Figure 39: Comparaison du temps de décryptage

3.5.1. Analyse de complexité

3.5.1.1. Complexité de l'algorithme RSA

Comme Muhammad l'a montré pour RSA, la complexité des deux nombres sélectionnés au hasard est :

$O(\underline{s}*(\log 2p)^2 * \ln p)$ et $O(\underline{s}*(\log 2q)^2 * \ln q)$, selon la complexité de MILLER RABIN. La complexité pour trouver la variable ad random '*e*' étant $O((\log 2(\log 2p\text{-}1) * (\log 2q\text{-}1))^2+1)$.

Pareillement pour notre EMSRSA, comme pour le MRSA de Muhammad, la complexité pour trouver les nombres premiers *p*, *q*, *r*, *s* que nous allons noter pour la circonstance w, x, y, z est respectivement :

$O(\underline{s}*(\log 2w)^4 * \ln w)$, $O(\underline{s}*(\log 2x)^4 * \ln x)$, $O(\underline{s}*(\log 2y)^4 * \ln y)$ et $O(\underline{s}*(\log 2z)^4 * \ln z)$.

La complexité pour que le hacker trouve les nombres au hasard e, f, et h étant pareils :

$O((\log 2(\log 2w\text{-}1) * (\log 2x\text{-}1) * (\log 2y\text{-}1) * (\log 2z\text{-}1))^4+1)$.

C'est cette complexité qui conforte notre RSA renforcé avec 4 nombres premiers au lieu de 2 chez RSA original.

3.5.1.2. Analyse de sécurité

Pareillement à ce qu'a exposé Muhammad, la technique de factorisation peut être utilisée pour trouver 'w', 'x', 'y', 'z', les quatre nombres premiers *p*, *q*, *r*, *s* que nous avons renommé pour la circonstance, mais pas pour trouver 'e', 'f', 'g', car pour eux, il faut forcement utiliser l'attaque de force brute. En effet, L'attaque la plus simple sur un chiffre est

l'attaque par force brute. Dans cette attaque, un attaquant essaie simplement de décrypter le message avec chaque clé secrète possible et vérifie le résultat du décryptage pour voir si cela a un sens. Avec suffisamment de temps et de ressources informatiques, cette attaque est garantie de fonctionner puisque la vraie clé secrète doit se trouver dans l'ensemble des clés secrètes possibles et l'attaquant finira par l'essayer et (espérer) réaliser que le texte en clair résultant soit celui qui convient [80].

$\Omega_{system1} = \Omega_{w,x,y,z} + \Omega_{brute\ force1}$ avec notre méthode EMSRSA où (3.9)

$\Omega_{system2} = \Omega_{x,y} + \Omega_{brute\ force2}$ avec RSA original (3.10)

Ω_{system} = Temps nécessaire pour casser le système

$\Omega_{w,x,y,z}$ = Temps nécessaire pour trouver *w, x, y, z* en utilisant, par exemple, les méthodes des algorithmes modernes de factorisation GNFS (General Number Field Sieve) et ECM (Elliptic Curve Method).

$\Omega_{x,y}$ = Temps nécessaire pour trouver *x,y* en utilisant, par exemple, les méthodes des algorithmes modernes de factorisation GNFS (General Number Field Sieve) et ECM (Elliptic Curve Method).

$\Omega_{brute\ force1}$ = Temps nécessaire pour l'attaque par brute force qui permettrait de trouver les nombres premiers ad random *e*, *f* et *h*.

$\Omega_{brute\ force2}$ = Temps nécessaire pour l'attaque par brute force qui permettrait de trouver le nombre e premiers à $\emptyset(n)$.

Nous venons de montrer que $\Omega_{w,x,y,z}$ est supérieur à $\Omega_{x,y}$.(key generation time).

De même, $\Omega_{brute\ force1} > \Omega_{brute\ force2,}$ car il faut plus de temps à la force brute pour trouver trois nombres ad randoom premiers entre eux (e, f, et h) qu'il n'en faut dans la méthode de RSA original.

Prenons un exemple : si nous utilisons le site https://howsecureismypassword.net, un outil de vérification de cryptananlyse en ligne de mot de passe, Il faut au minimum 34.0000 années pour arriver à bout d'un mot de passe comme Binl_ose1***. Plus le mot de passe est long et complexe, plus il faut du temps pour le cracker. Nous savons également qu'il y'a au moins $(62)^x$ possibilités pour cracker par brute force une clé de longueur x. si on a la longeur x= 5 caractères, cela nous donne 38440000000000 possibilités à trouver en un temps $\Omega_{brute\ force}$, selon la performance du serveur d'attaque. Cela démontre bien que $\Omega_{brute\ force1} > \Omega_{brute}$

$_{force2}$, car au lieu de fonctionner en entrée avec les deux nombres premiers pris au hasard, il faut en trouver quatre.

Nous en déduisons que $\Omega_{system1} > \Omega_{system2.}$ Le hacker prendra forcément plus de temps pour cracker notre RSA amélioré que de le faire avec RSA original.

La sécurité de notre algorithme EMSRSA est donc plus renforcée que RSA, car déjà plus corsé que MRSA de Muhammad, par le fait qu'il faut au hacker trouver quatre nombres premiers au lieu de deux. Ensuite il lui faut un temps plus long pour générer la clé primaire liée à la factorisation du grand nombre premier '*N*'. Cependant, notre temps de décryptage est plus court que celui de MRSA à partir des bits de grande taille. L'intérêt de notre travail est que RSA est utilisé juste pour l'échange des clés privées, car la clé publique traverse le réseau mobile de transmission des données médicales. Pour la transmission de ces données, un algorithme symétrique comme AES, par exemple serait plus adapté. Dans ce contexte, la sécurité de clé privée est importante, et le temps de génération de la clé primaire plus ou moins long compte beaucoup, et c'est ce que nous avons réussi par notre méthode, en améliorant la sécurité de RSA.

Conclusion partielle

La sécurisation de la transmission de nos données médicales dépend du cryptage que nous appliquons. Nous avons choisi RSA, reconnu mondialement déjà comme un algorithme robuste de cryptage, que nous modifions et qui utilise la factorisation des grands nombres. Nos travaux, pareillement à ceux de MUHAMMAD Ariful a consisté en 'n' nombres premiers au lieu de deux. Le triple cryptage-décryptage que nous avons fait a rendu plus corsé la possibilité de casser le nombre factorisé 'N' dont dépend tout le cryptage. Le temps nécessaire pour le casser dans notre cas est beaucoup plus long que celui du MRSA de Muhammad, et de RSA. Le temps de cryptage est beaucoup plus long que RSA et MRSA, mais grâce à notre stockage hors ligne, nous avons pu améliorer le temps de décryptage comparativement à MRSA, surtout quand les bits d'entrée sont plus grands. Nous comptons donc, dans nos futurs travaux, améliorer le temps du cryptage en appliquant à ce niveau l'algorithme AES modifié, ce qui donnerait une combinaison asymétrique AES modifié et EMSRSA, pour accroître les performances de notre nouvel algorithme.

3.6. Analyses récapitulatives (avantages économiques, gain en efficacité et en temps)

3.6.1. Analyse des avantages économiques

Nous pouvons conclure, au terme de nos travaux, que notre plateforme vient compléter les excellents résultats obtenus par les techniques classiques de l'ICA. Cet apport pourrait être judicieux dans les zones reculées du pays, en cas d'absence de matériels lourds d'analyse de laboratoire. Cette innovation permettrait d'éviter à des malades cardiaques, par exemple, de se déplacer forcement vers les Centres Hospitaliers Universitaires (CHU) ou les Centre hospitaliers régionaux (CHR). Le diagnostic du spécialiste distant pourrait être guidé, dans une première approche par notre plateforme, et lui permettre de décider si oui ou non le patient devrait se déplacer vers lui pour des analyses plus poussées. Ceci aura pour avantage des économies financières pour les patients critiques.

3.6.2. Tableau de comparaison de temps d'exécution des différentes analyses avec notre méthode et celle de l'ICA

3.6.2.1. Examens non invasifs

Le tableau 17 nous donne une comparaison du temps nécessaire à notre méthode et à celle de l'ICA pour la réalisation des différents examens non invasifs.

Tableau 17: Comparaison du temps de collecte non invasive par notre méthode et celle de l'ICA

Constante	Notre Méthode avec les multi capteurs	Méthode de l'Institut de Cardiologie d'Abidjan	Observation
Tension artérielle	60s	60s	convergent
Température	5s	30s	Notre méthode plus rapide
Rythme cardiaque	30s	30s	convergent
SPo2	10s	30s	Notre méthode plus rapide
ECG	30s	2min	Notre méthode plus rapide

3.6.2.2. Examens invasifs

Le tableau 18 nous donne une comparaison du temps nécessaire à notre méthode et à celle de l'ICA pour la réalisation des différents examens non invasifs.

Tableau 18: Comparaison du temps de collecte invasive par notre méthode et celle de l'ICA

Constante	Notre Méthode avec les multi-capteurs	Méthode de l'Institut de Cardiologie d'Abidjan	Observation
Glycémie, Hémoglobine, Cholestérol total, Acide Urique, Urée	40s	45 min	Notre méthode plus rapide

Interprétation du tableau de temps d'exécution :

En plus d'être économique en termes de coût d'achat (Confère le tableau annexe 19), notre méthode permet au patient d'obtenir plus rapidement ces constantes qui se rapprochent de celles obtenues par les examens en laboratoire.

Conclusion partielle

Ce dernier chapitre a exposé les résultats obtenus, notamment, les résultats du test de *Student* sur la comparaison des constantes collectées par notre méthode et celle de l'Institut de Cardiologie d'Abidjan (ICA), les résultats de la prédiction de pathologies, les résultats des électrocardiogrammes (ECG) acquis par les deux méthodes comparées, la classification des stades de l'hypertension artérielle par les réseaux de neurones artificiels, l'algorithme RSA modifié et amélioré. Une analyse récapitulative des avantages économiques, des gains en efficacité et temps, a été présentée à la fin de ce troisième chapitre.

CONCLUSION GENERALE ET PERSPECTIVES

Parmi les problèmes des populations, surtout en Afrique subsaharienne, on peut citer celui de la santé, face à l'insuffisance des structures sanitaires, et même le manque d'équipements adéquats pour des analyses biologiques des constantes de patients, quand bien-même ces centres de santé existent. La croissance démographique inclut une forte demande de soins de santé, mais malheureusement, nous assistons à des diagnostiques tardifs, et, très souvent, l'ignorance du statut sanitaire des populations. Le problème est beaucoup plus critique pour les zones les plus reculées des pays, où il y'a très peu de spécialistes (par exemple, des cardiologues), capables de diagnostiquer rapidement des pathologies graves, en vue d'éviter leur aggravation. Ce qui a pour conséquence une forte mortalité et une réduction de l'espérance de vie.

Face à cette situation, de nouvelles techniques sont à développer et à vulgariser. Parmi elles, les techniques de la télémédecine, encore appelée e-santé ou e-health en anglais, se présentent comme une solution d'avenir, pour développer un système sanitaire efficace, qui touche une grande population, quels que soient les lieux et les distances.

Ceci est possible avec les nouvelles technologies de l'information et de la communication, dont la téléphonie mobile constitue un pilier.

Les travaux effectués au cours de notre thèse de doctorat étaient centrés sur la mise au point d'une nouvelle technique d'acquisition de constantes de santé de patients. La nouvelle méthode devait pouvoir faire une interprétation de ces constantes collectées, puis les transmettre à un spécialiste distant, capable, à son tour, d'indiquer, en retour, par le même canal de téléphonie mobile, des recommandations à l'agent de santé qui a ausculté le patient.

En clair, nous avons montré qu'il était possible, de collecter directement des constantes de santé sur des patients, et ceci à faible coût. Ces données sont interprétées, par exemple, par une classification des stades de pathologies qu'elles impliquent, puis sont transmises, de façon sécurisée, à un spécialiste. Pour atteindre cet objectif, nous avons effectué les travaux suivants :

- La mise en place d'un nouveau dispositif d'acquisition, à faible coût, des constantes des personnes ;

- L'établissement des techniques de traitement et d'analyse des mesures collectées sur des personnes, notamment par la classification ;

- L'élaboration d'un nouvel algorithme de sécurisation de la transmission de ces données médicales par téléphonie mobile.

Nous avons donc proposé une nouvelle technique d'acquisition de 7 constantes non invasives qui sont : la pression artérielle systolique (PAS), la pression artérielle diastolique (PAD), la tension artérielle (TA), le rythme cardiaque ou pouls (RC), la saturation « pulsée » en oxygène (SpO2), la température du patient (T°) et l'ECG; 5 constantes invasives ont également été collectées : la glycémie ou Taux de sucre dans le sang (Gl), l'acide urique dans le sang (AC. Ur), l'hémoglobine (Hb), l'albumine ou les protéines dans l'urine et le PH. Le poids (Pd), la taille (T), le sexe (S), l'âge (Ag), la couleur des yeux et le groupe sanguin y ont aussi été renseignés manuellement. Cela nous a permis de déduire l'Indice de Masse corporelle (IMC) et le taux d'hématocrite (Ht) ; ce qui a complété à 14 le nombre de constantes collectées. Nous avons, par ailleurs, créé une librairie de symptômes en fonction des pathologies courantes. Nous avons donc collectés sur le client ses symptômes observés et les avons renseignés manuellement dans notre application.

A ce stade, nos algorithmes de premier niveau ont procédé d'abord aux tests des pathologies directement liées à ces valeurs physiques, en vue de déduire leur caractère normal, anormal ou critique. Ensuite, notre algorithme s'inspirant de la loi de Bayes nous a permis d'affiner la prédiction de pathologies. Cette prédiction a été consolidée par un apprentissage par réseaux de neurones artificiels de rétro-propagation. La transmission est sécurisée par un algorithme amélioré de RSA.

Les tests de pathologies et le diagnostic prédictif sont ainsi transmis à notre Mobile Cloud Computing, via la puce du réseau téléphonique embarquée dans nos terminaux mobiles, qui les transmet à son tour au médecin traitant, aux spécialistes ou tout simplement aux proches du patient.

Notre thèse, intitulée : « Contribution à une technique d'acquisition et de traitement de constantes de santé, transmises par voie sécurisée avec l'algorithme RSA amélioré (EMRSA), à un médecin distant, par téléphonie mobile **»,** se présente dans ce manuscrit, de la façon suivante :

Le chapitre 1 a présenté le contexte de notre recherche et une revue bibliographique sur les techniques d'acquisition de constantes de patients, et leur transmission par des technologies telles que la téléphonie mobile. Il a aussi présenté des généralités sur les modes

de fonctionnement des capteurs. Les principes des différentes constantes acquises dans notre recherche ont également été précisés.

Le chapitre suivant a mis en lumière les matériels que nous avons utilisés pour résoudre nos hypothèses, notamment notre échantillon biologique, le nouveau dispositif de collecte des constantes sur les patients. Il a également montré les méthodologies utilisées, à savoir :

- La nouvelle application mobile que nous avons développée, pour permettre la collecte des constantes sur un smartphone ou une tablette ;
- Le test statistique de *Student*, pour confirmer la fiabilité des constantes collectées par notre méthode ;
- Le nouvel algorithme d'évaluation de ces constantes collectées sur les appareils mobiles ;
- L'algorithme de prédiction de pathologies à partir de ces constantes et des symptômes connus de cette pathologie ;
- Le modèle neuronal de classification de pathologie telle que l'hypertension artérielle ;
- Le nouvel algorithme basé sur l'amélioration de celui de RSA, pour la sécurisation des données transmises par téléphonie mobile.

Le troisième chapitre a exposé les résultats obtenus, notamment, les résultats du test de *Student* sur la comparaison des constantes collectées par notre méthode et celle de l'Institut de Cardiologie d'Abidjan (ICA), les résultats de la prédiction de pathologies, les résultats des électrocardiogrammes (ECG) acquis par les deux méthodes comparées, la classification des stades de l'hypertension artérielle par les réseaux de neurones artificiels, l'algorithme RSA modifié et amélioré. Une analyse récapitulative des avantages économiques, des gains en efficacité et temps, a été présentée à la fin de ce troisième chapitre.

Les résultats de notre modèle ont donné une parfaite classification des types d'hypertension, avec une régression R^2 de 0.99, un RMSE de 0.03553, une sensitivité de 0.91, une spécificité de 0.93 et une performance de 0.94.

Une performance de Notre algorithme de prédiction des trois premières pathologies risquées par le patient collecté a donné un taux de 97,5 % de conformité de notre diagnostic avec celui de la fiche patient des malades de l'ICA. Ce qui nous a permis d'affirmer que notre solution pourrait être une bonne méthode suggestive et alternative de diagnostic. Ces données

nous ont permis de faire une simulation d'analyse Big Data dont les résultats se sont avérées conformes aux statistiques de causes d'entrée en cardiologie des patients, notamment avec 60% de prévalence de la dyspnée au sein des patients accueillis.

Cette transmission est sécurisée par l'algorithme de cryptage amélioré EMSRSA que nous avons développée, en nous basant sur l'algorithme RSA amélioré. Notre analyse économique comparative a permis de montrer que notre méthode permettrait aux patients d'économiser de l'argent et gagner du temps dans la réception de leurs constantes. Notre plateforme pourrait être déployée au plan national, avec quelques améliorations de constantes, et permettrait de juguler le paramètre distance et manque de laboratoires d'analyses dans nos centres de santé reculés.

En ce qui concerne les perspectives relatives à cette étude, il est possible de la compléter :

- En augmentant le nombre de constantes de santé collectées
- En étudiant une nouvelle technique de télémédecine pour l'ophtalmologie.

REFERENCES BIBLIOGRAPHIQUES

[1] C. Axelle, ''Multi-sensor platform for monitoring geographic positioning and behavioral signals'', Canada, Montréal, Digital document, (2013), 114p.

[2] B. Gavilanes, J. Gabriel, ''Sensor networks for medical monitoring applications'', PhD Thesis, (2013), 111p.

[3] M. Cerny, M. Penhaker, ''Telemetric measurement of selected biological signals, by bluetooth technology'', (2011), p.229.

[4] A. VEYSEL, R. Kurban, T. Caglikantar, ''Wireless medical surveillance system with lower cost, and transmission to an alarm station'', (2007), 5p.

[5] P. Crilly, V. MUTHUKKUMARASAMY, ''Using Smart Phones and Body Sensors to Deliver Pervasive Mobile Personal Healthcare''.
https://doi.org/10.1109/ISSNIP.2010.5706767, (2010), 4p.

[6] M. C. Silva Bruno, J. Rodrigues, J.P.C, ''Mobile-health: a review of Current state in 2015', in Elsevier, 'Journal of biomedical informatic',56, (2015), pp.265-272.

[7] X. Boyi, X. Lida, C. Hongming, J. Lihong, L.Yang and G.Yizhi, ''The design of an m-Health monitoring system based on a cloud computing platform'', Enterprise Information Systems, (2015), 20p.

[8] H. N., Alshareef, Mobile cloud healthcare systems using the concept of point–of–care, PhD Thesis, University College Cork, (2017), 235p.

[9] F. Diby, A. Adoubi, C. Diby, A. Gnaba; E. N'guessan; S. Zadi, I. Nanan, R. Kpon, M. Doumbia, G. Ayegnon, G. Meneas, D. Manga, F. Sall, A. Coulibaly, E. Ehui, M. Yao, B. Traore, S. Ehua, K.H. Yangni-Angaté, ''Le télé-ECG au service du dépistage des maladies cardiaques en Côte d'Ivoire'', Atelier bilan du projet télé-ECG et 2è séminaire technique sur la télémédecine et l'hôpital numérique à Bouaké, (2018), 85p.

[10] W. Lidong, A. A. Cheryl, ''Telemedicine Based on Mobile Devices and Mobile Cloud Computing'', International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.3, 1, (2014), pp.26-36.

[11] L. Po-Chou, ''Cost-effective Design of Real-time Home Healthcare Tele monitoring based on Mobile Cloud Computing'', PhD Thesis, Department of Computer Science Faculty of Engineering and Physical Sciences University of Surrey, (2016), 242p.

[12] Cardiopad, http://www.journalducameroun.com/article.php?aid =12264, consulté le 04/02/2015, 14h.

[13] Chaîne d'acquisition, https://eduscol.education.fr/sti/sites/eduscol.education.fr.sti, consulté le 25/09/2019 à 16h.

[14] Sur les Capteurs, https://www.les-electroniciens.com/sites/default/files/cours/ capteurs.pdf, consulté le 16/09/2019, à 12h.

[15] H. H. Molinaro, E. Vourc'h, J. P. Barbot, Capteurs et chaîne d'acquisition, ENS CACHAN, http://eduscol.education.fr/sti/si-ens-cachan, (2015), 8p.

[16] https://fr.wikipedia.org/wiki/Théorème_d'échantillonnage théorème de shannon-nyquist, consulté le 15/11/2019 à 16h.

[17] Principes d'électrocardiographie, https://www.louvainmedical.be/fr/article/rappels-des-principes-fondamentaux-en-electrocardiographie, consulté le 06/07/2019, à 23h.

[18] M. L. Talbi, Analyse et traitement du signal électrocardiographique (ECG), Thèse de doctorat, Université Mentouri de Constantine Faculté des Sciences de l'Ingénieur

Département d'Electronique, (2011), 122p.

[19] E. Clark, M. Sejersten, P. Clemmensen, Automated electrocardiogram interpretation programs versus cardiologists' triage decision making based on tele transmitted data in patients with suspected acute coronary syndrome, Am J Cardiol. (2010).

[20] Gargiulo, G., Bifulco, P., Cesarelli, M., Mcewan, A., Moeinzadeh, H., O'Loughlin, A., Thiagalingam, A. (2016). On the "Zero of Potential of the Electric Field Produced by the Heart Beat". A Machine Capable of Estimating this Underlying Persistent Error in Electrocardiography. Machines, 4(4), 18. Doi:10.3390/machines4040018

[21] P. Macfarlane, B. Devine, E. Clark. ECG analysis program. Computers in Cardiology. The University of Glasgow (Uni-G), (2005); 32: pp.451-454.

[22] Oxymétrie, https://urgences-serveur.fr/oxymetre-de-pouls-principes,2178.htm, consulté le 27/9/2019, 22h.

[23] Dr S. Zisimopoulou, Hypertension artérielle - Service de médecine de premier recours, DMCPRU – HUG, (2017), 16p.

[24] Hémoglobine, https://www.who.int/vmnis/indicators/haemoglobin_fr.pdf, consulté le 23 septembre 2019, à 14h00.

[25] WHO, Hypertension. https://www.who.int/health-topics/hypertension. Consulté le 19 août 2019.

[26] WHO, Cardiovascular diseases. https://afro.who.int/fr/node/521. Consulté le 17 août 2019.

[27] Australia Heart Foundation. Guidelines for the diagnosis and management of hypertension in adults, (2016), pp.50-51.

[28] P. Martha, M. Patricia, P. German. Blood pressure classification using the method of the modular neural networks. International Journal of Hypertension Volume, Article ID 7320365, (2019) 1-13. https://doi.org/10.1155/2019/732036.

[29] H.W. Tony, W.K. Enid, K.P. Grantham. Biomedical application on predicting systolic blood pressure using neural Networks, IEEE, First International Conference on Big Data Computing Service and Applications, (2015) pp.456-461.

DOI: 10.1109/BigDataService.2015.54

[30] D. M. Hlaudi, A. M. Mosima. Prediction of heart disease using classification algorithms, Proceedings of the World Congress on Engineering and Computer Science Vol II WCECS, (2014), 4p.

[31] S. Radhimeenakshi, G.M. Nasira. Prediction of heart disease using neural network with back propagation, Integrated Intelligent Research (IIR), International Journal of Data Mining Techniques and Applications, 04 (2015), pp.19-22.

[32] P. A. Idowu, Predictive model for the classification of hypertension risk using decision trees algorithm, American Journal of Mathematical and Computer Modelling, 2, (2017) 48-59. https://doi.org/10.11648/j.ajmcm.20170202.12.

[33] N. Satyanarayana , Y. Ramadevi, R. Sahith, C. Ramalingaswamy, High blood pressure prediction based on AAA++ using machine-learning algorithms, Cogent Engineering, 5 (1), (2018), pp.1-12.

[34] C.G. Juan, Patricia M., P. German, Design of an optimized fuzzy classifier for the diagnosis of blood pressure with a new computational method for expert rule optimization, Algorithms, 10, 79; (2017) pp.1-27.

[35] Saloni, R.K. Sharma, A. K. Gupta, Classification of high blood pressure persons vs

normal blood pressure persons using voice analysis. 1 (2014), pp.47-52. doi:10.3390/a10030079.

[36] J. N. Teemu, S.H. Aki, L.L. Ville, S. Veikko, M.J. Antti, Prediction of blood pressure and blood pressure change with a genetic risk score, The Journal of Clinical Hypertension, (2016) pp.181-186.

[37] M. Patricia, M. Ivette, P. German, A hybrid model based on modular neural network and fuzzy systems for classification and blood pressure and hypertension risk diagnosis, Experts Systems With Applications, (2018) pp.146-164. https://doi.org/10.1016/j.eswa.2018.04.023.

[38] B. Gilles, Réseaux de Neurones en Traitement d'Images - Des Modèles théoriques aux Applications Industrielles -. Traitement du signal et de l'image. Université de Bretagne occidentale - Brest. (1991).

[39] D. Rummelhart., G. E. Hinton and R. J. Williams, Learning internal representations by error retro propagation, parallel distributed processing/exploration in micro-structure of cognition, MIT Press, (1986), 506p.

[40] G. Kaliraj, S. Baskar, An efficient approach for the removal of impulse noise from the corrupted image using neural network based impulse detector, Image and Vision Computing, 28(3): (2010), pp.458-466, doi: 10.1016/j.imavis.2009.07.007.

[41] R. K. Agrawal, N. G. Bawane, Optimized neural network for classification of multispectral images, ACEEE International Journal on Signal and Image Processing, 5(1):(2014), pp.65-70.

[42] Coulibaly, P., Anctil, F., Bobée, B., Prévision hydrologique par réseau de neurones artificiels: état de l'art, Canadian Journal civil engineering. 26(3) : (1999), pp. 293–304.

[43] K. A.Kouakou, Analyse Microscopique de l'Etat Physiologique des Plantes Tropicales par Imagerie Multi Spectrale et Multi modale, thèse de doctorat,(2018), 157p.

[44] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Vol.21, (1978), pp. 120-126.

[45] D. Sathya, P. G. Kumar, Secured remote health monitoring system, Healthcare Technology Letters, Vol. 4, Iss. 6, (2017), pp.228–232, doi:10.1049/htl.2017.0033.

[46] J. Heurix and T. Neubauer, Privacy-preserving storage and access of medical data through pseudonymization and encryption, Institute of Software Technology and Interactive Systems, Austria, (2011), 12p.

[47] M. Layouni, K. Verslype, M. T. Sandıkkaya, B. De Decker, and H.Vangheluwe, Privacy-preserving tele monitoring for eHealth, IFIP International Federation for Information Processing 2009, Data and applications security, LNCS 5645, (2009), pp. 95–110.

[48] M. Milutinovic, B. De Decker, Privacy-preserving data management in eHealth systems, Conference on enterprise information systems /HCIST – International Conference on Health and Social Care Information Systems and Technologies, (2013), 8p.

[49] Sun, H. M., M. E. Ting, W.C. and Hinek, M.J., Dual RSA and its security analysis. IEEE Transactions on information Theory,53,(2007), pp.2922-2933.

[50] S. K. Abd and S.A.R Al-Haddad, F. Hashim and A. Abdullah, A review of cloud security based on cryptographic mechanisms, International Symposium on Biometrics and Security Technologies (ISBAST), (2014), pp.106-111.

[51] M. R. Patidar, Mrs. R. Bhartiya, Implementation of modified RSA cryptosystem based on offline storage and prime number, International Journal of Computing and Technology, Volume 1, Issue 2, (IJCAT), ISSN: 2348-6090, (2014), pp. 205-209.

[52] M. A. Islam, Md. A. Islam, N. Islam, B. Shabnam, "A modified and secured RSA public key cryptosystem based on 'n' prime numbers", Journal of Computer and Communication, 6, (2018), pp.78-90.

[53] A. Hamza, M. Al-Salami, Timing attack prospect for RSA cryptanalysts using genetic algorithm technique, Computer science department, Zarka Private University, Jordan, The International Arab Journal of Information Technology, Vol. 1, No. 1, (2004), 5p.

[54] B. Kumar, J. Boaddh and L. Mahawar, A hybrid security approach based on AES and RSA for cloud data, International Journal of Advanced Technology and Engineering Exploration, Vol 3(17), (2016), 7p.

[55] A. Bhardwaja, G. Subrahmanyamb, V. Avasthic, H. Sastryd, Security algorithms for Cloud computing, Procedia Computer Science, 85, (2016), pp.535-542.

[56] B. Swamia, R. Singh, S. Choudharyc, Dual modulus RSA based on Jordan-Totient function, International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST), (2015), 6p.

[57] Dr. P. Mahajan & A. Sachdeva, A study of encryption algorithms AES, DES and RSA for Security, Global Journals Inc.(US), Vol. 13, (2013), 9p.

[58] D. Preuveneersa, Y. Berbersa, W. Joosena , The future of mobile e-health application development: exploring HTML5 for context-aware diabetes monitoring, Procedia Computer Science, 21, (2013), pp.351-359.

[59] M. Kethari, Prof. L. Desai, A survey on secure web based medical data transmission for eHealth", International Journal of New Innovations in Engineering and Technology, Volume 6 Issue 3, ISSN : 2319-6319, (2016), 3p.

[60] V. Kapoor and R. Yadav, A hybrid cryptography technique for improving network security, International Journal of Computer Applications (0975 – 8887) Volume 141 – No.11, (2016), 6p.

[61] K.G. Kadam and Prof. V. Khairnar, Hybrid RSA-AES Encryption For Web Services, International Journal of Technical Research and Applications e-ISSN:2320-8163, 31, (2015), pp.51-56.

[62] K. Rege, N. Goenka, P. Bhutada, S. Mane, Bluetooth communication using hybrid encryption algorithm based on AES and RSA, International Journal of Computer Applications (0975-8887) Volume 71-No.22, (2013), 4p.

[63] R. Raj, Y. S. Solunke, A modified RSA cryptosystems and analysis, Published By : Blue Eyes Intelligence Engineering & Sciences Publication Pvt. Ltd, (2015), 3p.

[64] S. Patel, P. P. Nayak, A novel method of encryption using modified RSA algorithm and Chinese remainder theorem, Department of Electronics and Communication Engineering National Institute of Technology, (2009), 44p.

[65] A. Gupta and V. Sharma, Modified double Mod RSA tested with brute force attack, International Journal of Innovative Research & Development, (2014), 4p.

[66] B. Yüksel, A. Küpçü, Ö. Özkasap, Research issues for privacy and security of Electronic health services, Future Generation Computer Systems,68,(2017), pp.1-13,

[67] S. Bhuyan, H. Kim, O. Oluwaseyi. Isehunwa, N. Kumar, J. Bhatt, D. K. Wyant, S. Kedia, C.F. Chang, D. Dasgupta, Privacy and security issues in mobile health: current research and future directions, The University of Memphis School of Public Health

135 Robison Hall, (2017),11p. https://doi.org/10.1016/j.hlpt.2017.01.004

[68] S. Harsha, G. Pussewalage, V.A. Oleshchuk, Privacy preserving mechanisms for enforcing security and privacy requirements in e-health solutions, International journal of Information Management,36, (2016), pp.1161-1173.

[69] L. Yunfei, Q. Liu, L. Tong, Design and implementation of an improved RSA algorithm, International Conference on e-Health Networking, Digital Ecosystems and Technologies, (2010), 4p.

[70] S. Sharma, S. Hiranwal, P. Sharma, A new variant of subset-sum cryptosystem over RSA, International Journal of Advances in Engineering & Technology, (2012), 8p.

[71] A.A. Ayele, Dr. V. Sreenivasarao, A modified RSA encryption technique based on multiple public keys, International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 4, (2013), 6p.

[72] H. Huang, T. Gong, Y. Ning, R. Wang and Y. Dou, Private and secured medical data transmission and analysis for wireless sensing healthcare system, 1551-3203, (c) IEEE, (2016),10p.

[73] B. Persis, Urbana Ivy, P. Mandiwa & M. Kumar, A modified RSA cryptosystem based On 'n' prime numbers, International Journal Of Engineering And Computer Science,1,2, (2012), pp.63-66.

[74] https://www.alibaba.com/product-detail/Multifunctional-smart-digital-health-monitor-ECG_60731772616.html, consulté le 27/9/2019, à 15h30.

[75] G. Saporta, Probabilités, Analyse des Données et Statistique, Editions Technip, Paris, (2011), 622p.

[76] P. Naïm, P.H Wuillemin, P. Leray, O. Pourret, A. Becker, Réseaux bayésiens, Eyrolles, (2004), 442p.

[77] B. Gilles, Réseaux de Neurones en Traitement d'Images - Des Modèles théoriques aux Applications Industrielles -. Traitement du signal et de l'image. Université de Bretagne occidentale - Brest. (1991).

[78] Sensitivity and specificity, https://en.wikipedia.org/wiki/Sensitivity_and_specificity, Consulté le 12/07/2019, à 16h35.

[79] A. H. Thiziers, H. C. Théodore, J. T. Zoueu and B. Michel, "Enhanced, Modified and Secured RSA Cryptosystem based on n Prime Numbers and Offline Storage for Medical Data Transmission via Mobile Phone" . International Journal of Advanced Computer Science and Applications (IJACSA), 10(10), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0101050

[80] https://www.commonlounge.com/discussion/4c8ace459d1840408e487a673cca255d, Consulté le 16 juillet 2019, à 11h36.

ANNEXES

Annexe 1: Comparaison de la température avec les deux méthodes de collecte de constantes

Notre Méthode	Méthode de l'Institut de Cardiologie	Différence
Température(T° C)	Température(T° C)	
36,9	36,8	0,1
36,7	36,6	0,1
35,5	35,6	0,1
35,4	35,5	0,1
36,7	36,6	0,1
37,1	37	0,1
36,9	36,8	0,1
35,2	35,1	0,1
37	37,4	0,4
38,3	38,1	0,2
35,3	35,2	0,1
34,5	34,2	0,3
36,4	36,3	0,1
34,6	34,4	0,2
37	36,8	0,2
36,4	36,8	0,4
35,6	36	0,4
37,2	37	0,2
36	36,5	0,5
31	33	2
36	35,4	0,6
36,5	36,8	0,3
35,4	35	0,4
35,7	35,4	0,3
37	37	0
36,6	36,2	0,4
36,5	36,7	0,2
35,4	36	0,6
35,2	36,1	0,9
35,9	36	0,1
35,7	36,2	0,5
36	36,2	0,2
36,8	36,4	0,4
37	37,3	0,3
37,4	37,2	0,2
38	37,6	0,4
37	37,2	0,2
36,4	36,1	0,3

35,1	34,9	0,2
36,4	36,1	0,3

Annexe 2 : Comparaison de la tension artérielle systolique avec les deux méthodes de collecte de constantes

Notre Méthode (1ère Prise)	Méthode de l'Institut de Cardiologie d'Abidjan	Différence		Notre Méthode (2ème Prise)	Méthode de l'Institut de Cardiologie d'Abidjan	Différence
Pression systolique(SYS)	Pression systolique(SYS) en mmHg			Pression systolique(SYS)	Pression systolique(SYS) en mmHg	
126	126	0		126	126	0
127	127	0		127	127	0
138	138	0		137	138	1
128	128	0		128	128	0
128	128	0		127	128	1
92	92	0		92	92	0
128	128	0		128	128	0
154	154	0		153	154	1
106	106	0		106	106	0
108	108	0		107	108	1
240	240	0		241	240	1
205	205	0		205	205	0
118	118	0		117	118	1
111	111	0		111	111	0
108	108	0		106	108	2
21	21	0		21	21	0
102	102	0		102	102	0
111	111	0		111	111	0
99	99	0		99	99	0
118	118	0		118	118	0
122	122	0		122	122	0
204	204	0		204	204	0
208	208	0		208	208	0
220	220	0		220	220	0
148	148	0		148	148	0
104	104	0		104	104	0
128	128	0		128	128	0
126	126	0		126	126	0
215	215	0		215	215	0
130	130	0		130	130	0
187	187	0		187	187	0
140	140	0		140	140	0
231	231	0		231	231	0
177	177	0		177	177	0
180	180	0		180	180	0
150	150	0		150	150	0

189	189	0		189	189	0
112	112	0		110	112	2
139	139	0		139	139	0
119	119	0		118	119	1

Annexe 3 : Base de données de tension artérielle sur les 40 patients de l'ICA, comprenant la tension systolique et diastolique sur deux prises consécutives séparées de de 1 à 2h, avec notre multi capteur « 6 in 1 Health Monitor ».

SYS 1ère prise	SYS 2ème prise	DIA 1ère prise	DIA 2ème jour	Décision
106	106	98	97	1
205	205	119	119	1
118	117	132	133	1
111	111	103	103	1
108	106	98	96	1
99	99	90	92	1
122	122	94	92	1
220	220	108	106	1
148	148	140	139	1
130	130	126	125	1
140	140	103	101	1
231	231	100	98	1
177	177	144	142	1
180	180	98	98	1
150	150	108	106	1
189	189	100	99	1
126	126	90	91	0
127	127	76	77	0
138	137	87	86	0
128	128	54	53	0
128	127	85	85	0
92	92	54	53	0
128	128	73	71	0
154	153	72	72	0
108	107	70	71	0
240	241	61	61	0

21	21	69	69	0
102	102	11	10	0
111	111	87	85	0
118	118	76	77	0
204	204	74	71	0
208	208	17	16	0
104	104	84	84	0
128	128	83	82	0
126	126	87	87	0
215	215	84	82	0
187	187	89	88	0
112	110	68	66	0
139	139	82	80	0
119	118	89	89	0

Annexe 4 : Autorisation d'enquête par la Direction Médiale Scientifique de l'ICA.

REPUBLIQUE DE COTE D'IVOIRE
UNION-DISCIPLINE-TRAVAIL

ICA

INSTITUT DE CARDIOLOGIE D'ABIDJAN

afaq ISO 9001 Qualité AFNOR CERTIFICATION

DIRECTION MEDICALE ET SCIENTIFIQUE

LE DIRECTEUR

Abidjan, le 19 DEC 2018

AKJB/GK
N° **036-2018** / MSHP/ICA/DG/DMS

AUTORISATION D'ENQUETE

Le Directeur Médical et Scientifique de l'Institut de Cardiologie d'Abidjan, autorise **M. ACHI HARRISSON THIZIERS,** étudiant à l'Ecole Doctorale Polytechnique de l'INPHB de Yamoussoukro, à effectuer une enquête à l'Institut de Cardiologie d'Abidjan dans le cadre de la réalisation de sa thèse de Doctorat en Physique, spécialité Electronique et Electricité Appliquées qui a pour thème :

« Acquisition et transmission de données médicales par téléphone mobile ».

En foi de quoi, la présente autorisation lui est délivrée pour servir et valoir ce que de droit.

NB : Ce travail sera effectué sous la supervision du Pr ANZOUAN-KACOU Jean-Baptiste, Chef du service des Explorations, Directeur Médical et Scientifique de l'ICA.

INSTITUT DE CARDIOLOGIE ABIDJAN Le Directeur

Pr ANZOUAN-KACOU J-B

Ampliations :

- Chef de service de Consultation
- S/DRH
- SUS Consultation
- Intéressé
- Archivistes

BP V 206 ABIDJAN - TEL : (225) 21-21-61-71 - FAX : (225) 21-25-92-10 - E-mail : infos@ica.ci

Annexe 5 : Fiche d'identification du patient anonyme

INSTITUT DE CARDIOLOGIE D'ABIDJAN (ICA)

SERVICE DE BIOLOGIE

FICHE DE CONSENTEMENT DU PATIENT

Patient N° :……
Nom :……
Prénoms :……
Sexe :……
Niveau d'études :……
Profession :……
Statut Marital :……
Antécédents cardio-vasculaires : ……

Cher (chère) M/Mlle/Mme……Nous allons procéder à la prise de vos constantes de santé par des petits capteurs, en vue de les comparer aux valeurs ordinaires des examens de bilan au niveau du service biologie. Les constantes sanguines qui seront prises sont : Acide urique, glycémie, cholestérol LDL, Hémoglobine, Hématocrite, CCMH et une constante urinaire, l'Albumine, Les autres constantes non sanguines sont : la température, le poids, le sexe, la taille, l'indice de masse corporelle, la tension systolique, la tension diastolique, la tension artérielle, le rythme cardiaque, la saturation en oxygène dans le sang, la couleur des yeux.

Je soussigné (M/Mlle/Mme)……donne mon libre

Consentement pour la prise de constantes sanguines et non sanguines par le dispositif des multi capteurs.

Fait à Abidjan, le ……

Signature du Patient

Annexe 6 : Fiche de collecte des constantes invasives du patient anonyme

INSTITUT DE CARDIOLOGIE D'ABIDJAN

INSTITUT DE CARDIOLOGIE D'ABIDJAN (ICA)

SERVICE BIOLOGIE

FICHE DE PRISE DE CONSTANTES INVASIVES

Patient N° :

Val.	Ac.Ur (mmol/l) dans le sang	Gl (g/l) dans le sang	Albumine, Protéine dans l'urine, (mol/l)	Hb (g/100ml) dans le sang	PH (1 à 9)	Ht %	CCMH
N.M							
Md							
écart							
Conc.							
Indic.							

……Date……

Annexe 7: Fiche de constantes non invasives du patient anonyme

INSTITUT DE CARDIOLOGIE D'ABIDJAN (ICA)

SERVICE BIOLOGIE

FICHE DE PRISE DE CONSTANTES NON INVASIVES

Patient N° :……Date……..

Val.	T (°C)	Poids (kg)	Sexe M/F	Taille (m)	Age (An)	SYS (mm Hg)	DIA (mm Hg)	RC Bpm	TA (S/D)	SpO2 (%)	IMC (%)	Ye B/J
N.M												
Md												
écart												
Conc.												
Indic.												

Annexe 8 : Fiche de collecte des symptômes du patient.

INSTITUT DE CARDIOLOGIE D'ABIDJAN

FICHE DE COLLECTE DES SYMPTÔMES DU PATIENT

Patient

N°……..…..Date……..

1-Symptôme du diabète (lié taux de glucose dans le sang Gl) **9**

- Un besoin de boire et de manger accru;
- Un besoin fréquent d'uriner;
- Une diminution de la sensibilité ou un engourdissement des mains et des pieds;
- Un état de faiblesse générale;
- De fréquentes infections de la vessie et du vagin;
- L'impuissance (une dysérection);
- Un ralentissement de la cicatrisation, des coupures ou des lésions;
- Une sécheresse de la peau accompagnée d'une démangeaison;
- Une vue trouble.

2-Symptôme de l'hypertension artérielle (lié à la tension PAS/PAD) **9**

- Des maux de tête le matin sur le sommet ou derrière la tête ;
- Des étourdissements ;
- Des troubles visuels : mouches volantes, brouillard devant les yeux...
- Une fatigue ;
- Des saignements de nez ;
- Des hémorragies conjonctivales ;
- Des crampes musculaires ;
- Une pollakiurie (envie fréquente d'uriner) ;
- Une dyspnée (gêne respiratoire traduisant une insuffisance ventriculaire gauche).

3-Symptômes de l'anémie (taux d'hémoglobine inférieur à 14 g/l chez l'homme, 12 g/l chez la femme) **11**

- Pâleur, bien visible à l'intérieur des paupières, au niveau des ongles et des lèvres ;
- Dyspnée à l'effort puis au repos ;
- Fatigue persistante ;
- Palpitations ;
- Étourdissements, vertiges, faiblesse en se levant d'une chaise, sensation de tête qui tourne ;
- Maux de tête ;
- Difficultés à se concentrer, à se souvenir, à lire ;
- Manque de motivation, d'entrain ;
- Baisse du désir sexuel (baisse de la libido) ;
- Difficultés à mener ses activités habituelles ;
- Épuisement physique, émotionnel ou psychologique.

4-Symptôme de l'asthénie (liée au dysfonctionnement du rythme cardiaque, à l'anémie et la baisse du SpO2) **11**

- De la fatigue
- Le teint pâle
- L'accélération du rythme cardiaque et un essoufflement plus prononcé à l'effort
- Les mains et les pieds froids
- Des maux de tête
- Des étourdissements
- Une plus grande vulnérabilité aux infections (en cas d'anémie aplasique, d'anémie à hématies falciformes ou d'anémie hémolytique)
- Des douleurs dans les membres, l'abdomen, le dos ou la poitrine,
- Des troubles visuels,
- Une jaunisse
- De l'enflure aux membres.

5-Symptômes de l'hypoxie ou de l'anoxie (baisse de l'oxygène dans le sang SpO2<60%) **18**

- Des nausées ;
- Des céphalées ou maux de tête ;
- Une hyperventilation ;
- Une tachycardie ;
- Des troubles du comportement.
- Fatigue
- Dyspnée ou manque du souffle
- Des palpitations peuvent être vues pendant les premières étapes de l'hypoxie.
- La fréquence cardiaque peut rapidement tomber par un degré significatif.
- Les rythmes cardiaques anormaux ou les arythmies peuvent se développer.
- De la pression sanguine augmentée en quelques premières étapes de l'hypoxie est
- Headedness léger
- Vomissement
- La cyanose est l'un des la plupart des signes classiques d'hypoxie.
- Les bouts des doigts, des tep, des oreilles et du nez peuvent devenir froids et bleutés en couleurs.
- Perte de conscience
- Grippages ou convulsions,
- Coma

6-Symptômes de la tachycardie (lié au Rythme cardiaque RC>100 BPM) **9**

- sensation de cœur qui s'accélère ;
- vertiges ;
- malaise ;
- essoufflement, difficulté à respirer ;
- palpitations ;

- faiblesse ;
- douleurs au thorax ;
- évanouissement ;
- perte de connaissance.

8-Symptômes de l'obésité (lié au poids ou IMC indice de masse corporelle) **10**

- Une surcharge graisseuse.
- Essoufflement,
- Fatigue
- Douleurs aux pieds
- Douleurs aux jambes
- Douleurs au dos
- Hypertension
- Insuffisance cardiaque
- Diabète
- Arthrose

9-Symptômes de la fièvre (liée à la température élevée T° au-delà de 40 °C) **13**

- Des battements cardiaques rapides ou une respiration rapide;
- Des modifications du comportement;
- Une humeur extrêmement difficile ou irritable;
- Des maux de tête, un cou raide, de la confusion mentale;
- Une douleur, une rougeur, ou une enflure localisée;
- Un vomissement ou une diarrhée qui persiste;
- Une pression artérielle basse ou des étourdissements (particulièrement en se tenant debout);
- Des convulsions;
- Une éruption cutanée;
- Des frissons violents et une sensation de brûlure ou de douleur surviennent à l'évacuation de l'urine;
- Un essoufflement, une respiration sifflante ou une toux;
- De la difficulté à se réveiller ou des délires;
- Un manque de réaction ou de la mollesse.

10-Symptômes de la dyspnée à l'effort ou au repos **4**

- Modification du rythme respiratoire ;
- Battement des ailes du nez :
- Toux :
- Douleur thoracique (tirage intercostal)

11-Symptômes du CMD (Cardiomyopathie Décompensée) **8**

- La fatigue ;
- Dyspnée à l'effort, y compris lors d'activités habituelles ;
- Une pâleur ;
- Des étourdissements ;
- Des vertiges ;
- Des évanouissements ;
- Palpitations cardiaques ;
- Douleur thoracique.

12- Symptômes de la Précordialgie **3**

- Douleurs discrètes ou au contraire très intenses, ressenties comme des coups d'aiguille ;
- Des brûlures,
- Des crampes, ou encore associées à une sensation de broiement ou de torsion.

13- Symptômes de la Péricardite **6**

- Un état fébrile ;
- Des difficultés respiratoires ;
- Une fatigue intense ;
- Des nausées ;
- Une toux importante ;
- Des gonflements au niveau de l'abdomen ou encore des jambes.

Annexe 9 : Protocole d'essai clinique validé par la Direction Médicale Scientifique

INSTITUT DE CARDIOLOGIE D'ABIDJAN	COMITE D'ETHIQUE	Code : DMS.02.04 Date : 03/03/2017 Version : 04 Page : 1/8	afaq ISO 9001 Qualité AFNOR CERTIFICATION

PROTOCOLE D'UN ESSAI CLINIQUE OU D'UNE EXPERIMENTATION

☒ THESE
☐ MEMOIRE
☐ AUTRE (précisez) .....

2. Titre de l'étude

Acquisition et transmission de données médicales par téléphonie mobile.

3. Etudiant/ Enquêteur/ Chercheur (E/E/C)

Nom et prénom : ACHI HARRISSON THIZIERS
Service : INP-HB YAMOUSSOUKRO
Chef de Service / Département: ECOLE DOCTORALE POLYTECHNIQUE

4. Directeur de l'étude

Nom: Professeur Haba Cisse Theodore
Adresse: 07842000
Service /Département : Professeur Adoubi, ICA. 02024436

5. Type d'étude

5.1. ← EVALUATION D'UN TRAITEMENT

A. ← Essai clinique
← Expérimentation
← Expérimentation non commerciale (académique)

B. ← Monocentrique
← Multicentrique

C. ← Phase I
← Phase II
← Phase III
← Phase IV
← Titre compassionnel
← Autre

D. ← Essai impliquant des médicaments de thérapie génique et de cellulothérapie somatique, ainsi que tous les médicaments contenant des organismes génétiquement modifiés.

Dénomination du traitement:

[ ]

← Chez des volontaires sains
← Chez des patients

Diagnostic des patients enrôlés:

[ ]

5.2. ← EVALUATION D'UN ACTE DIAGNOSTIQUE

Dénomination de l'acte diagnostique

[collecté de constantes cliniques et biologiques à l'aide de deux multi-capteurs nommés Health monitor]

← Chez des volontaires sains
(←) Chez des patients

Diagnostic des patients enrôlés:

[Tension artérielle, Saturation en oxygène dans le sang rythme cardiaque, ECG, Glycémie, cholestérol.]

5.3. ← EVALUATION D'UNE ETUDE OBSERVATIONNELLE

← Etude prospective ← Etude rétrospective

6. Originalité de l'étude

6.1. En quoi cette étude présente-t-elle un caractère original, utile et bénéfique?

[Montrer qu'avec des équipements fiables et peu coûteux, on peut collecter directement des constantes sur des patients, les analyser et les interpréter, puis les transmettre à de spécialiste]

6.2. Le protocole comprend-il des références bibliographiques récentes documentant l'intérêt de l'étude?

← (oui) ← non

7. Donnez une évaluation des risques de l'expérimentation

7.1. Pour le sujet d'expérience

Aucun

7.2. Pour l'expérimentateur et le personnel

Aucun

7.3. Pour l'environnement

Aucun

8. Eléments relatifs au protocole

8.1. L'expérimentation concerne des enfants de moins de 18 ans
← oui ← (non)

8.2 L'expérimentation concerne des majeurs, incapables de donner leur consentement
← oui ← (non)

8.3 L'expérimentation concerne des personnes dont le consentement ne peut être recueilli du fait de l'urgence.
← oui ← (non)

8.4 L'expérimentation concerne des patients de plus de 80 ans
← oui ← (non)

8.5. L'expérimentation prévoit l'inclusion de femmes enceintes
← oui ← (non)

8.6. Les autres critères d'inclusion sont explicités
← (oui) ← non

8.7. Les autres critères d'exclusion sont explicités
← (oui) ← non

- 4 -

8.8. Le protocole prévoit des prélèvements de matériel humain
← oui ← non

Si oui, ← sang
← urines
← autres liquides biologiques (préciser la nature)

← biopsies (préciser le site de prélèvement)

8.7. Le protocole prévoit d'autres examens spécialisés (y compris à l'inclusion)
← oui ← non
Si oui, lesquels?

8.8. Le protocole prévoit l'administration d'éléments radioactifs
← oui ← non

9. Mode d'appréciation du consentement du patient ou du volontaire sain

9.1. Accord écrit, après avoir reçu les informations signées et datées du volontaire sain, du patient et/ou de ses parents/tuteur/représentant légal, sur un formulaire rédigé dans la langue de l'intéressé
← oui ← non

9.2. Lorsque la personne participant n'est pas en mesure d'écrire, son accord verbal devant au moins un témoin majeur et indépendant vis-à-vis du promoteur et de l'investigateur

← oui ← non

9.3. Autre

10. Confidentialité - Protection de la vie privée

Dans le principe, l'ensemble des données collectées durant l'étude doivent être gardées rigoureusement anonymes, sauf vis-à-vis des personnes amenées à assurer la continuité des soins. Cet anonymat concerne aussi bien les cahiers d'observation, les dossiers médicaux, les formules de consentement éclairé et tout listing des patients inclus dans une étude.
Précisons que le dossier médical ne peut sous aucun prétexte être consulté par une tierce personne, que ce soit à l'occasion du monitoring de l'étude ou de toute procédure d'audit.

10.1. Quelles sont les précautions prises pour assurer la confidentialité des données, dans le cadre de leur collecte, de leur stockage, de leur transmission et de leur traitement?

Pour le consentement éclairé
Les données en possession seule de l'investigateur principal

Pour les cahiers d'observation
Gardés soigneusement par l'investigateur principal

Pour les procédures de monitoring
les noms sont codés

Pour toute procédure d'audit

Pour le stockage des données
les noms sont codés (et cryptés)

10.2. Dans le cadre de l'étude des données à caractère personnel non-anonymisées seront-elles communiquées à des tiers ?
← oui ← (non)

Dans le cas affirmatif, est-ce qu'une déclaration de traitement de données à caractère personnel a-t-elle été introduite par le directeur de l'étude auprès du Ministère de la Justice et des libertés individuelles?
← oui ← non

11. Aspects financiers de l'étude

11.1

L'ensemble des coûts de l'étude et de ses éventuelles conséquences doit être explicitement pris en charge par le directeur de l'étude. Ceci concerne les consultations pour évaluation et les examens spécialisés réalisés dans le cadre de l'étude. Aucun de ces coûts ne peut être imputé, même partiellement, à l'assurance maladie ou à tout organisme assureur dont dépendrait le patient.
Nous rappelons par ailleurs que les honoraires générés par toute étude doivent être perçus dans le respect des obligations contractuelles de l'E/E/C.

11.2. Coûts de l'étude

Consultations
← oui ← non
Prises en charge par?
Par les propres moyens de l'investigateur

Examens spécialisés
← oui ← non
Pris en charge par?
par l'investigateur

11.3. Assurance

Le directeur de l'étude et E/E/C assument conjointement, même sans faute, la responsabilité du dommage causé au participant, dommage lié directement ou indirectement à l'expérimentation.
← oui ← non

E/E/C	DIRECTEUR DE L'ETUDE	AVIS DU COMITE D'ETHIQUE	DMS
Date :	Date : 27/11/18	Date : 14/12/18	Date :
26/11/2018	Pr ACHI Harrisson Maître de Conférences Cardiologie Thoracique	FAVORABLE	

Dr TANOH Yves B.
Professeur
Chirurgie Thoracique

*E/E/C : Etudiant/ Enquêteur/ Chercheur
*DMS : Directeur Médical et Scientifique

NB : Un exemplaire du document final devra être remis au DMS de l'ICA.

Annexe

Essai clinique dénommé ci-après "essai" : toute investigation menée chez la personne humaine, afin de déterminer ou de confirmer les effets cliniques, pharmacologiques et/ou les autres effets pharmacodynamiques d'un ou de plusieurs médicaments expérimentaux et/ou de mettre en évidence tout effet indésirable d'un ou de plusieurs médicaments expérimentaux et/ou d'étudier l'absorption, la distribution, le métabolisme et l'élimination d'un ou de plusieurs médicaments expérimentaux dans le but de s'assurer de leur innocuité et/ou efficacité.

Expérimentation : essai, étude ou investigation menée sur la personne humaine qui a pour objectif le développement des connaissances propres à l'exercice des professions de soins de santé.

Etudes rétrospectives : toutes études dans lesquelles on examine le passé en utilisant les données déjà disponibles, partant des dossiers médicaux ou administratifs existants. Dans ces études, les personnes dont il s'agit ne sont pas elles-mêmes impliquées.

Expérimentation non commerciale (académique) : toute expérimentation dont le promoteur est une université, un hôpital ou un Fond de la Recherche scientifique. Le promoteur exerce les droits de propriété intellectuelle sur la conception de l'expérimentation, sa réalisation et les données scientifiques qui en résultent.

Annexe 10 : Tableau récapitulatif des constantes collectées

Constante	Valeurs normales	Valeurs anormales	Valeurs critiques	marges
SpO2 (%)	[96-100]	[76-96]	<60	± 20
TA (PAS/PAD) mmHg	140/90	[140-150/90-100]	>150/100	± 10
Gl (g/l)	[0,6-1,10]	[1,26-1,36]	>1,40	± 0,20
Ac.Ur µmol/l Ou en mg/L	[150-300]F ou [25-60] mg/L [300-400] H ou [35-70] mg/L	<25 mg/L ou >70	-	-
Hb (g/10ml)	[12-14.5] H [11-13] F	[9-12] ou [14.5-17.5] [8-11] ou [13-17]	>17.5 >17	± 3
Ht (%)	[36-48] F [40-52] H	[30-36] ou [48-55] [36-40] ou [40-46]	<30 ou >55 F <36 ou >46 H	± 6
RC (Bpm)	[60-100]	[40-60] et [100-120]	<40 et >120	± 20
T° (°C)	[32-37]	[37-40]	>40	± 3
C-LDL (g/L)	[0,9-1,6]	<0,9 ou >1.6	-	-
IMC	[18.5, 24.9]	[25, 29,9]	>30	-
ECG	-	-	-	-
PH	[7,3 - 7,4]	<7 ou [7,4-7,45]	<5 ou >7,45	-

Annexe 11 : spécifications techniques pour le bon fonctionnement du « 6 in 1 Health Monitor » (Source : Notice de l'équipement)

Spécifications générales

- La température idéale : 5°C - 40°C
- Pas de tissus synthétiques à proximité.
- Humidité ambiante: 15%~80%
- Pression barométrique: 70 kPa ~ 106 kPa
- Protocole de communication Bluetooth 4.0: 2.4000 ~ 2.4835 GHz

Distance minimum de séparation entre les équipements mobile à RF et les Multi-capteurs EasyMate et « 6 in 1 Health Monitor »

Sortie maximum de puissance de l'émetteur en Watt	Distance de séparation selon la fréquence de transmittance (en mètre)		
	150 kHz à 80 MHz $d=1,2\sqrt{P}$ Avec P (Puissance maximum de sortie de l'émetteur)	80 MHz à 800 MHz $d=1,2\sqrt{P}$	800 MHz à 2,5 GHz $d=2,3\sqrt{P}$
0,01	0,12	0,12	0,23
0,1	0,38	0,38	0,73
1	1,2	1,2	2,3
10	3,8	3,8	7,3
100	12	12	23

Pour le test de la tension artérielle/Rythme cardiaque:

- Méthode de mesure: méthode oscillométrique
- Intervalle de mesure: 0-300 mmHg
- Tension systolique: 60-260 mmHg
- Tension diastolique: 40-199 mmHg
- Rythme cardiaque: 40-180 bpm
- Erreur de mesure pour la tension artérielle: ±3 mmHg
- Erreur de mesure pour le rythme cardiaque: ±5%

Pour le test d'oxygène dans le sang (SpO2):

- Méthode de mesure: méthode réflective
- Intervalle de mesure: 90%-99% mmHg
- Erreur de mesure pour le SpO2: ±2%

Pour la mesure de la température:

- Méthode de mesure: méthode infrarouge
- Zone de mesure: frontale
- Intervalle: 32°C-42°C
- Erreur de mesure pour la température:

  36-39°C ±0.2°C

  >39°C ou <36°C ±0.3°C

Pour la bonne mesure du glucose:

- Méthode de mesure: méthode infrarouge
- Intervalle de mesure: 1.1 mmol/L ~ 33.3 mmol/L
- Répétabilité du système de test:

  Concentration de l'échantillon <5.5 mmol/L (100mg/dL)

  Imprécision du test est la déviation standard: SD<0.42 mmol/L (<7.7 mg/dL)

  Concentration de l'échantillon ≥5.5 mmol/L (≥ 100mg/dL)

  Imprécision du test est le coefficient variable: CV<7.5%

Pour la bonne mesure de l'ECG:

- Mode de Mesure: une seule dérivation
- Impédance d'entrée: >10 MΩ
- Circuit de courant d'entrée: < 0.1 μA
- Voltage de calibration: 1mV±0.05mV
- Tolérance de la sensitivité: <10%
- Fréquence de réponse: 0.5 ~40Hz
- Dépassement: pas plus de 20%
- Humidité de l'environnement: 5°C – 40°C

Annexe 12 : Spécifications pour le bon fonctionnement des EasyMate (Source : Notice de l'équipement)

Spécifications générales :

- La température idéale : 14°C - 40°C²
- Pas de tissus synthétiques.
- Le téléphone cellulaire ou tout équipement à résonnance électromagnétique doit être tenu à une certaine distance (Tableau suivant).
- Le volume de l'échantillon doit être supérieur à 0.8 µl pour l'hémoglobine, 2.6 µl pour le Glucose, 22 µl pour le Cholestérol et 2.7 µl pour l'acide urique

Composants dans le sang dont la concentration peuvent entrainer de mauvais résultats pour le EasyMate GHb

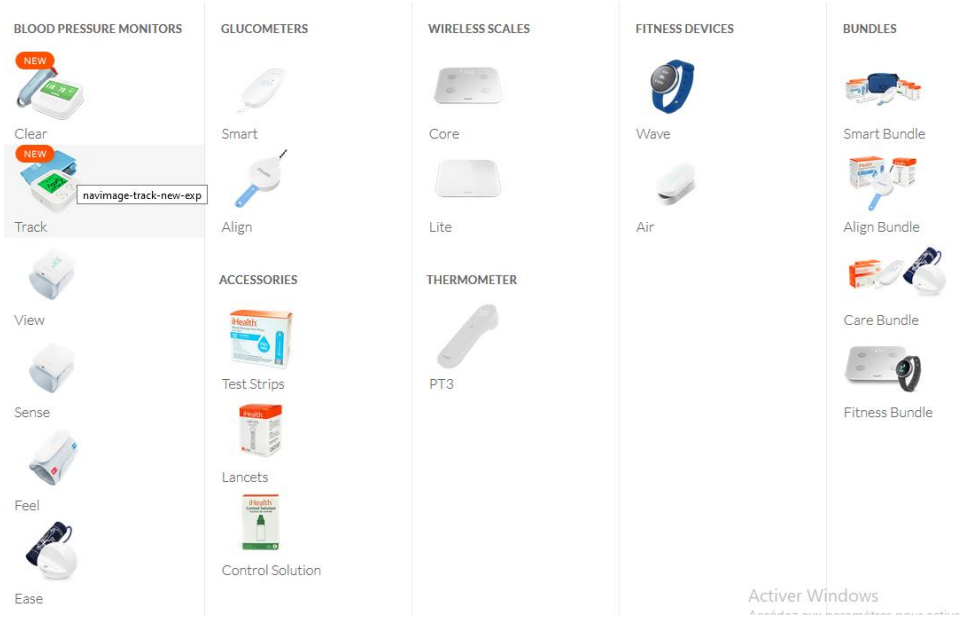
Composants dans le sang	Glucose	Hémoglobine
Acide ascorbique (Vitamine C)	>150 mg/dL	>150 mg/dL
Amiloride	>20 mg/dL	x
Acetaminophen	>8 mg/dL	x
L-Dopa	>20 mg/dL	>20 mg/dL
Dopamine	>20 mg/dL	>20 mg/dL
Methyl-Dopa	>4 mg/dL	>4 mg/dL
Galactose	>400 mg/dL	x
Acide urique	>10.5 mg/dL	x
Xylose	>50 mg/dL	x
Hématocrite	<30%, >50%	<20%, >70%

Composants dans le sang dont la concentration peuvent entrainer de mauvais résultats pour le EasyMate GCU

Composants dans le sang	Cholestérol	Acide urique
Acetaminophen	20 mg/dL	2 mg/dL
Amiloride	-	20 mg/dL
Acide ascorbique	10 mg/dL	5 mg/dL
Bilirubin	21.2 mg/dL	-
Cholestérol	-	358 mg/dL
Créatinine		30 mg/dL
Diclofenac	-	75 mg/dL
Dopamine	10 mg/dL	2 mg/dL
Ketoprofen	-	500 mg/dL
L-Dopa	5 mg/dL	5 mg/dL
Méthyl-Dopa	-	1.0 mg/dL
Acide urique	19.5 mg/dL	-
Hématocrite	<30%, >55%	<30%, >55%

Annexe 13 : Présentation de capteurs de la société Ihealth (A), (B), (C), (D) et tableau comparatif de coût et de consommation de leur dispositif et du notre (E).

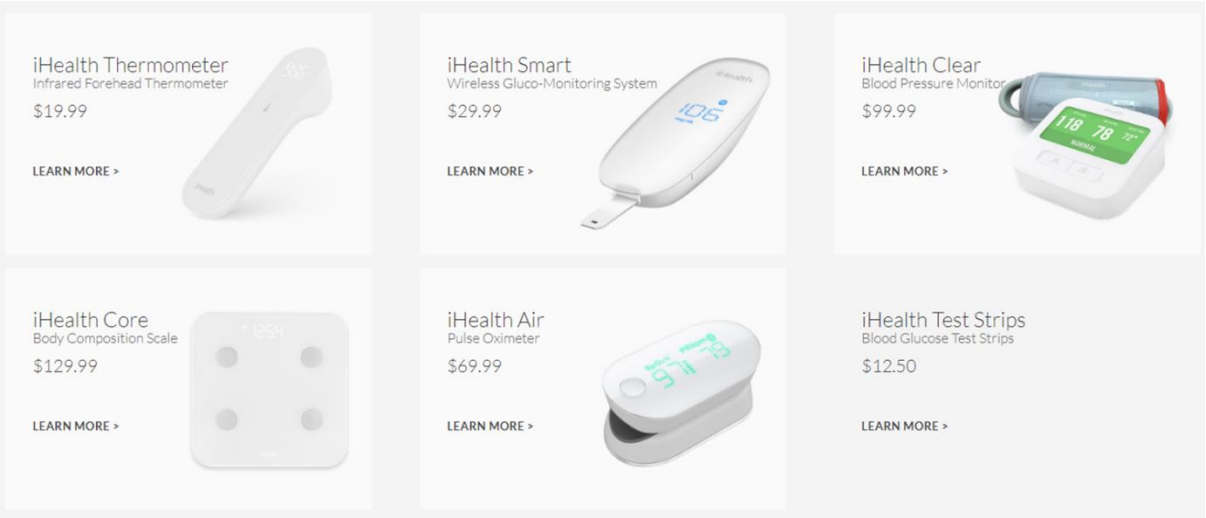
(A) https://ihealthlabs.com/mobile-apps



(B) https://www.google.fr/search

(C) https://ihealthlabs.eu/fr/24-tension

(D) https://ihealthlabs.com

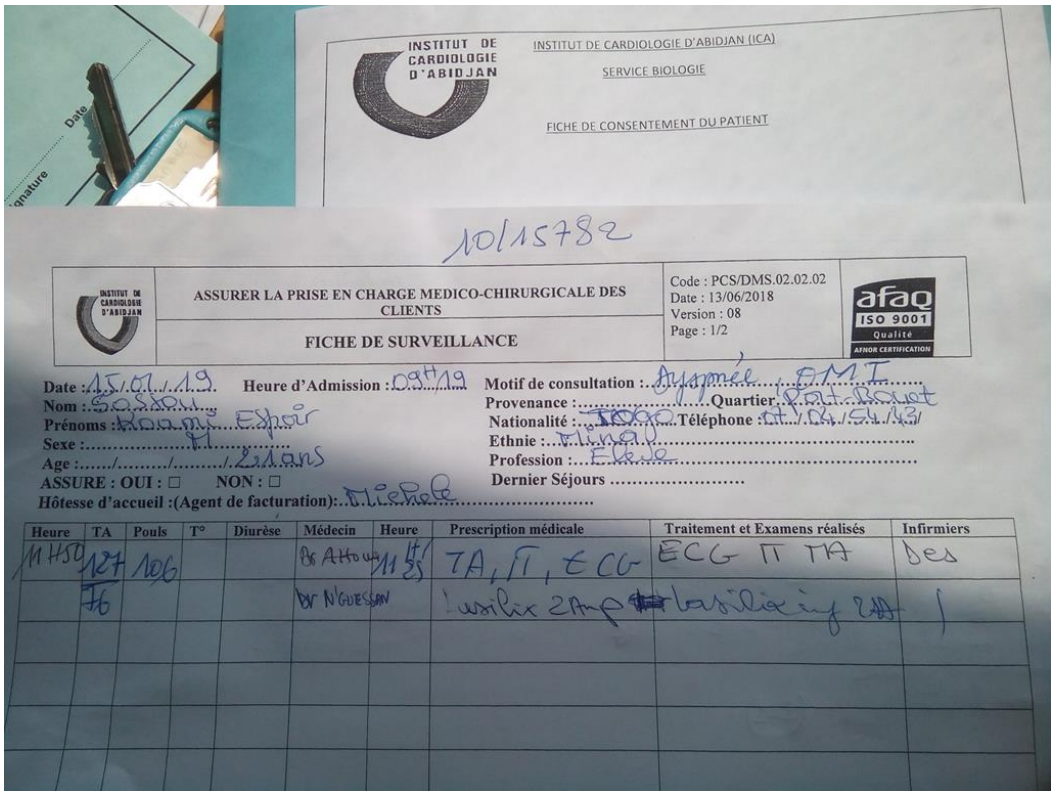


(E)

Capteur	Nombre	Coût moyen	Consommation moyenne d'énergie
Notre dispositif	3	250.000 F CFA	(2x1,5 V)+5V=8V
Capteurs Ihealth	6	450 Euros (295.280 F CFA)	24V

Annexe 14 : Fiche patient de l'ICA (A) et cartographie de provenance des patients (B).

(A)



INSTITUT DE CARDIOLOGIE D'ABIDJAN

INSTITUT DE CARDIOLOGIE D'ABIDJAN (ICA)

SERVICE BIOLOGIE

FICHE DE CONSENTEMENT DU PATIENT

10/15782

INSTITUT DE CARDIOLOGIE D'ABIDJAN

ASSURER LA PRISE EN CHARGE MEDICO-CHIRURGICALE DES CLIENTS

FICHE DE SURVEILLANCE

Code : PCS/DMS.02.02.02
Date : 13/06/2018
Version : 08
Page : 1/2

afaq ISO 9001 Qualité AFNOR CERTIFICATION

Date : 15.07.19 Heure d'Admission : 09h19 Motif de consultation : Asthénie, DMI

Nom : Sossou Provenance : ..... Quartier : Cocody Deux

Prénoms : Koamy Espoir Nationalité : Togo Téléphone : 07.04.54.43

Sexe : F Ethnie : Mina

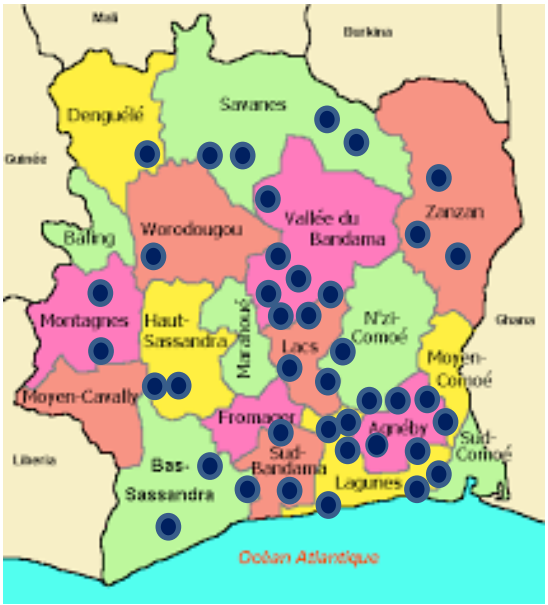
Age : ...../...../...../ 2 ans Profession : Elève

ASSURE : OUI : ☐ NON : ☐ Dernier Séjours .....

Hôtesse d'accueil :(Agent de facturation): Michelle

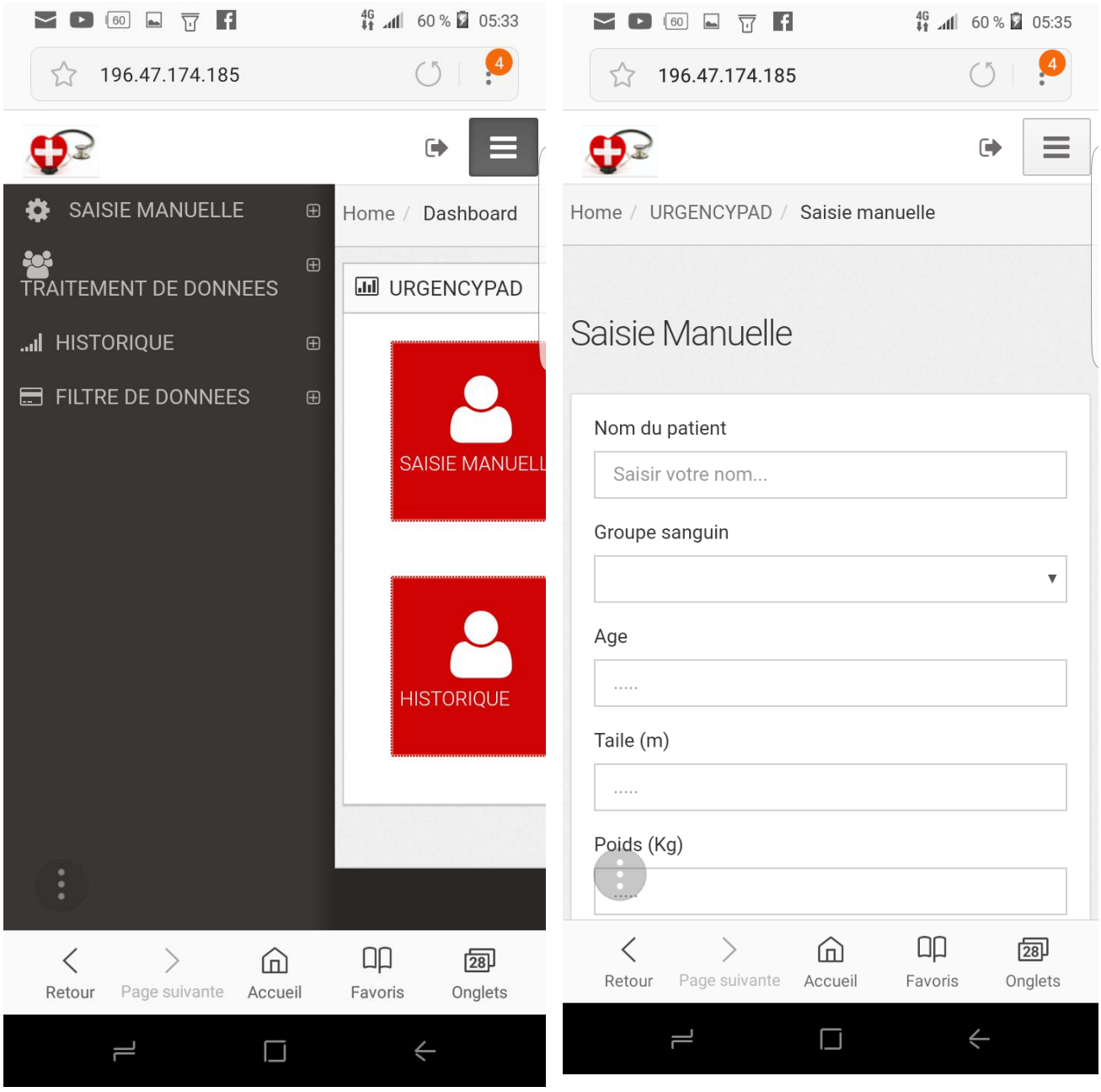
Heure	TA	Pouls	T°	Diurèse	Médecin	Heure	Prescription médicale	Traitement et Examens réalisés	Infirmiers
11H50	127	106			Dr Attoh	11h35	TA, T, ECG	ECG TA	Des
	76				Dr N'Guessan		1 usilix 2Amp + lasilix 2Amp		

(B)



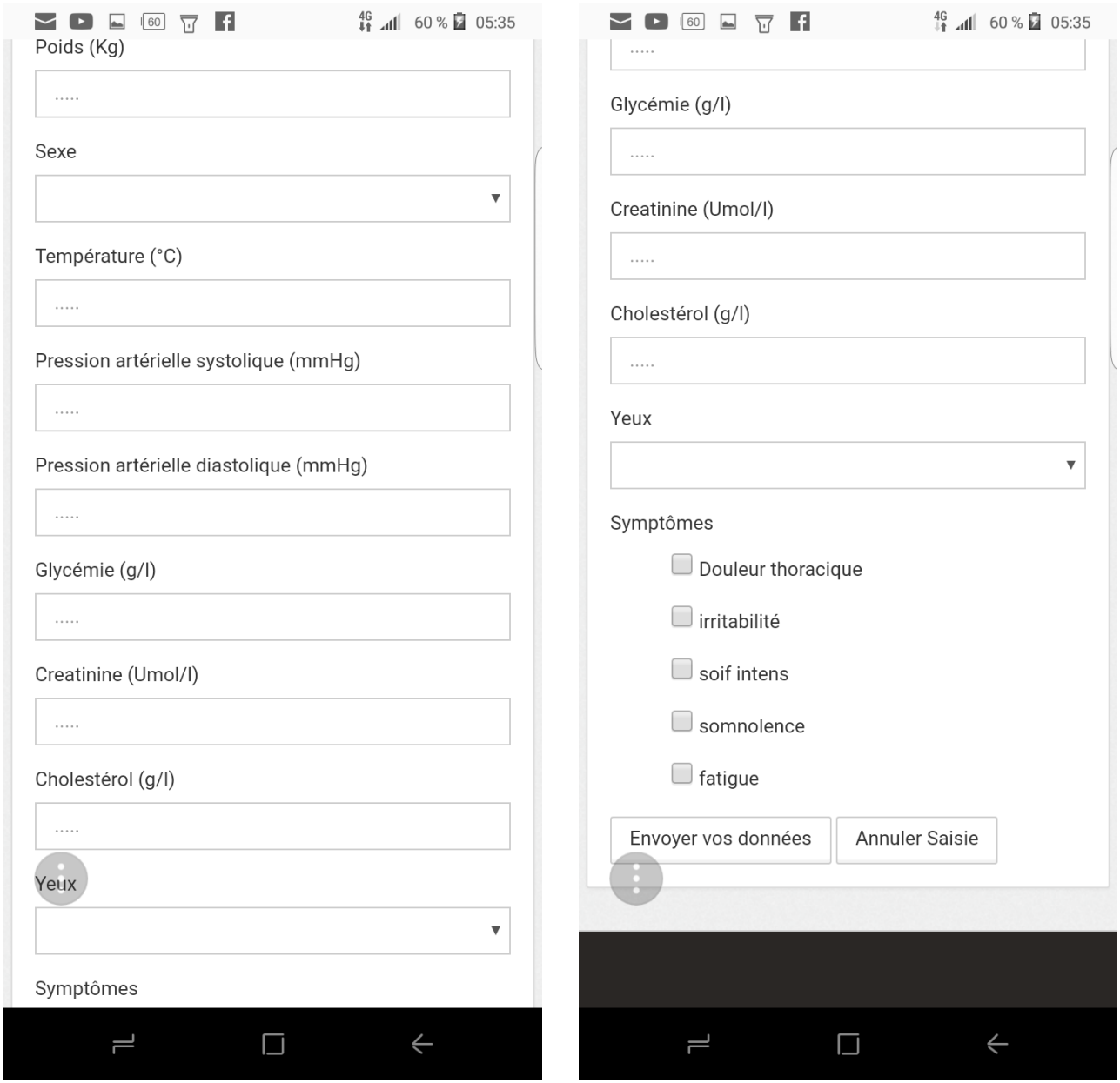
Annexe 15 : Interfaces de notre application mobile URGENCYPAD

(A) (B)



L'écran (A) permet d'accéder à l'interface de saisie manuelle des constantes que nous pouvons observer sur l'écran (B).

(C) (D)

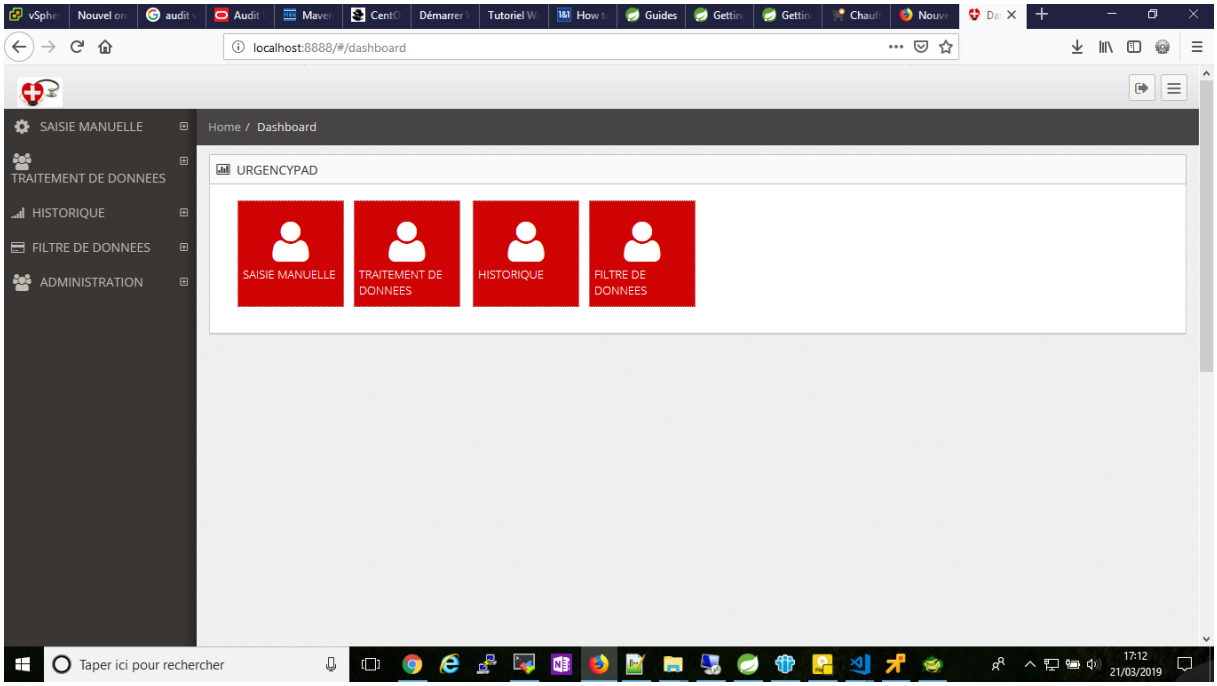


Les écrans (C) et (D) constituent la même interface de saisie manuelle des constantes sur l'application.

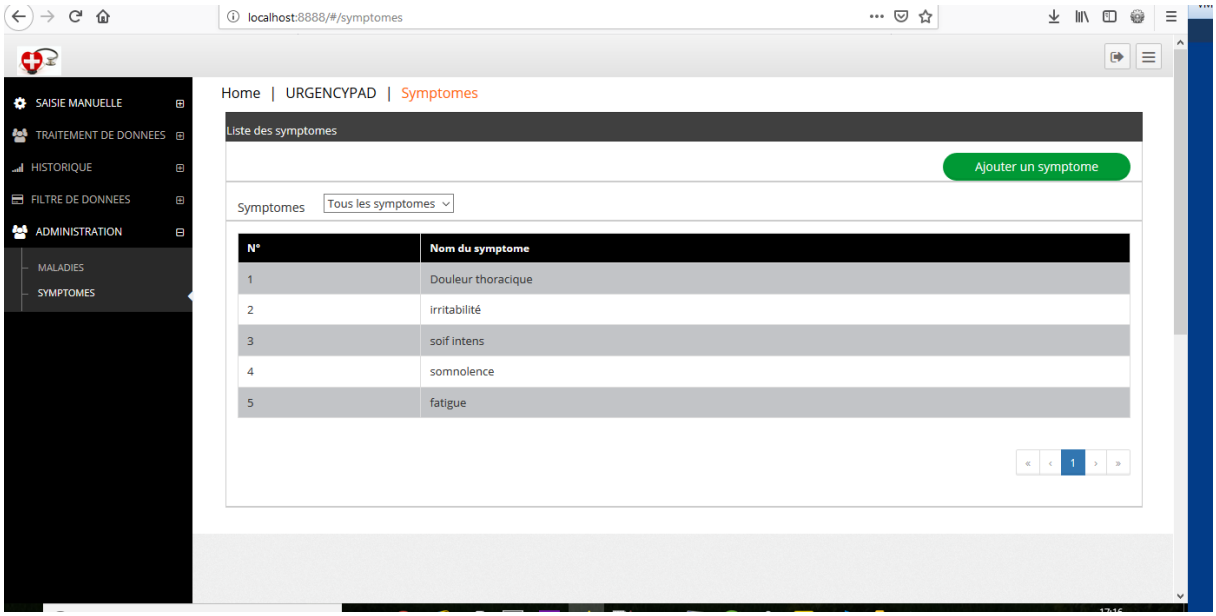
Annexe 16 : Interfaces de l'application web sur le serveur cloud.

(A) permet d'accéder à la consultation des données saisies dans la base de données, tandis que (B) et (C) permettent de créer de nouveaux symptômes. (D) et (E) permettent d'ajouter une maladie, et (F) permet également la saisie de constantes et permet de cocher des symptômes.

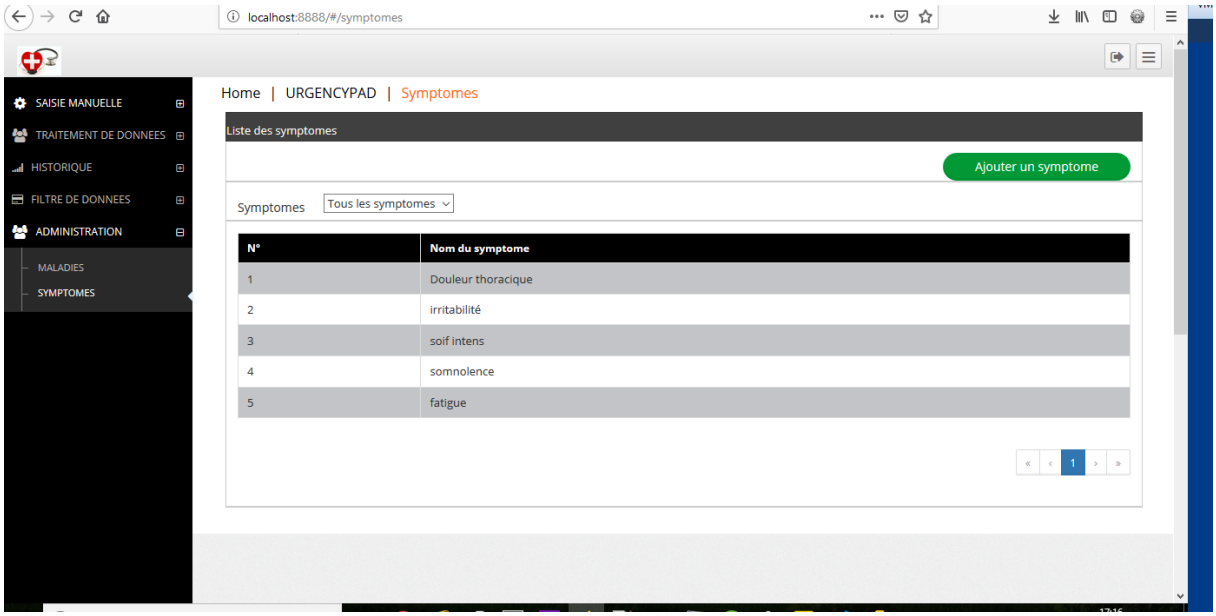
(A)



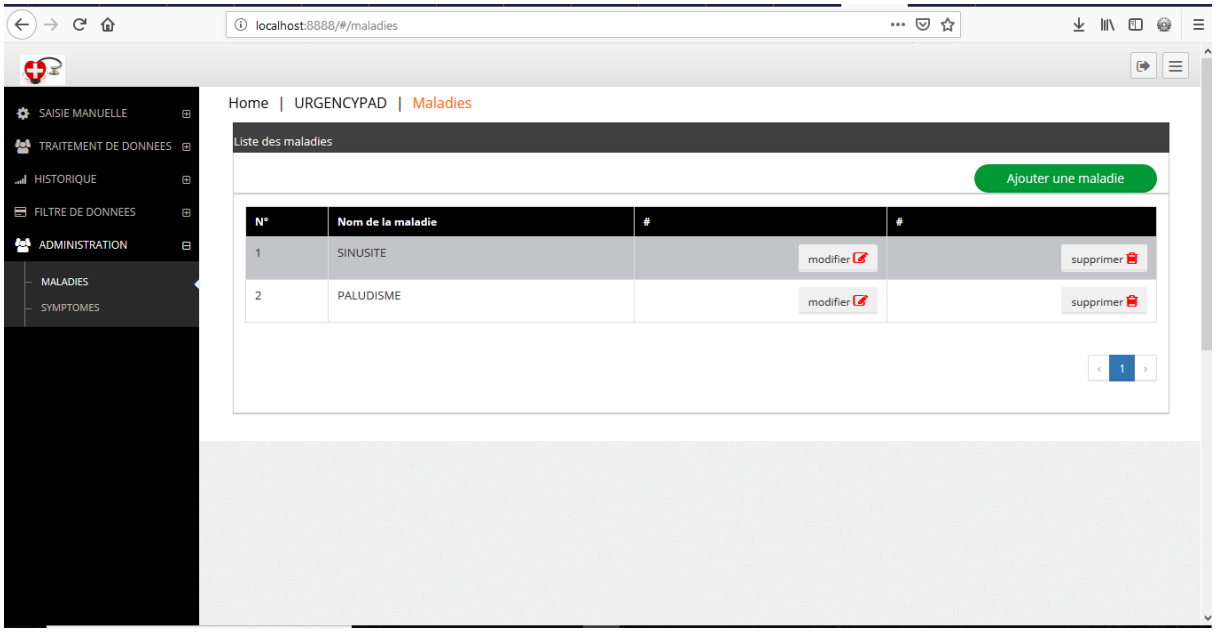
(B)



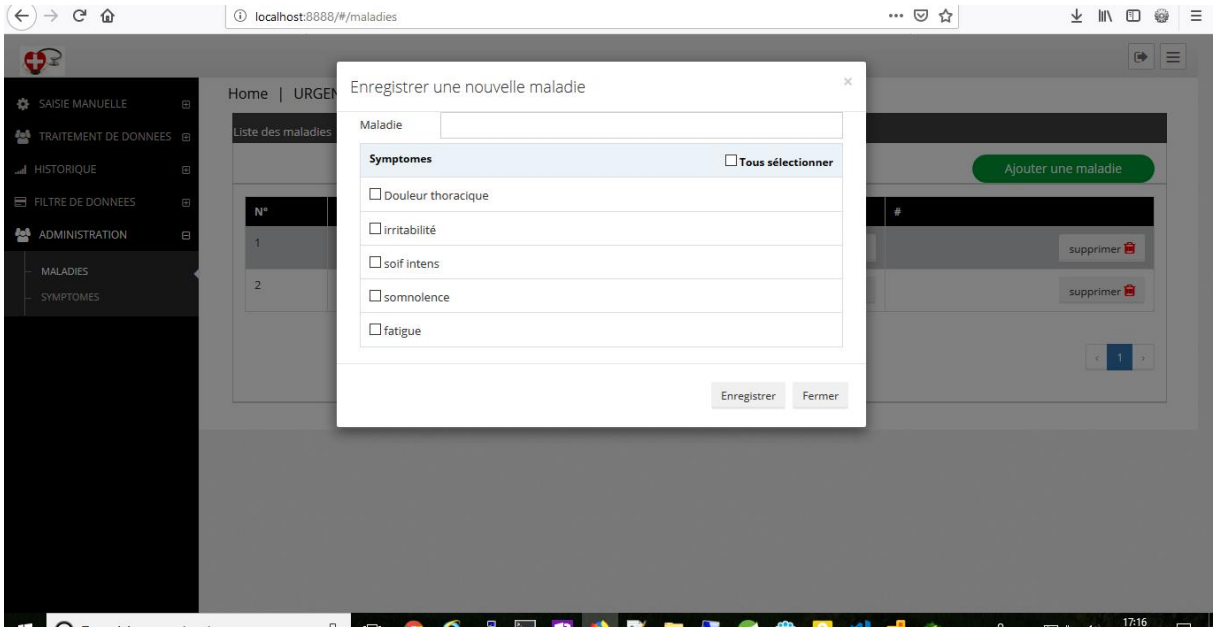
(C)


localhost:8888/#/symptomes
SAISIE MANUELLE
TRAITEMENT DE DONNEES
HISTORIQUE
FILTRE DE DONNEES
ADMINISTRATION
MALADIES
SYMPTOMES
Home | URGENCYPAD | Symptomes
Liste des symptomes
Ajouter un symptome
Symptomes
Tous les symptomes
N°
Nom du symptome
1
Douleur thoracique
2
irritabilité
3
soif intens
4
somnolence
5
fatigue

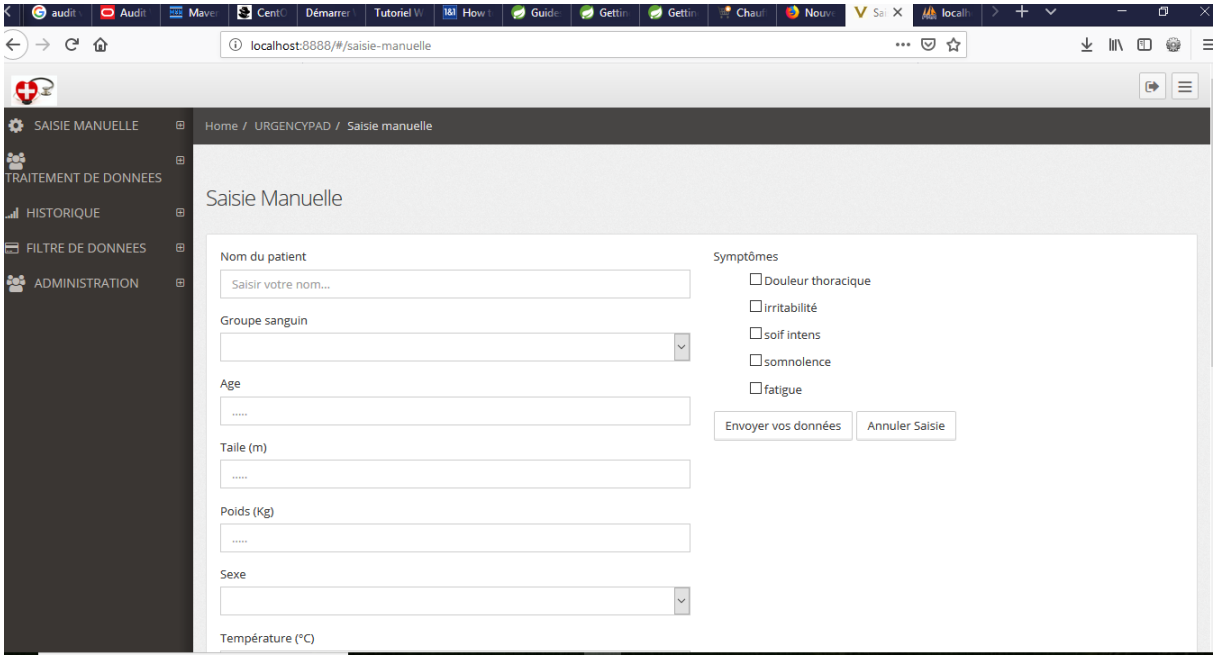
(D)


localhost:8888/#/maladies
SAISIE MANUELLE
TRAITEMENT DE DONNEES
HISTORIQUE
FILTRE DE DONNEES
ADMINISTRATION
MALADIES
SYMPTOMES
Home | URGENCYPAD | Maladies
Liste des maladies
Ajouter une maladie
N°
Nom de la maladie
#
#
1
SINUSITE
modifier
supprimer
2
PALUDISME
modifier
supprimer

(E)


localhost:8888/#/maladies
SAISIE MANUELLE
TRAITEMENT DE DONNEES
HISTORIQUE
FILTRE DE DONNEES
ADMINISTRATION
MALADIES
SYMPTOMES
Home | URGEN
Liste des maladies
Ajouter une maladie
N°
1
2
supprimer
supprimer
Enregistrer une nouvelle maladie
Maladie
Symptomes
Tous sélectionner
Douleur thoracique
irritabilité
soif intens
somnolence
fatigue
Enregistrer
Fermer

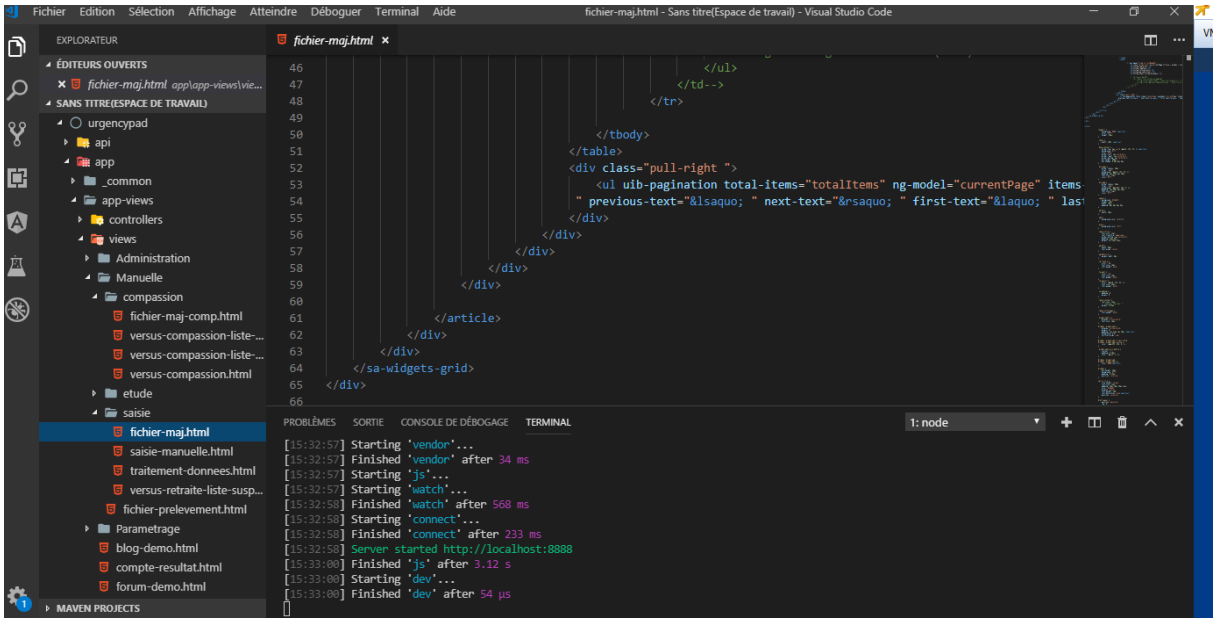
(F)


localhost:8888/#/saisie-manuelle
SAISIE MANUELLE
TRAITEMENT DE DONNEES
HISTORIQUE
FILTRE DE DONNEES
ADMINISTRATION
Home / URGENCYPAD / Saisie manuelle
Saisie Manuelle
Nom du patient
Saisir votre nom...
Groupe sanguin
Age
Taille (m)
Poids (Kg)
Sexe
Température (°C)
Symptômes
Douleur thoracique
irritabilité
soif intens
somnolence
fatigue
Envoyer vos données
Annuler Saisie

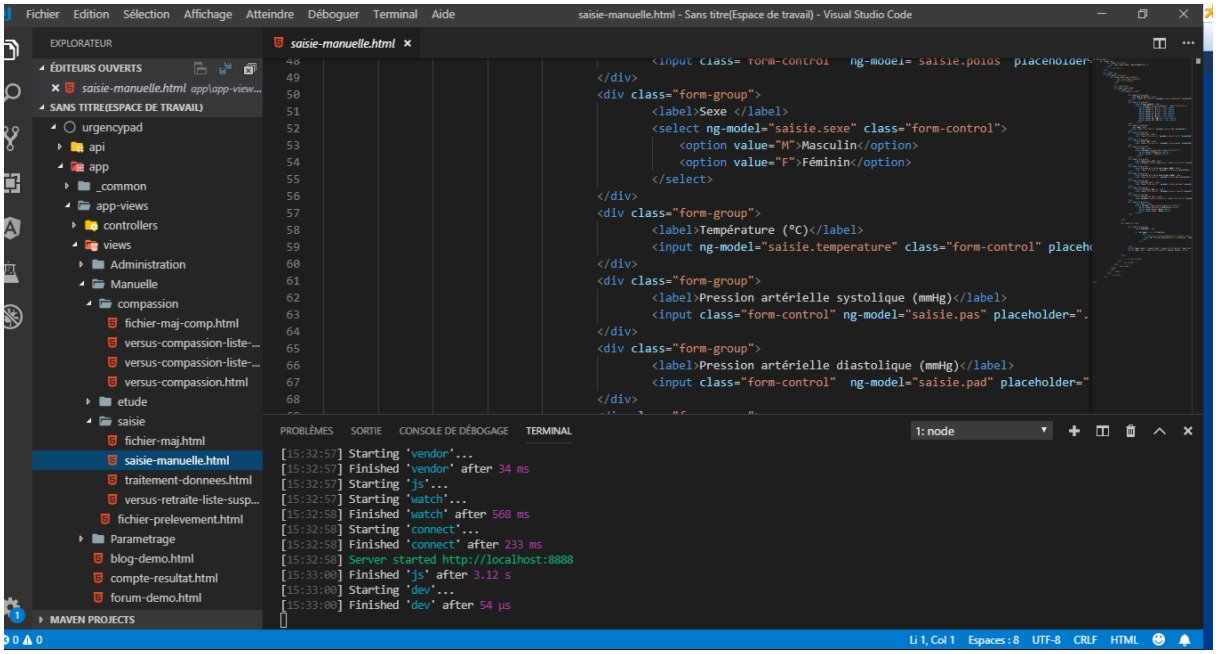
Annexe 17 : Interfaces de l'environnement JAVA.

(A) et (B) représente le code source de développement de l'application

(A)

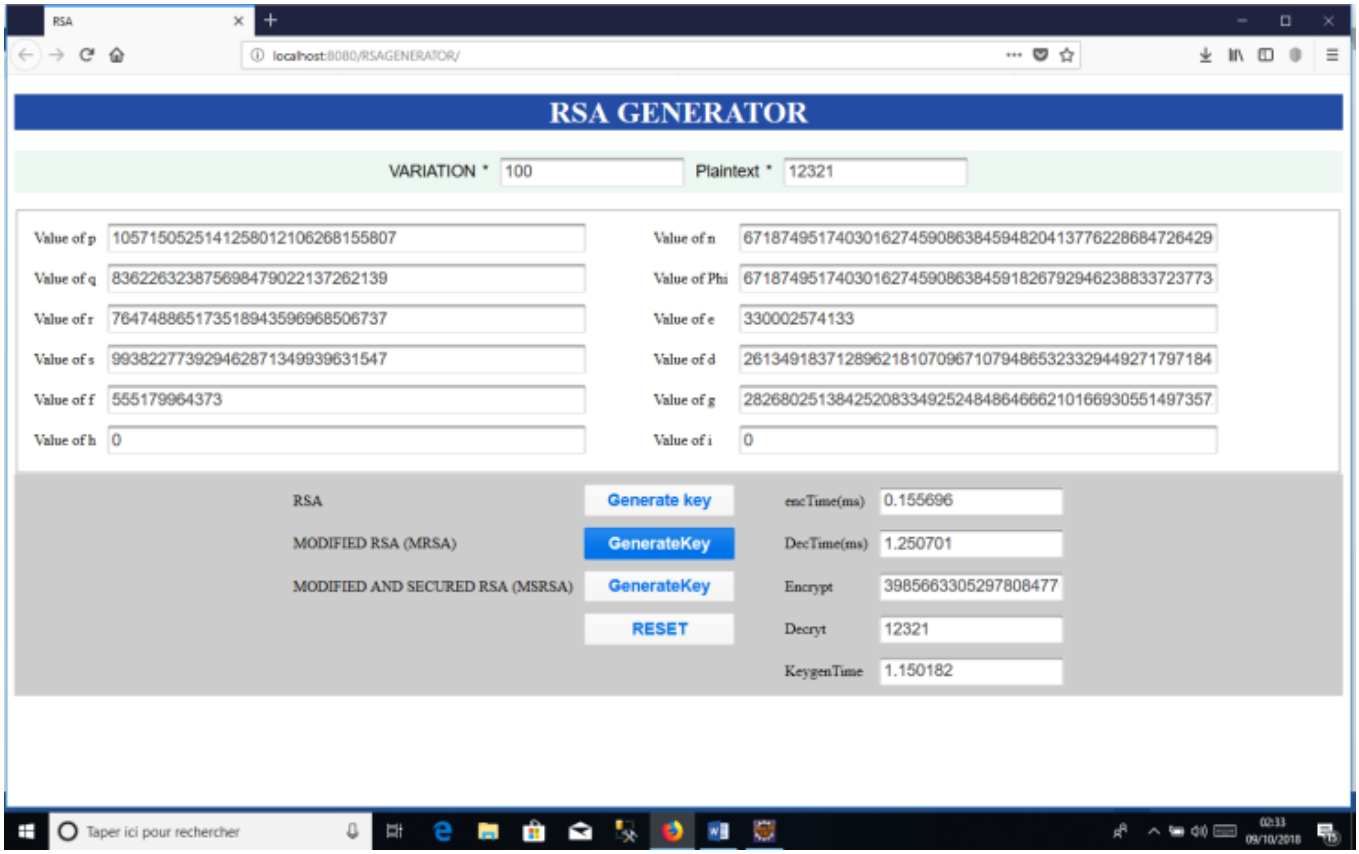


(B)

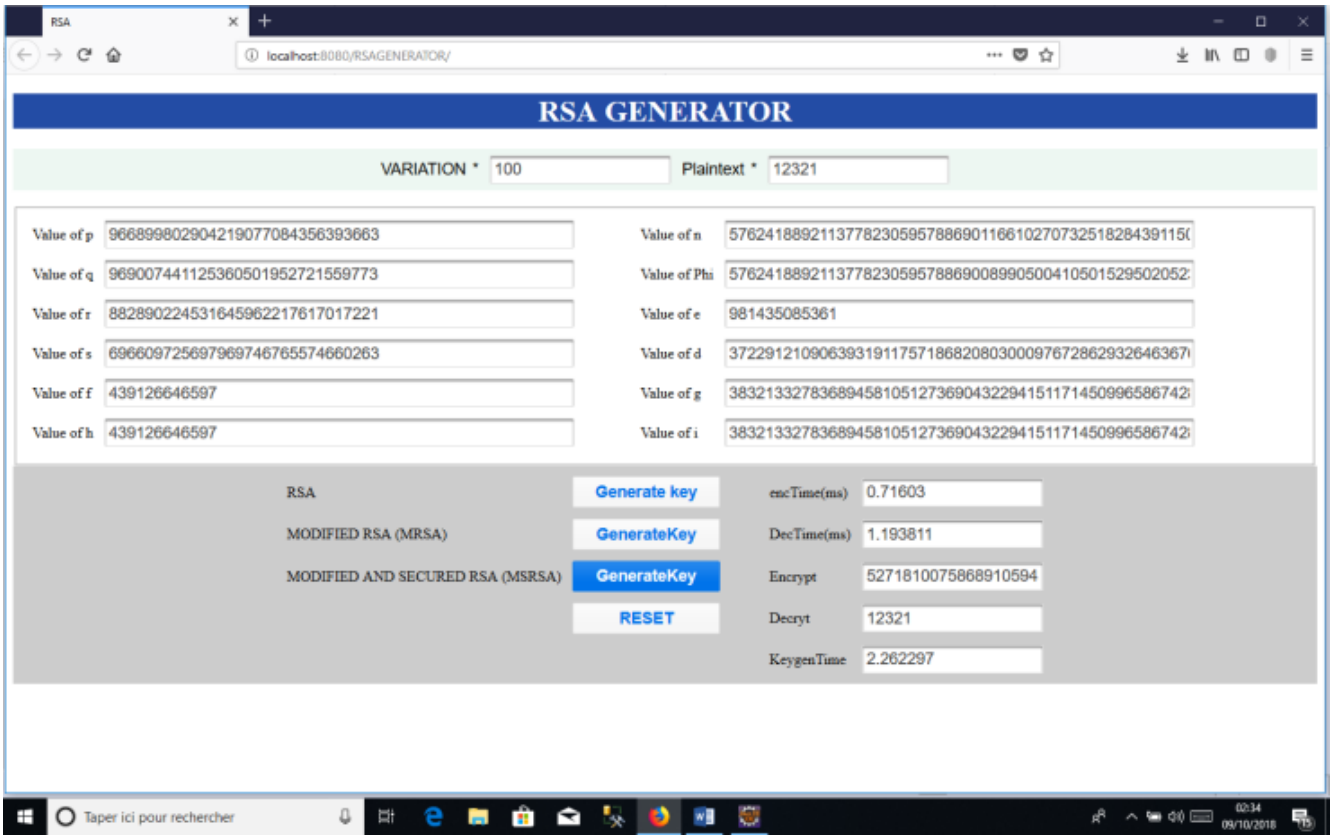


Annexe 18 : Interfaces java 'RSA GENERATOR' pour une taille de bit à 100, avec le même message 12321, dans MRSA (A), puis dans EMSRSA (B).

(A)



(B)


RSA
localhost:8080/RSAGENERATOR/
RSA GENERATOR
VARIATION * 100
Plaintext * 12321
Value of p 966899802904219077084356393663
Value of q 969007441125360501952721559773
Value of r 882890224531645962217617017221
Value of s 696609725697969746765574660263
Value of f 439126646597
Value of h 439126646597
Value of n 576241889211377823059578869011661027073251828439115(
Value of Phi 576241889211377823059578869008990500410501529502052
Value of e 981435085361
Value of d 372291210906393191175718682080300097672862932646367
Value of g 383213327836894581051273690432294151171450996586742
Value of i 383213327836894581051273690432294151171450996586742
RSA
Generate key
MODIFIED RSA (MRSA)
GenerateKey
MODIFIED AND SECURED RSA (MSRSA)
GenerateKey
RESET
encTime(ms) 0.71603
DecTime(ms) 1.193811
Encrypt 5271810075868910594
Decryt 12321
KeygenTime 2.262297
Taper ici pour rechercher

Annexe 19 : Tableau comparatif des prix des équipements de collecte des deux méthodes

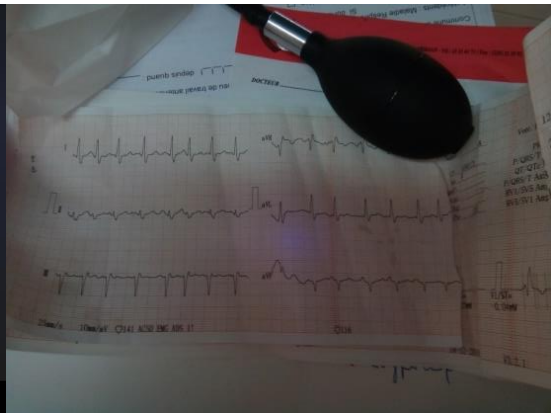
 SYSMEX CA-600 series	3.000.000 F CFA HT
 Stago STA compact Max	3.500.000 F CFA HT
 GEM Premier 3000	2.000.000 F CFA HT
 Hitachi Cobas c 311	11.000.000 F CFA HT
 Hitachi Cobas e 411	14.610.000 F CFA HT
Coût total pour les quelques équipements de l'ICA	34.110.000 F CFA HT
 Multi-capteur « 6 in 1 health Monitor »	150.000 F CFA HT
 Multi-capteur EasyMate GhCU et EasyMate GHb	90.000 F CFA HT
 Bandelette d'urine 10 paramètres	10.000 F CFA HT
Coût total des équipements de notre dispositif expérimental	250.000 F CFA

Même en ajoutant le coût d'un serveur cloud de 1.500.000 F CFA, ce tableau nous montre que le dispositif de l'ICA coûte au moins 20 fois plus cher que notre dispositif expérimental.

Annexe 20 : ECG comparés, ayant étant obtenus par notre méthode à gauche et celle de l'ICA à droite.

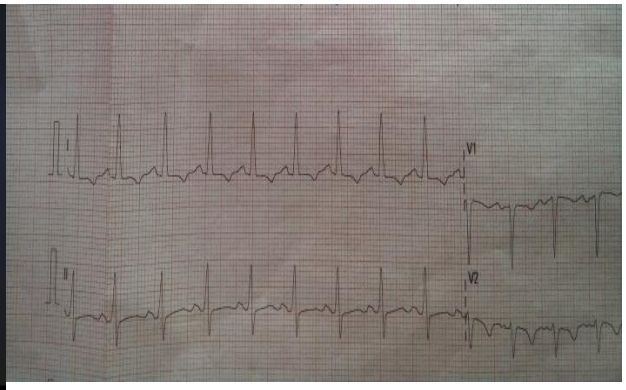
ECG 1 par notre méthode

ECG 1 par la méthode de l'ICA



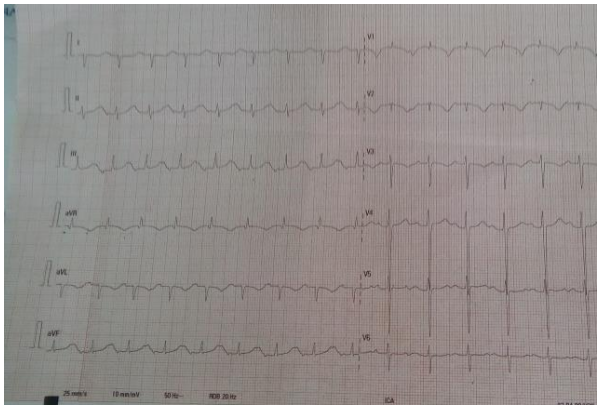
ECG 2 par notre méthode

ECG 2 par la méthode de l'ICA



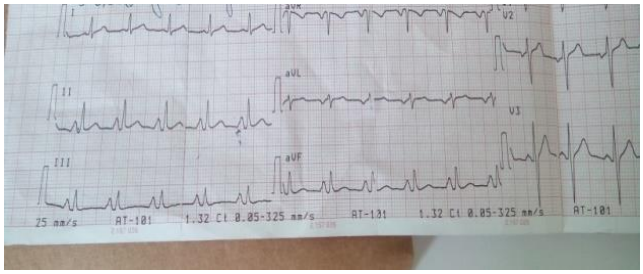
ECG 3 par notre méthode

ECG 3 par la méthode de l'ICA



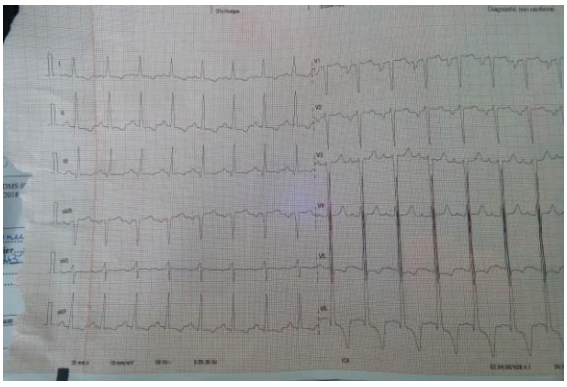
ECG 4 par notre méthode

ECG 4 par la méthode de l'ICA



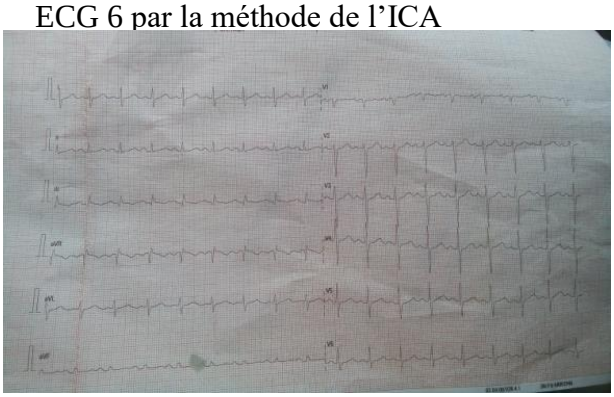
ECG 5 par notre méthode

ECG 5 par la méthode de l'ICA



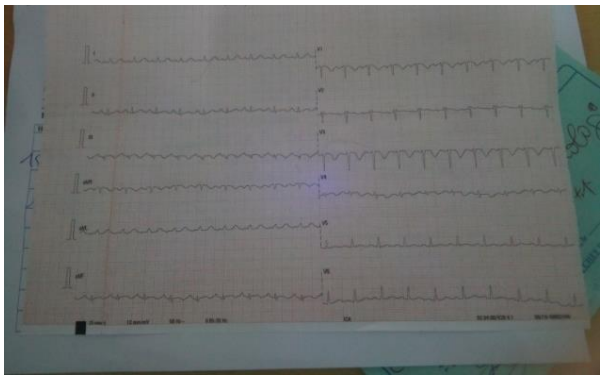
ECG 6 par notre méthode

ECG 6 par la méthode de l'ICA



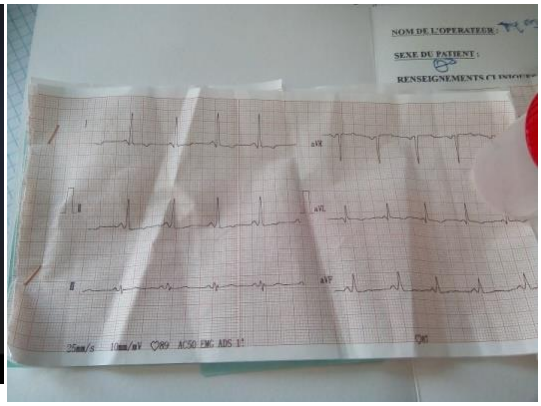
ECG 7 par notre méthode

ECG 7 par la méthode de l'ICA



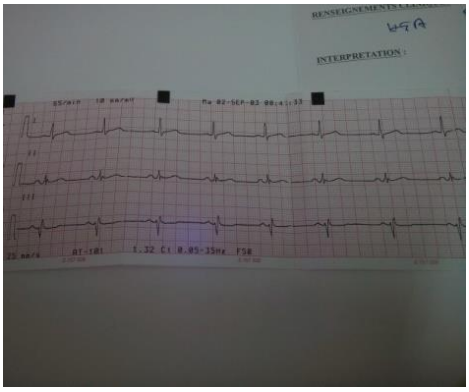
ECG 8 par notre méthode

ECG 8 par la méthode de l'ICA



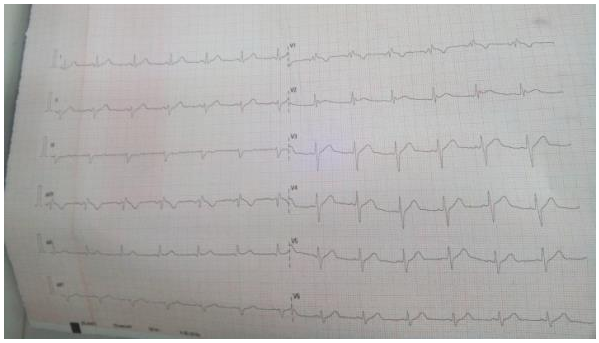
ECG 9 par notre méthode

ECG 9 par la méthode de l'ICA



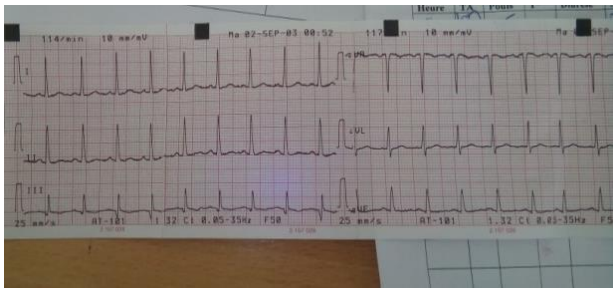
ECG 10 par notre méthode

ECG 10 par la méthode de l'ICA



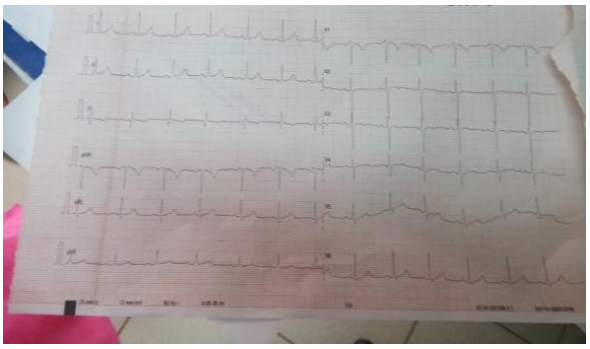
ECG 11 par notre méthode

ECG 11 par la méthode de l'ICA



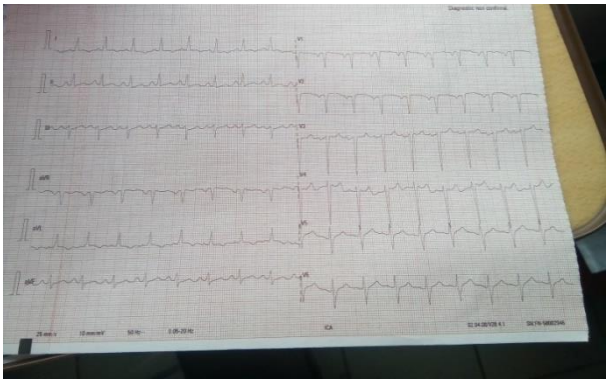
ECG 12 par notre méthode

ECG 12 par la méthode de l'ICA



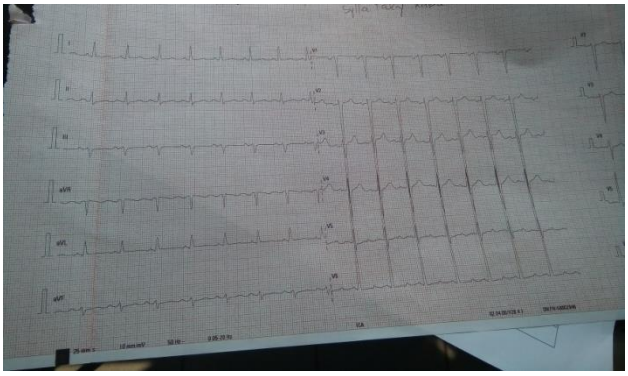
ECG 13 par notre méthode

ECG 13 par la méthode de l'ICA



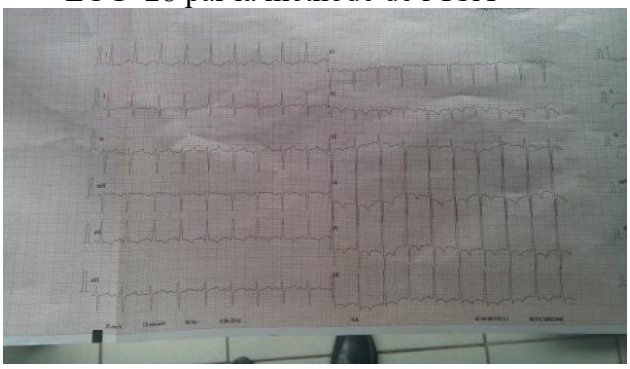
ECG 14 par notre méthode

ECG 14 par la méthode de l'ICA



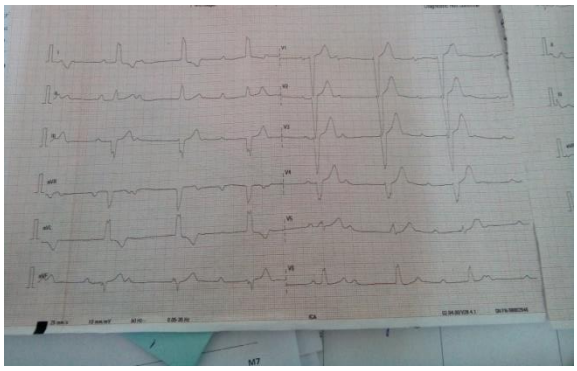
ECG 15 par notre méthode

ECG 28 par la méthode de l'ICA



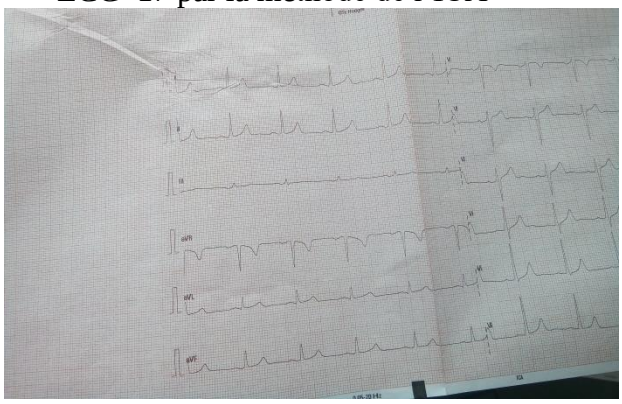
ECG 16 par notre méthode

ECG 16 par la méthode de l'ICA



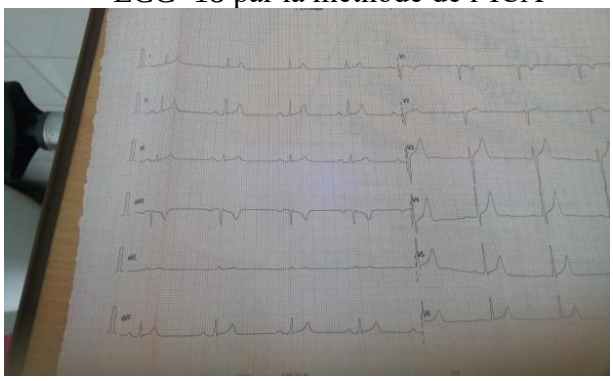
ECG 17 par notre méthode

ECG 17 par la méthode de l'ICA



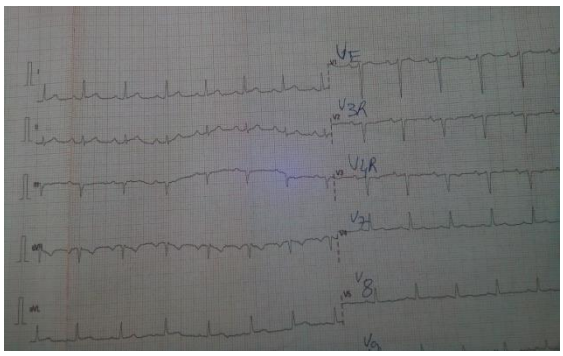
ECG 18 par notre méthode

ECG 18 par la méthode de l'ICA



ECG 19 par notre méthode

ECG 19 par la méthode de l'ICA



Publications scientifiques

1- Achi Harrisson Thiziers, **Jérémie T. Zoueu**, **Haba Cissé Théodore**, A Novel Medical Data Acquisition and Transmission Technique, *International Journal of Science and Research (IJSR)*, Volume 7 (7), (2018), 7p. DOI: 10.21275/ART2019190.

2- Achi Harrisson Thiziers, Haba Cisse Théodore, Jérémie T. Zoueu and Babri Michel, "Enhanced, Modified and Secured RSA Cryptosystem based on n Prime Numbers and Offline Storage for Medical Data Transmission via Mobile Phone" . *International Journal of Advanced Computer Science and Applications* (IJACSA), 10(10), 2019. http://dx.doi.org/10.14569/IJACSA.2019.0101050

3-Achi Harrisson Thiziers, Haba Cisse Théodore, Olivier K. Baguia, Jérémie T. Zoueu, Adoubi A. Kassi, Detection and Classification of High Blood Pressure by Artificial Neural Network at the Abidjan Cardiology Institute of Ivory Coast, *International Journal Of Hypertension (IJHY)*, (Soumis, en cours).