République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

MÉMOIRE DE MASTER RECHERCHE

En
Informatique

Option
Adminstration et Sécurité des Réseaux

Thème

Authentification des Dispositifs de santé 5G

Présenté par : M . DJAFOUR Oussama

Devant le jury composé de :

Président	**Dr. DJEBARI**	**Nabil**	**U. A/Mira**	**Béjaia.**
Rapporteurs	**Dr. SADI**	**Mustapha**	**U. A/Mira**	**Béjaia.**
Examinateurs	**Dr. CHEKRID**	**Mohamed**	**U. A/Mira**	**Béjaia.**

Promotion 2023/2024.

⁕ Remerciements ⁕

Au nom du dieu le clément et le miséricordieux louange à ALLAH le tout puissant.

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui ont contribué à la réalisation de ce mémoire.

Tout d'abord, je remercie chaleureusement mon encadreur SADI MUSTAPHA, pour ses conseils avisés, son soutien indéfectible et sa disponibilité tout au long de ce travail. Ses encouragements et ses précieuses suggestions ont grandement enrichi cette recherche.

Je souhaite également exprimer ma reconnaissance à l'ensemble des professeurs et des membres du jury, dont les enseignements et les remarques ont été d'une grande utilité pour la finalisation de ce mémoire.

Mes remerciements vont également à mes collègues et amis pour leurs encouragements, leur soutien moral et les échanges constructifs qui ont alimenté ma réflexion.

Je n'oublie pas de remercier ma famille, notamment mes parents , pour leur soutien constant et leur patience tout au long de cette aventure académique. Leur amour et leur compréhension m'ont été d'un grand réconfort.

Enfin, je remercie toutes les personnes qui, de près ou de loin, ont contribué à la réalisation de ce mémoire et à la réussite de mon parcours universitaire.

⁂ Dédicaces ⁂

Je dédie ce modeste travail en signe de respect, reconnaissance et de remerciement à :

Mes parents

Mes soeurs

Mes frères

Toute ma famille

Mes amis

Table des matières

Table des figures

Liste des abréviations

l'IOT Internet of Things (Internet des objets)

IoMT Internet of Medical Things

3G Troisième Génération Réseaux mobile

4G Quatrième Génération Réseaux mobile

5G Cinquième Génération Réseaux mobile

IA Intelligence Artificielle

IMTs International Mobile Telecommunications

WIoT Wireless Internet of Things

ECG Electrocardiogram

Wi-Fi Wireless Fidelity

M2M Machine to Machine

ML Machine Learning

DL Deep Learning)

TIC Technologies de l'Information et de la Communication

SDN Software-Defined Networking

NFV Network Function Virtualization

VNF Virtual Network Functions

D2D Device-to-Device

PIN Personal Identification Number (Numéro d'Identification Personnel)

EAP Extensible Authentication Protocol

AKA Authentication and Key Agreement

UMTS Universal Mobile Telecommunications System

LTE Long Term Evolution

NAI Network Access Identifier

DoS Déni de Service

DDoS Déni de Service Distribué

SQN Numéro de Séquence

UE Équipement Utilisateur

MiTM Man-in-the-Middle (Homme du Milieu)

IPS Intrusion Prevention System

TLS Transport Layer Security (Sécurité de la Couche de Transport)

VPN Virtual Private Network

MFA Authentification Multi-Facteur

mMTC massive Machine Type Communications

ngRAN Next Generation Radio Access Network

3GPP Projet de Partenariat de Troisième Génération

MNO Mobile Network Operator

SEAF Security Edge Protection Proxy

AUSF Authentication Server Function

ARPF Authentication and Routing Policy Function

UDM User Data Management

SUCI Subscription Concealed Identifier

SNN Stochastic Neural Network

UDM User Data Management

SUPI Subscription Permanent Identifier

SIDF Subscription Identifier De Conceal Function

RAND Random Number

AUTN Authentication Token

XRES Expected Response

CK' Cipher Key (Clé de Confidentialité Dérivée Concaténée)

IK' Integrity Key. (Clé d'Intégrité Dérivée)

USIM Universal Subscriber Identity Module

SIM Subscriber Identity Module

RES Response

MAC Message Authentication Code

KSEAF Key for Security Edge Protection Proxy

HN Home Network

AV Authentication Vector

SPAN Security Protocol ANimator

AVISPA Automated Validation of Internet Security Protocols and Applications

OFMC On-the-Fly Model Checking

CL-AtSe Constraint Logic-based Attack Searcher

SATMC SAT-based Model Checker

TA4SP Tree-Automata-based Protocol Analyzer

HLPSL High-Level Protocol Specification Language

CAS+ Community Adaptable Protocol Specification

TLA Temporal Logic of Actions

Introduction générale

La révolution numérique transforme de nombreux secteurs, et le domaine de la santé ne fait pas exception. L'émergence des réseaux de cinquième génération (5G) et de l'Internet des Objets (IoT) ouvre de nouvelles perspectives pour améliorer la qualité des soins, l'efficacité des services médicaux, et l'expérience des patients. Les technologies 5G et IoT permettent la connectivité en temps réel et la gestion des données à grande échelle, offrant ainsi des opportunités sans précédent pour les dispositifs médicaux connectés.

Cependant, cette interconnexion accrue et la dépendance aux technologies de l'information soulèvent des défis importants en matière de sécurité. Les dispositifs de santé 5G doivent non seulement être fiables et performants, mais aussi garantir la confidentialité et la protection des données médicales sensibles. L'authentification des dispositifs de santé devient ainsi une priorité cruciale pour prévenir les accès non autorisés et les cyberattaques potentielles.

Ce mémoire s'inscrit dans cette dynamique en explorant les mécanismes d'authentification adaptés aux dispositifs de santé connectés à des réseaux 5G. Notre objectif est de proposer des solutions robustes et sécurisées qui répondent aux exigences spécifiques du domaine médical. Nous aborderons les différentes caractéristiques des réseaux 5G et de l'IoT dans le contexte de la santé, les protocoles de sécurité existants, et les défis liés à leur mise en œuvre.

Le premier chapitre sera consacré à une vue d'ensemble des dispositifs de santé intelligents connectés au réseau 5G et à leur rôle dans la vie des patients.

Dans le deuxième chapitre, nous aborderons le protocole d'authentification EAP-AKA et son rôle dans la protection des dispositifs de santé intelligents.

Le troisième chapitre sera dédié à l'étude du fonctionnement de ce protocole dans le domaine de la santé intelligente.

Enfin, dans le dernier chapitre, nous mettrons en œuvre ce protocole EAP-AKA en utilisant l'outil Span Avispa basé sur le langage HLPSL.

Chapitre 1

Réseaux 5G et l'IoT dans la santé

1.1 Introduction

L'émergence des systèmes de santé intelligents a créé de nouvelles opportunités dans l'industrie médicale, notamment dans les domaines du diagnostic médical, de la prédiction, du traitement et de la prise de rendez-vous cliniques, incitant à une réévaluation des méthodes traditionnelles de soins de santé. La mise en œuvre de la télémédecine et des nouvelles technologies de santé numérique devrait réduire considérablement les consultations inutiles en personne et faciliter le diagnostic précoce des maladies. Les systèmes de santé axés sur la télémédecine permettent des services médicaux en temps réel et rentables, avantageant à la fois les patients et les médecins. L'Internet des objets médicaux IoMT améliore les activités quotidiennes et rend les services de santé plus abordables et conviviaux. L'IoMT et les technologies connexes sont devenus très prisés dans l'industrie de la santé, les technologies portables basées sur l'IoMT stimulant la transformation des systèmes de santé intelligents ces dernières années . De plus, la téléopération et les équipements télécommandés deviennent pratiques pour gérer les chirurgies à distance. Les plateformes de santé intelligentes peuvent rendre les procédures médicales plus efficaces, rentables et portables, augmentant ainsi l'accessibilité même dans les zones reculées .[7]

Ce chapitre prend en compte le paquet de soins de santé 5G qui comprend un aperçu complet de la Caractéristiques et avantages des réseaux 5G pour la santé connectée et Applications de l'IoT dans le domaine de la santé et architecture générale Réseaux 5G et l'IoT dans la santé avec les Défis liés à l'intégration des technologies 5G et IoT dans le système de santé.

1.2 Caractéristiques et avantages des réseaux 5G pour la santé connectée :

Les réseaux 5G offrent plusieurs caractéristiques et avantages pour la santé connectée [3] :

1.2.1 Surveillance à distance des patients

La 5G permet aux professionnels de santé de surveiller les patients à distance et en temps réel grâce à des dispositifs médicaux portables connectés, des chat bots et d'autres technologies, améliorant ainsi la personnalisation des soins et la prise de décisions rapides.

1.2.2 Télésanté et partage de données en temps réel

Les réseaux 5G favorisent l'utilisation accrue des services de télésanté en permettant des consultations à distance, le partage d'informations complémentaires en temps réel et la démocratisation des soins de santé, réduisant ainsi les coûts pour les établissements de santé et les patients.

1.2.3 Aide au diagnostic avec l'intelligence artificielle

L'intégration de l'intelligence artificielle (IA) dans le domaine de la santé connectée grâce à la 5G permet une analyse plus précise des données médicales en temps réel, offrant des diagnostics améliorés et une prestation de soins plus efficace et personnalisée

Ces éléments soulignent l'impact positif de la 5G sur la santé connectée en améliorant la surveillance des patients, en facilitant la télésanté et le partage de données, ainsi qu'en renforçant les capacités diagnostiques grâce à l'intelligence artificielle.

1.3 Architecture générale Réseaux 5G et l'IoT dans la santé :

Les dispositifs IoMT peuvent être classés en deux catégories principales : les Dispositifs Médicaux Implantés (IMTs) et les Objets Connectés Portables (WIoT). Les IMTs sont implantés dans le corps humain pour soutenir ou remplacer des organes biologiques, tels que les stimulateurs cardiaques et les stimulateurs cérébraux profonds. Ils sont conçus pour être petits et avoir une longue durée de vie de la batterie, des facteurs cruciaux pour les dispositifs destinés à être implantés à long terme. En revanche, les dispositifs WIoT, tels que les montres connectées et les moniteurs ECG, suivent les biométriques des individus dans leurs activités quotidiennes. Bien que les dispositifs WIoT offrent une commodité et une surveillance continue, ils peuvent manquer de précision et de durée de vie de la batterie nécessaires pour les conditions critiques par rapport aux IMTs.[7]

Dans le domaine des architectures IoT, l'architecture machine à machine (M2M) est la plus répandue et largement utilisée, l'IoMT étant une application importante dans le domaine de l'IoT médical. Les systèmes IoMT se composent généralement de quatre couches : la couche de capteur, la couche de liaison physique, la couche réseau et la couche de visualisation. La couche de capteur collecte les données biométriques des IMTs ou des dispositifs WIoT, qui

sont ensuite transmises à un hôte passerelle pour le prétraitement et les analyses de base. Ensuite, les données traitées sont envoyées à la couche réseau pour le stockage, l'analyse et l'accès sécurisé. Enfin, la couche de visualisation permet aux professionnels de la santé d'analyser les données et aux patients de visualiser leur état de santé, améliorant ainsi la communication et la prise de décision dans la prestation des soins de santé.[7]

En exploitant les technologies IoMT, les prestataires de soins de santé peuvent améliorer les résultats des patients, réduire les admissions à l'hôpital et renforcer l'efficacité de la prestation des soins de santé. Cependant, des défis tels que la confidentialité des données, l'interopérabilité et l'interprétation efficace des données doivent être relevés pour réaliser pleinement le potentiel de l'IoMT dans la transformation de la prestation des soins de santé.

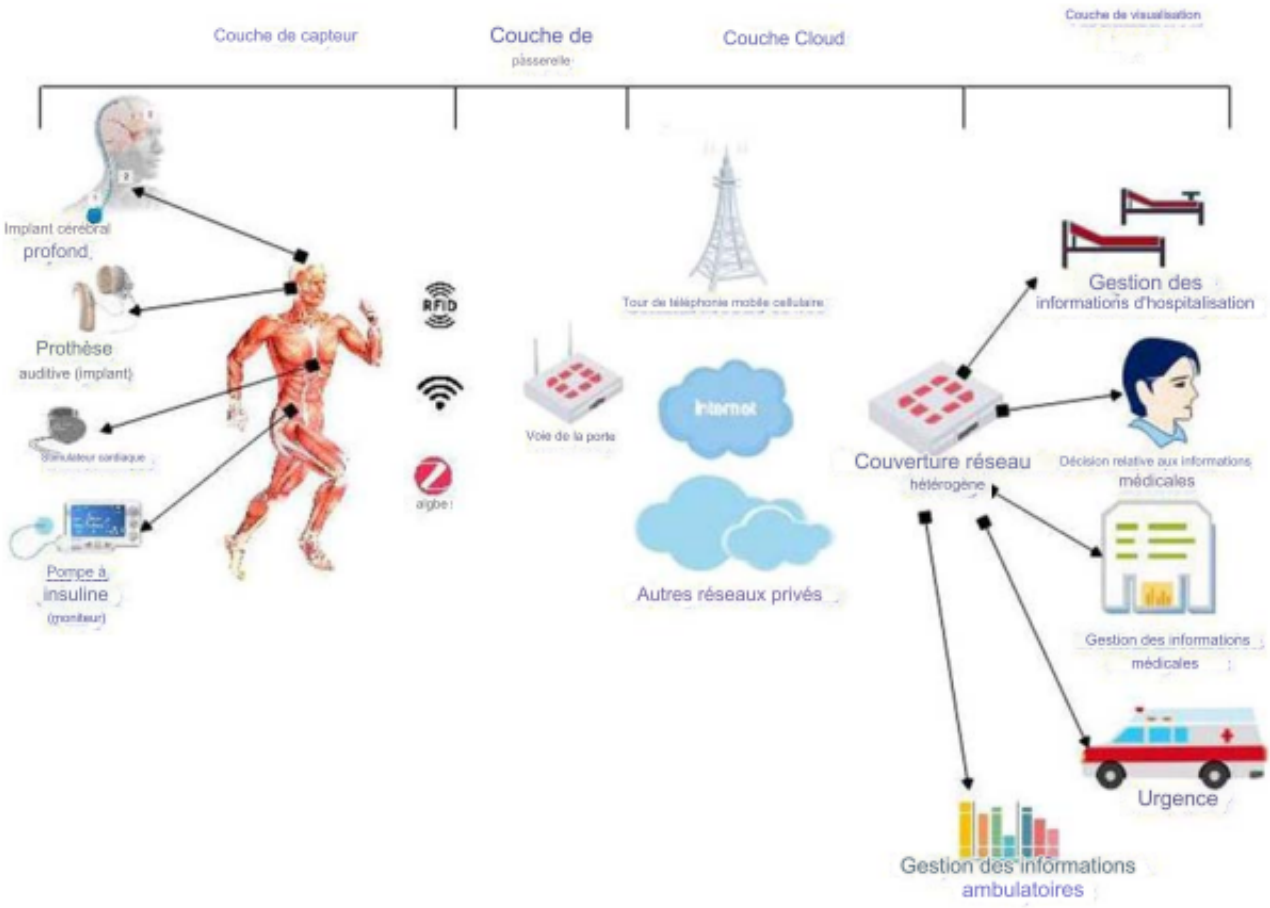

FIGURE 1.1 – Architecture générale Réseaux 5G et l'IoT dans la santé [7]

Cette Figure exposé le architecture générale Réseaux 5G et l'IoT dans la santé [7] :

1.3.1 Couche des capteurs

Cette couche comprend des dispositifs portables et des capteurs implantables qui collectent les données de santé du patient. Les données biométriques sont transmises à la couche suivante via des technologies sans fil à courte portée comme Wi-Fi, ZigBee, et Bluetooth.

1.3.2 Couche de passerelle

En raison de la petite taille des IoMT, le traitement et le stockage des données ne sont pas possibles sur cette couche. Les données brutes sont envoyées à des dispositifs plus puissants comme les smartphones ou les montres intelligentes du patient, qui servent de nœuds périphériques. Ces dispositifs effectuent un prétraitement léger et transmettent les données au cloud pour un traitement intensif.

1.3.3 Couche réseau

Cette couche assure le stockage sophistiqué des données, l'analyse des big data et l'accès sécurisé. Des techniques avancées de ML et DL sont utilisées pour analyser les données des capteurs IoMT. Cependant, des problèmes de bande passante peuvent entraîner des retards, ce qui est critique en surveillance médicale. Des solutions comme l'informatique de périphérie et la blockchain sont proposées pour améliorer la sécurité et l'efficacité du traitement des données.

1.3.4 Couche de visualisation

Aussi appelée couche d'application, c'est là que les données sont accessibles par les médecins et les patients pour suivre la santé. Les médecins peuvent faire des recommandations et prescrire des actions à entreprendre par les patients en fonction de leurs conditions de santé, comme des prescriptions de médicaments ou des références à d'autres spécialistes.

1.4 Applications de l'IoT dans le domaine de la santé :

Les frais considérables liés aux soins de santé ainsi que la gestion de données massives lors des crises sanitaires nécessitent des avancées technologiques permettant un accès aux services de santé à tout moment et en tout lieu. Les progrès technologiques ont facilité l'émergence de la télémédecine, qui propose des services de santé en ligne pour les patients incapables de se déplacer, ainsi que pour les zones rurales et les régions éloignées qui manquent d'accès aux soins médicaux. Les applications de la télémédecine incluent la transmission et le stockage d'images médicales, les consultations en ligne avec les patients, la formation continue et les outils de santé électronique. Cependant, l'adoption de la télémédecine est freinée par des obstacles techniques et financiers.[3]

À cet égard, des études ont mis en avant le potentiel de l'informatique en nuage, qui offre une capacité de soutien à distance, des ressources transparentes et accessibles, une connectivité Internet efficace à grande échelle, ainsi que des solutions robustes pour le partage et le traitement des données médicales, y compris les dossiers des patients contenant des volumes importants d'informations. Les innovations numériques en santé ont révolutionné les programmes de soins en améliorant leur qualité tout en réduisant les coûts, grâce à des outils tels que les dossiers médicaux automatisés, les dispositifs médicaux portables et d'autres technologies novatrices.

Les gouvernements et les responsables de la santé s'efforcent constamment d'adopter et de mettre en œuvre les technologies de l'information et de la communication (TIC) dans les programmes de santé, remodelant ainsi les interactions entre les patients et les structures de santé. Cette transition vers les soins de santé numériques, également appelée cyber santé, représente une évolution systémique des soins de santé conventionnels, intégrant divers dispositifs tels que les dossiers médicaux électroniques, les systèmes de surveillance en ligne, les services de santé mobiles, l'analyse de données et d'autres innovations transformatrices.[7]

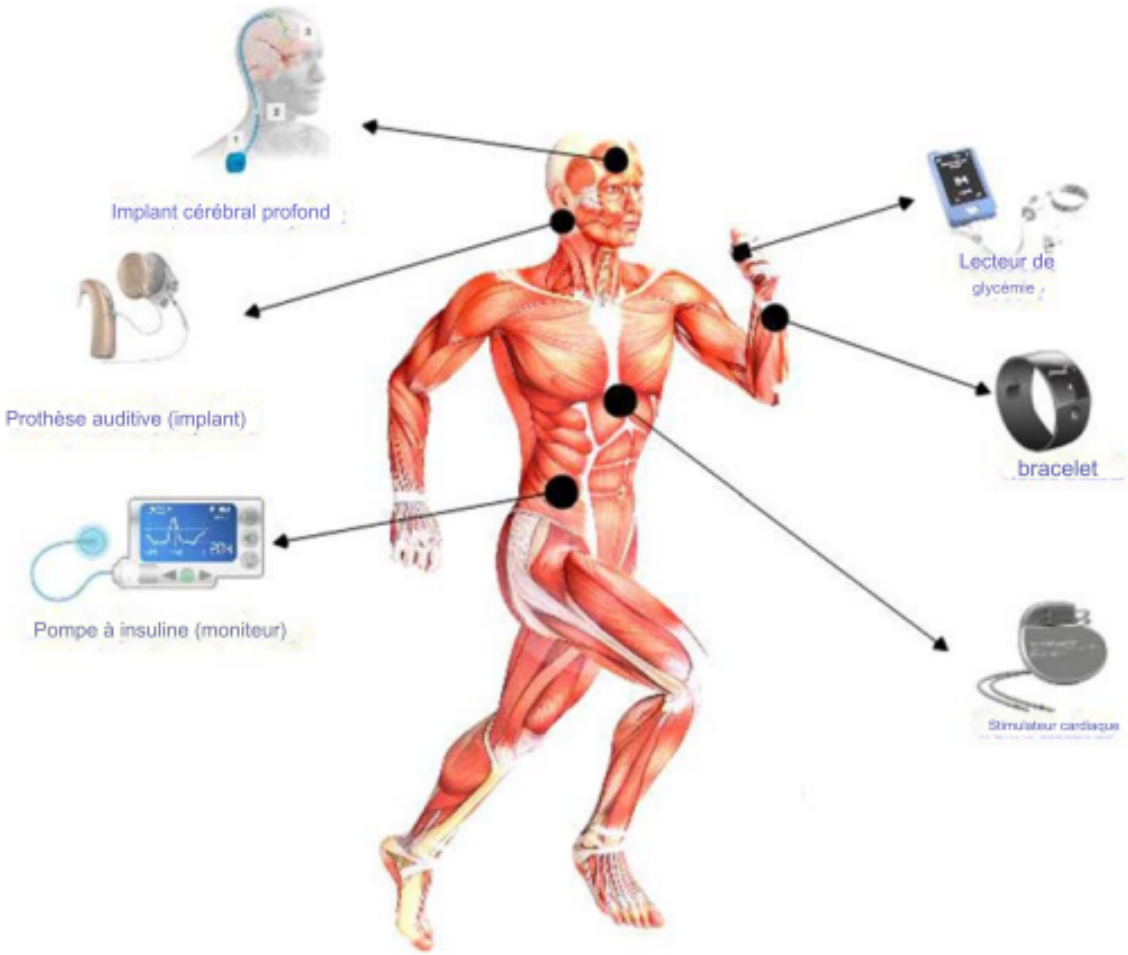

FIGURE 1.2 – Dispositifs de soins de santé intelligents dans le corps humain [7]

Cette Figure montre une gamme des appareils de soins de santé intelligents les plus importants.

Ce sont les utilisations et les applications l'IOT les plus importantes dans le domaine médical [5] :

1.4.1 Détection de glucose

grâce à des capteurs et des outils médicaux portables. Il est devenu possible de mesurer le glucose dans le sang humain, de réguler l'alimentation, l'activité physique et le temps de médication, tout cela à distance, grâce au réseau 5G qui prend en charge les applications de soins de santé intelligents.

1.4.2 Supervision ECG

Grâce aux appareils intelligents connectés au corps humain, en particulier pour les patients cardiaques, la supervision peut être suivie. L'électrocardiographie est l'examen des dossiers d'activité électrique liés au cœur humain, intègre l'approximation directe des impulsions et la concentration biologique avec l'identification des arythmies complexes, des périodes QT tardives et du muscle cardiaque ischémique.

1.4.3 Surveillance de la pression artérielle

Nous pouvons surveiller la pression artérielle, le signal cardiaque et la pression en utilisant des capteurs tels que des capteurs de pression, le pouls électronique et le résultat peut être partagé numériquement et accessible par le médecin spécialiste, grâce aux Internets of Things des réseaux 5G.

1.4.4 Surveillance de la température corporelle

La surveillance du vélo thermique du corps est l'une des parties les plus importantes des soins de santé intelligents et en mesurant la température du corps peut mesurer la stabilité du corps du patient. Permettre l'idée de m-IoT, en utilisant un capteur qui surveille la température corporelle, est implanté dans TelosB, et le contrôle de la traction du moulin pour les lectures de température effectuées à partir du corps est la fonction utile du système m-IoT généré.

1.4.5 Vérification de la saturation en oxygène

La vérification de la saturation en oxygène par l'oxymétrie des battements de cœur est une méthode appropriée pour surveiller de manière non invasive la saturation en oxygène dans le sang. La convergence entre l'oxymétrie cardiaque et l'Internet des objets (IOT) revêt

une importance cruciale pour les soins de santé intelligents axés sur l'adaptation. Un examen de la validation des soins de santé de l'oxymétrie du rythme cardiaque basée sur l'IoT a été effectué. Nonin a présenté l'Ox2, un oxymètre portable au poignet, démontrant sa capacité à mesurer le rythme cardiaque. Cet appareil utilise des capteurs connectés directement à la plateforme Monere et s'appuie sur les profils de dispositifs de santé Bluetooth.

1.4.6 Système de réadaptation

Le système de réadaptation vise à améliorer la capacité fonctionnelle et la satisfaction personnelle des individus souffrant de faiblesse physique ou de handicap. L'IoT peut contribuer à ce système en facilitant le stockage et l'accès à des données médicales expertes. Une stratégie d'automatisation basée sur l'ontologie est proposée pour ce système de réadaptation dans le domaine des soins de santé intelligents. Cette approche illustre efficacement comment l'IoT peut être utilisé pour connecter différents composants essentiels, garantissant ainsi une communication constante et des avantages accrus pour les utilisateurs.

1.5 Défis liés à l'intégration des technologies 5G et IoT dans le système de santé

La 5G offre des caractéristiques capables de répondre aux exigences de l'IoT de demain, mais elle soulève également de nouveaux défis de recherche intéressants concernant l'architecture de la 5G-IoT, les communications de confiance entre les appareils, les problèmes de sécurité, etc. La 5G-IoT intègre plusieurs technologies et exerce un impact significatif sur les applications dans le domaine de l'IoT. Dans cette section, nous passerons en revue les défis potentiels de recherche ainsi que les tendances futures dans le domaine de la 5G-IoT [2] :

1.5.1 défis techniques :

Les défis techniques liés à la mise en œuvre de réseaux 5G-IoT dans le domaine de la santé sont nombreux :

- **Architecture**

Concevoir une architecture évolutive pour les réseaux 5G-IoT dans le domaine de la santé présente des défis, notamment en ce qui concerne la gestion de réseau, l'interopérabilité et la sécurité. [5]

- **Réseau défini par logiciel sans fil (SDN)**

Bien que prometteur pour sa scalabilité, le SDN sans fil rencontre encore des lacunes dans la gestion efficace du cœur de réseau et dans la séparation des plans de contrôle et de données. [5]

- **Virtualisation des fonctions réseau (NFV)**

La NFV, bien que complémentaire au SDN, présente ses propres défis tels que l'efficacité énergétique de la cloudification, les problèmes de sécurité et de confidentialité, ainsi que la gestion efficace des fonctions réseau virtuelles (VNF). [5]

- **Communication de Device-to-Device (D2D)**

Assurer un débit élevé dans la communication D2D nécessite de relever des défis liés à l'efficacité énergétique et spectrale, ainsi qu'à la gestion des ressources et des interférences. [5]

- **Déploiement des applications IoT en santé**

Le déploiement à grande échelle des applications IoT en santé est complexe en raison des limitations de ressources, des environnements hétérogènes et de la nécessité d'une collecte et d'une diffusion efficaces des données. Des solutions proposées incluent des plates-formes de provision de services multi-niveaux. [5]

- **Autres défis**

Parmi les autres défis figurent le déploiement de réseaux hétérogènes denses en santé, le développement de techniques d'accès multiples pour les réseaux 5G et au-delà, ainsi que la possibilité de transmission en duplex intégral. [5]

S'attaquer à ces défis sera crucial pour la mise en œuvre et le déploiement réussis des réseaux 5G-IoT dans le domaine de la santé, garantissant leur scalabilité, leur sécurité et leur efficacité.

1.5.2 Assurance de la sécurité et protection des renseignements personnels :

Dans le paysage évolutif des soins de santé, la sécurité et la confidentialité sont des considérations cruciales alors que nous nous tournons vers l'adoption des systèmes avancés 5G-IoT. Ces systèmes, essentiels dans des applications telles que les villes intelligentes et les réseaux, exigent des mesures de sécurité robustes tant au niveau des appareils que des réseaux. Compte tenu de la diversité du 5G-IoT, les complexités de sécurité sont amplifiées, obligeant les concepteurs à faire face non seulement aux intrusions logicielles à distance, mais aussi aux atteintes locales directement au niveau de l'appareil. Pour naviguer efficacement dans ces défis, l'assurance de sécurité doit prioriser l'élimination des vulnérabilités dans tout le système. Les principaux domaines nécessitant une attention particulière incluent [5] :

- **Identité**

Établir des identités fiables et vérifiables pour les appareils et les utilisateurs au sein du réseau.

- **Authentification**

Veiller à ce que l'accès aux données sensibles et aux services soit accordé uniquement aux appareils et utilisateurs autorisés. Assurance Instiller la confiance dans l'efficacité des mesures de sécurité mises en œuvre dans l'ensemble du système.

- **Gestion des clés**

Protéger la génération, la distribution et le stockage des clés cryptographiques pour empêcher l'accès non autorisé.

- **Algorithmes cryptographiques**

Utiliser des techniques de chiffrement robustes pour protéger l'intégrité des données lors de la transmission et du stockage.

- **Mobilité**

Gérer efficacement les protocoles de sécurité dans des environnements dynamiques où les appareils peuvent passer d'un réseau à un autre.

- **Stockage**

Protéger les données stockées sur les appareils ou dans le cloud contre l'accès ou la manipulation non autorisés.

- **Compatibilité descendante**

Assurer une intégration fluide avec les systèmes hérités tout en respectant des normes de sécurité strictes.

- **Assurance**

Valider en continu l'efficacité des mesures de sécurité pour maintenir un niveau élevé de protection.

En abordant de manière exhaustive ces considérations de sécurité, les parties prenantes peuvent atténuer efficacement les risques et protéger la confidentialité, l'intégrité et la disponibilité des données et des services de santé au sein des écosystèmes 5G-IoT.

1.6 Conclusion :

l'intégration des dispositifs IoT dans le domaine de la santé avec la technologie 5G représente une avancée majeure pour l'amélioration des soins de santé. Grâce à la connectivité ultra-rapide, à la faible latence et à la capacité de gérer un grand nombre d'appareils simultanément, la 5G ouvre des possibilités sans précédent pour la surveillance médicale à distance, le suivi des patients, la gestion des maladies chroniques et la fourniture de soins de santé personnalisés. Les tendances de recherche émergentes, telles que l'informatique périphérique, la convergence de la 5G avec l'IA et l'analyse des données, ainsi que l'efficacité énergétique et spectrale, promettent de transformer encore davantage le paysage des soins de santé connectés.

Ce pendant, il est crucial de relever les défis liés à la sécurité, à la confidentialité et à l'interopérabilité pour garantir que ces avancées bénéficient réellement aux patients et aux professionnels de la santé. Une collaboration continue entre les chercheurs, les entreprises, les régulateurs et les prestataires de soins de santé est essentielle pour maximiser le potentiel des dispositifs L'IoT alimentés par la 5G et révolutionner la prestation des soins de santé, améliorant ainsi la qualité de vie des individus à travers le monde.

Pour protéger les utilisateurs et leurs données très sensibles, des mécanismes d'authentification intelligents ont été développés. Nous examinerons ces mécanismes en détail dans le chapitre 2 de cette recherche.

Chapitre 2

Authentification pour les dispositifs de santé 5G

2.1 Introduction

Dans le domaine de la santé connectée sur les réseaux 5G, l'authentification est cruciale pour sécuriser les données médicales échangées. Ce chapitre examine les bases de l'authentification pour les dispositifs de santé 5G, en présentant diverses approches, menaces potentielles, et protocoles de sécurité. La connectivité accrue des technologies de santé expose les dispositifs et les données à de nouveaux risques de sécurité. Les méthodes traditionnelles comme les mots de passe et les codes PIN sont insuffisantes face à ces menaces. L'authentification intelligente, utilisant des techniques avancées telles que la biométrie et l'intelligence artificielle, offre une solution prometteuse. Le chapitre détaille ces approches, analyse les menaces potentielles, et discute du protocole de sécurité EAP-AKA pour l'authentification des dispositifs de santé 5G, fournissant une vue d'ensemble complète pour comprendre et implémenter des solutions de sécurité robustes dans le domaine en constante évolution de la santé connectée.

2.2 Protocole EAP-AKA' dans les réseaux 5G :

L'authentification dans les réseaux 5G est une composante vitale de la sécurité des Communications mobiles. Le protocole EAP-AKA' (Extensible Authentication Protocol - AKA Prime) émerge comme une solution fondamentale pour garantir la confidentialité et la sécurité des données dans cet environnement hautement dynamique. Avec l'avènement des réseaux mobiles de cinquième génération (5G), l'utilisation de ce protocole dans les dispositifs de santé 5G devient également important pour assurer la confidentialité et la sécurité des données médicales sensibles. Ce chapitre explore en détail le fonctionnement, les caractéristiques, les avantages et les inconvénients du protocole EAP-AKA' dans le contexte des réseaux 5G, en mettant particulièrement l'accent sur son utilisation dans les dispositifs de santé 5G.[22]

2.3 Contexte et Origine :

Le protocole EAP-AKA' trouve ses racines dans le contexte de l'évolution des réseaux mobiles, en particulier avec le passage à la technologie 5G. Pour comprendre son importance, il est nécessaire de revenir sur les précédentes générations de réseaux mobiles [1]

2.3.1 Réseaux 3G (UMTS)

Les premiers réseaux mobiles de troisième génération ont introduit des fonctionnalités telles que la transmission de données à haut débit et la connectivité Internet mobile. Cependant, la sécurité des communications était encore relativement limitée, avec des protocoles d'authentification moins sophistiqués.

2.3.2 Réseaux 4G (LTE)

Avec l'avènement des réseaux 4G, tels que la LTE, la sécurité des communications a été renforcée par l'introduction de l'algorithme d'authentification et d'accord de clé (AKA). Cet algorithme a permis d'établir des clés de session sécurisées entre les utilisateurs et les réseaux, renforçant ainsi la confidentialité et l'intégrité des échanges.

2.4 Besoins Croissants de Sécurité :

Avec la transition vers les réseaux 5G, les besoins en matière de sécurité et de confidentialité ont considérablement augmenté. Les réseaux 5G visent à offrir des capacités révolutionnaires telles que des débits ultra-rapides, une latence ultra-faible et une connectivité massive des appareils IoT (Internet des objets). Cependant, cette évolution technologique s'accompagne de nouveaux défis en matière de sécurité, notamment en raison de la multiplication des points d'accès et de la complexité croissante des réseaux.

2.5 Développement d'EAP-AKA' :

Face à ces défis, le protocole EAP-AKA' a été développé comme une extension du protocole EAP, spécifiquement conçue pour répondre aux besoins d'authentification des abonnés dans les réseaux 5G. Basé sur l'algorithme AKA utilisé dans les réseaux 3G et 4G, EAP-AKA' intègre des améliorations significatives pour renforcer la sécurité et la confidentialité des échanges. Ces améliorations sont essentielles pour garantir la confiance des utilisateurs dans les nouveaux services et applications offerts par les réseaux 5G.[10]

2.6 Objectifs d'EAP-AKA' :

Le développement d'EAP-AKA' répond à plusieurs objectifs clés [10] :

- ▷ Renforcer la confidentialité et l'intégrité des communications dans les réseaux 5G.
- ▷ Assurer l'authentification sécurisée des abonnés mobiles dans un environnement hautement dynamique et connecté.
- ▷ Fournir une solution d'authentification interopérable et efficace, compatible avec les infrastructures existantes des réseaux mobiles.[12]

2.7 Caractéristiques Clés du Fonctionnement :

2.7.1 Mutualité de l'Authentification

L'authentification est mutuelle entre l'utilisateur et le réseau, renforçant ainsi la confiance des deux côtés.

2.7.2 Utilisation de Clés Temporaires

Le protocole utilise des clés temporaires et des identités temporaires pour protéger les informations sensibles des utilisateurs pendant l'authentification.

2.7.3 Échange Sécurisé de Messages

Les échanges de messages entre l'utilisateur et le réseau sont sécurisés à l'aide de mécanismes cryptographiques pour garantir l'intégrité et la confidentialité des données.

2.8 Caractéristiques Principales d'EAP-AKA' :

Voici les caractéristiques principales d'EAP-AKA'[22] :

2.8.1 Confidentialité Renforcée :

- **Utilisation d'Identités Temporaires :** EAP-AKA' protège les identités permanentes des utilisateurs en utilisant des identités temporaires lors des échanges d'authentification.
- **Protection des Informations Sensibles :** Les informations sensibles, telles que les clés et les identifiants, sont protégées par des mécanismes cryptographiques tout au long du processus d'authentification.

2.8.2 Sécurité Accrue :

- **Mécanismes de Dérivation de Clé :** EAP-AKA' utilise des mécanismes de dérivation de clé pour générer des clés de session uniques lors de l'établissement de la connexion, renforçant ainsi la sécurité des échanges.

- **Résistance aux Attaques :** Conçu pour résister à différents types d'attaques, EAP-AKA' intègre des mécanismes de sécurité pour détecter et prévenir les attaques telles que les attaques par rejeu et par homme du milieu.

2.8.3 Interopérabilité :

- **Compatibilité avec Divers Dispositifs et Réseaux :** EAP-AKA' est conçu pour être interopérable avec une variété de dispositifs et de réseaux, favorisant ainsi son adoption et son intégration dans les infrastructures existantes des réseaux 5G.

- **Standardisation :** Conforme aux normes établies par les organismes de normalisation, EAP-AKA' facilite son déploiement et son utilisation dans différents environnements réseau, favorisant l'interopérabilité entre les fournisseurs et les opérateurs de services.

2.9 Avantages et Inconvénients d'EAP-AKA' :

Les avantages et l'inconvenients de protocole de authentification EAP-AKA'[12] :

2.9.1 Avantages :

Les avantages de protocole de authentification EAP-AKA' :

- **Sécurité Renforcée :** Protection contre les attaques sophistiquées, garantissant l'intégrité et la confidentialité des échanges.

- **Confidentialité des Abonnés :** Prise en charge de l'anonymisation de l'identité des utilisateurs pour protéger leurs informations personnelles.

- **Efficacité Opérationnelle :** Protocole léger et efficace adapté aux déploiements à grande échelle, assurant des performances optimales.

- **Compatibilité :** Interopérabilité avec les réseaux 3G et 4G pour une transition en douceur vers les réseaux 5G.

2.9.2 Inconvénients :

l'inconvenients de protocole de authentification EAP-AKA' :

- **Complexité :** La mise en œuvre peut être complexe, nécessitant une configuration et une gestion avancées.
- **Déploiement :** Nécessite une mise à jour des infrastructures existantes, ce qui peut prendre du temps et des ressources.
- **Normalisation :** En cours de standardisation, ce qui peut poser des problèmes d'interopérabilitéentre les fournisseurs.

2.10 Déploiement dans dispositifs de santé 5G :

Le déploiement du protocole EAP-AKA' dans les dispositifs de santé 5G revêt une importance particulière compte tenu des exigences de sécurité et de confidentialité associées aux données médicales sensibles. Voici une analyse détaillée de son déploiement dans ce contexte [23] :

2.10.1 Confidentialité et Sécurité des Données Médicales :

- **Protection des Données Sensibles :** EAP-AKA' offre un niveau élevé de sécurité pour les échanges d'authentification entre les dispositifs de santé et les réseaux 5G. Cela garantit que les données médicales sensibles sont protégées contre les accès non autorisés et les cyberattaques potentielles.
- **Anonymisation de l'Identité des Patients :** L'anonymisation de l'identité des patients, réalisée grâce à la prise en charge de l'identifiant d'accès au réseau (NAI), assure la confidentialité des informations personnelles des patients, conformément aux réglementations sur la protection des données médicales.[15]

2.10.2 Intégration avec les Dispositifs Médicaux Connectés :

▷ EAP-AKA' peut être intégré de manière transparente aux protocoles de communication des dispositifs médicaux connectés, garantissant une authentification sécurisée lors de l'accès aux réseaux 5G. Cela permet une utilisation sûre et efficace des données médicales dans un environnement connecté.

▷ Interopérabilité avec les Infrastructures de Santé Existantes : Le protocole EAP-AKA' est conçu pour être compatible avec les infrastructures de santé existantes, facilitant ainsi son déploiement dans les établissements de santé et les réseaux médicaux. Cette interopérabilité garantit une transition en douceur vers les nouvelles technologies 5G.

2.10.3 Gestion des Autorisations d'Accès :

- **Contrôle Centralisé des Autorisations :** Le déploiement d'EAP-AKA' permet un contrôle centralisé des autorisations d'accès aux données médicales, ce qui permet aux administrateurs de gérer efficacement les niveaux d'accès des utilisateurs et des dispositifs aux informations médicales sensibles.

- **Suivi des Activités d'Accès :** Le protocole offre des fonctionnalités de suivi des activités d'accès, permettant aux responsables de la sécurité de surveiller et d'auditer les interactions entre les dispositifs de santé et les réseaux 5G. Cela renforce la conformité aux normes de sécurité et de confidentialité des données médicales.

2.10.4 Formation et Sensibilisation :

- **Formation des Utilisateurs et des Personnels de Santé :** Un déploiement réussi d'EAP-AKA' nécessite une formation adéquate des utilisateurs et du personnel de santé sur les meilleures pratiques en matière de sécurité et d'utilisation des dispositifs médicaux connectés. Cela garantit une utilisation sécurisée et efficace des technologies 5G dans le domaine de la santé.

- **Sensibilisation à la Sécurité des Données Médicales :** Une sensibilisation continue à la sécurité des données médicales est essentielle pour garantir que tous les acteurs impliqués comprennent les risques potentiels et les mesures de sécurité nécessaires pour protéger les informations médicales sensibles.

2.11 Analyse de sécurité :

L'analyse de sécurité du protocole EAP-AKA' dans le contexte des réseaux 5G, en particulier pour les dispositifs de santé, est essentielle pour évaluer sa robustesse et son efficacité dans la protection des données médicales sensibles. Voici une analyse détaillée de la sécurité du protocole [22] [10] [12]

2.11.1 Points Forts :

- **Authentification Mutuelle :** Le protocole assure une authentification mutuelle entre les dispositifs de santé et les réseaux 5G, établissant ainsi un niveau de confiance entre les parties et réduisant les risques d'accès non autorisés.

- **Confidentialité des Données Sensibles :** Les mécanismes de chiffrement et de protection des données garantissent la confidentialité des informations médicales échangées, préservant ainsi la vie privée des patients et la sécurité des données sensibles.

- **Résistance aux Attaques Connues :** Le protocole est conçu pour résister à plusieurs types d'attaques, y compris les attaques par rejeu, les attaques par l'homme du milieu et les attaques par surveillance, assurant ainsi l'intégrité et l'authenticité des communications.

- **Gestion des Clés Sécurisée :** Les mécanismes de gestion des clés intégrés garantissent la sécurité des clés de session utilisées pour le chiffrement et l'authentification, empêchant ainsi les attaques basées sur la compromission des clés.

2.11.2 Vulnérabilités Potentielles :

- **Gestion des Clés Faible :** Certaines conditions pourraient compromettre la sécurité des clés, notamment en cas de découverte des clés utilisées dans les sessions précédentes. Une gestion insuffisante des clés pourrait rendre le système vulnérable aux attaques de récupération de clés.

- **Accords Faibles :** Dans certaines situations, les accords entre les entités ne sont pasgarantis, ce qui pourrait affecter la fiabilité du protocole et ouvrir la voie à des attaques telles que la désynchronisation ou la falsification des messages.

2.11.3 Mesures d'Atténuation :

- **Renforcement de la Gestion des Clés :** Une attention particulière doit être accordée à la gestion des clés pour prévenir les attaques basées sur la compromission des clés. Cela peut inclure l'utilisation de techniques de rotation des clés et de stockage sécurisé des clés.

- **Amélioration des Mécanismes de Surveillance :** Des mécanismes de surveillance robustes doivent être mis en place pour détecter et répondre aux activités suspectes, y compris les tentatives d'authentification non autorisées ou les anomalies dans les échanges de données.

- **Mises à Jour Régulières :** Il est crucial de maintenir le protocole à jour en appliquant les correctifs de sécurité et les mises à jour logicielles pour remédier aux vulnérabilités découvertes et améliorer la résilience du système face aux nouvelles menaces.[17]

2.12 Menaces et attaques potentielles :

L'essor de la technologie 5G a ouvert de nouvelles perspectives dans le domaine des soins de santé,facilitant l'émergence de services innovants tels que la télémédecine, la télésanté et la surveillance médicale à distance. Cependant, cette évolution s'accompagne également d'un

élargissement significatif de la surface d'attaque pour les cybercriminels. Non seulement les dispositifs de santé 5G sont devenus des cibles potentielles, mais également les services associés à ces dispositifs, tels que les plateformes de gestion des données médicales et les systèmes de prise de rendez-vous. Cette expansion de la surface d'attaque crée de nouvelles vulnérabilités et expose les dispositifs de santé 5G à un éventail croissant de menaces potentielles. Les risques vont de l'interception des données médicales confidentielles à la compromission des dispositifs eux-mêmes, en passant par les attaques visant à perturber les communications vitales entre les patients et les professionnels de la santé.[21]

La complexité croissante de la chaîne logistique dans le secteur de la santé ajoute une couche supplémentaire de défis en matière de sécurité. Les dispositifs médicaux connectés doivent interagir avec une multitude d'acteurs, tels que les fournisseurs de services, les assureurs, les organismes de réglementation et les prestataires de soins de santé, ce qui élargit le périmètre d'attaque et accroît la difficulté de garantir une protection adéquate contre les menaces. De plus, la nature critique des données de santé et des opérations médicales rend les dispositifs desanté 5G particulièrement attrayants pour les cybercriminels, qui cherchent à exploiter ces informations à des fins malveillantes telles que le vol d'identité, le chantage et la fraude financière.

Face à ces défis, il devient impératif de mettre en place des mécanismes d'authentification intelligente robustes pour protéger les dispositifs de santé 5G contre les menaces émergentes. En comprenant les risques potentiels et en adoptant des contre-mesures de sécurité appropriées, nous pouvons garantir l'intégrité, la confidentialité et la disponibilité des données médicales dans un environnement de santé connecté en évolution constante.[21]

2.12.1 Types d'attaques :

2.12.1.1 Attaques par déni de service (DoS) et déni de service distribué (DDoS)

Les attaques par déni de service (DoS) et déni de service distribué (DDoS) sont des techniques visant à rendre un service indisponible en saturant les ressources du réseau ou des serveurs avec un flux massif de trafic. Les attaquants utilisent souvent des botnets, des réseaux d'ordinateurs compromis, pour coordonner des attaques DDoS à grande échelle. Par exemple, une attaque DDoS pourrait cibler un serveur de gestion des dispositifs médicaux, perturbant ainsi les communications et les services de santé en ligne, mettant potentiellement en danger la vie des patients. Ces attaques représentent une menace majeure pour les dispositifs de santé 5G, car elles peuvent entraîner une perturbation des services vitaux de santé, tels que la surveillance à distance des patients ou les consultations médicales en ligne. En compromettant la disponibilité des services médicaux, ces attaques peuvent avoir des conséquences graves, notamment des retards dans les soins et des risques pour la vie des patients.[15]

2.12.1.2 Les attaques par interception de données sensibles

Impliquent l'interception non autorisée des communications entre les dispositifs de santé et les systèmes de gestion, dans le but d'obtenir des informations confidentielles. Les attaquants peuvent capturer des données telles que des identifiants d'accès, des informations médicales personnelles ou des transmissions entre les dispositifs médicaux et les serveurs d'authentification. Par exemple, un attaquant utilise des outils de sniffing pour intercepter le trafic réseau entre un moniteur cardiaque portable et une application de gestion des soins. En écoutant discrètement les échanges de données, l'attaquant peut obtenir des informations confidentielles sur l'état de santé du patient, telles que les données de fréquence cardiaque et les activités physiques. Ces attaques peuvent entraîner une violation de la confidentialité des données médicales, l'exposition des informations personnelles des patients à des tiers non autorisés, ainsi que le risque de vol d'identité et d'utilisation abusive des données médicales. De plus, elles compromettent la sécurité des dispositifs de santé en exposant les identifiants d'accès et en mettant en péril l'intégrité des transmissions médicales.[9]

2.12.1.3 Les attaques par force brute et par dictionnaire

Sont des techniques utilisées par les pirates informatiques pour tenter de deviner les identifiants de connexion en essayant systématiquement toutes les combinaisons possibles de mots de passe, ou en utilisant des listes de mots de passe couramment utilisés. Par exemple, un attaquant pourrait lancer une attaque par force brute pour découvrir les identifiants d'un administrateur de système de gestion des dispositifs médicaux, accédant ainsi à des fonctionnalités critiques. Ces attaques présentent un risque de compromission des identifiants d'accès aux dispositifs médicaux 5G, exposant ainsi les données de santé des patients à des accès non autorisés et compromettant la confidentialité et l'intégrité des informations médicales.[21]

2.12.1.4 Les interférences et les attaques par signal jamming

Sont des tactiques utilisées pour perturber les communications sans fil en émettant des signaux radio qui brouillent les fréquences utilisées par les dispositifs, les rendant incapables de communiquer correctement. Par exemple, un attaquant pourrait utiliser un émetteur de brouillage pour perturber les communications entre les capteurs de santé sans fil et les stations de base 5G, compromettant ainsi la surveillance continue des patients. Ces attaques peuvent entraîner des interruptions dans les flux de données critiques, compromettant la qualité des soins de santé et la sécurité des patients. Pour contrer ces attaques.[21]

2.12.1.5 Les attaques par canal latéral

Exploitent les vulnérabilités des dispositifs de santé ou des serveurs d'authentification pour extraire des informations sensibles. Ces attaques peuvent conduire au vol de mots de

passe, de clés dechiffrement ou d'autres données confidentielles. Par exemple, un attaquant pourrait exploiter une faille dans un dispositif de santé pour extraire les informations biométriques d'un patient ou compromettre les clés de chiffrement utilisées pour sécuriser les communications.[21]

2.12.2 Une attaque de désynchronisation

Se produit lorsqu'il y a une perturbation de la synchronisation du numéro de séquence (SQN) entre l'UE (l'Équipement Utilisateur) et le réseau, ce qui entraîne un échec d'authentification. Cette perturbation peut être exploitée par un attaquant pour empêcher l'utilisateur légitime de s'authentifier, entraînant ainsi des interruptions de service. Par exemple, un attaquant peut manipuler le numéro de séquence pour désynchroniser les échanges entre l'utilisateur et le réseau, entraînant des échecs d'authentification répétés et des interruptions de service.[21]

2.12.2.1 La compromission de clé

Survient lorsque la clé à long terme (K) est compromise, permettant à un attaquant de générer des clés d'authentification futures et passées. Cette compromission menace la sécurité des sessions futures et passées, rendant l'ensemble des communications vulnérables. Par exemple, si un attaquant parvient à compromettre la clé de chiffrement utilisée pour sécuriser les communications entre les dispositifs de santé et les serveurs d'authentification, il pourrait intercepter, modifier ou déchiffrer les données transmises, compromettant ainsi la confidentialité et l'intégrité des informations médicales.[21]

2.12.2.2 Les attaques par ransomware

Sont des attaques malveillantes qui chiffrent les données des dispositifs de santé 5G et exigent le paiement d'une rançon pour les débloquer. Ces attaques peuvent paralyser les opérations médicales et compromettre la sécurité des patients en empêchant l'accès aux données médicales critiques. L'impact de ces attaques est significatif, entraînant une perturbation des services de santé, une llperte d'accès aux données médicales critiques, ainsi qu'un risque de retard dans les soins aux patients et de mise en danger de la vie des patients. Par exemple, si les données médicales essentiees sont chiffrées par un ransomware, les professionnels de la santé peuvent être incapables d'accéder aux informations nécessaires pour fournir des soins appropriés, ce qui peut mettre en danger la vie des patients. [21]

2.12.2.3 Les attaques physiques

Impliquent le vol, la manipulation ou la destruction physique des dispositifs médicaux 5G, compromettant ainsi leur fonctionnement et l'intégrité des données médicales. Ces attaques peuvent avoir un impact grave, notamment en entraînant un risque de falsification

des données médicales, un mauvais fonctionnement des dispositifs médicaux, voire des dommages directs à la santé des patients, en fonction de la nature de l'attaque. Par exemple, un attaquant peut voler un dispositif médical contenant des données médicales sensibles, les manipuler pour modifier les informations ou les détruire physiquement, ce qui peut entraîner des conséquences graves pour la santé des patients.[21]

2.12.2.4 Les attaques par rejeu

Surviennent lorsque un pirate informatique capture une transaction d'authentification valide ou enregistre des messages légitimes, puis les rejoue ultérieurement pour accéder au système ou tromper le système. Ces attaques peuvent conduire à un accès non autorisé aux dispositifs de santé et aux données médicales, ainsi qu'à la possibilité pour un attaquant de se faire passer pour un utilisateur légitime ou de répéter des actions critiques.[21]

2.12.2.5 Les attaques de l'homme du milieu (MiTM)

Soulèvent des préoccupations concernant la confidentialité et l'intégrité des données médicales échangées entre les dispositifs de santé 5G et les systèmes de stockage ou les professionnels de la santé. Ces attaques surviennent lorsqu'un attaquant insère discrètement un dispositif ou un logiciel entre les dispositifs de santé et les systèmes de stockage, interceptant ainsi les communications et pouvant manipuler ou accéder aux données échangées. Cela met en évidence le besoin urgent de cryptage et de vérification d'identité pour sécuriser les communications et prévenir les interceptions malveillantes [19]

2.12.2.6 Les attaques de réseaux zombies

Soulignent le risque associé à la compromission des dispositifs connectés, tels que les dispositifs médicaux 5G, qui pourraient être utilisés comme des "marionnettes" dans des attaques massives. Ces attaques se produisent lorsqu'un attaquant infect et prend le contrôle de nombreux dispositifs connectés à internet, les transformant en "zombies" qui peuvent être utilisés pour lancer des attaques coordonnées et massives contre des cibles spécifiques. [21]

2.13 Contre-mesures et solutions de sécurité :

2.13.1 Mesures de Sécurité :

Dans le contexte des dispositifs de santé 5G, la sécurité est une préoccupation primordiale en raison de la nature sensible des données médicales et de la criticité des services fournis. Les dispositifs de santé connectés sont exposés à une variété de menaces et d'attaques qui peuvent compromettre la confidentialité, l'intégrité et la disponibilité des informations et des services. Afin de protéger ces dispositifs contre les cybermenaces croissantes, il est important

de mettre en place des mesures de sécurité robustes et adaptées. L'objectif est de garantir un environnement sécurisé pour les communications, le stockage des données et l'authentification des utilisateurs.

2.13.2 Mesures de Sécurité Essentielles :

2.13.2.1 Filtrage du trafic et Répartition de la charge :

- **Filtrage du trafic :** Utiliser des pare-feux et des systèmes de prévention des intrusions (IPS) pour filtrer le trafic et bloquer les attaques DDoS avant qu'elles n'affectent les systèmes.[15]

- **Répartition de la charge :** Mettre en place des solutions de répartition de charge pour distribuer le trafic et éviter la surcharge des serveurs critiques.[15]

2.13.2.2 Détection et Réponse aux Anomalies :

- **Détection des anomalies :** Implémenter des systèmes de détection des anomalies basés sur l'intelligence artificielle pour identifier et répondre rapidement aux attaques DoS/DDoS et autres comportements suspects.[15]

2.13.2.3 Chiffrement et Authentification des Communications :

- **Chiffrement des communications :** Utiliser des protocoles de chiffrement robustes comme TLS pour protéger les données échangées entre les dispositifs de santé et les serveurs.[9]

- **Authentification mutuelle :** Mettre en place une authentification mutuelle entre les dispositifs et les serveurs pour garantir l'intégrité et la confidentialité des communications.

2.13.2.4 Utilisation de VPN et Politiques de Mots de Passe :

- **VPN** : Utiliser des réseaux privés virtuels (VPN) pour sécuriser les connexions et éviter les interceptions non autorisées.[9]

- **Politiques de mots de passe forts :** Exiger des mots de passe forts et complexes, et mettre en place des politiques de rotation régulière des mots de passe pour renforcer la sécurité.

2.13.2.5 Limitation des Tentatives de Connexion et Authentification Multifactorielle (MFA) :

- **Limitation des tentatives de connexion :** Mettre en œuvre des mécanismes de limitation des tentatives de connexion pour empêcher les attaques par force brute.

- **Authentification multifactorielle (MFA) :** Utiliser des méthodes d'authentification multifactorielle pour ajouter une couche de sécurité supplémentaire.[9]

2.13.2.6 Détection de Brouillage et Communication Redondante :

- **Détection de jamming :** Installer des systèmes de détection de brouillage pour identifier et répondre rapidement aux attaques de signal jamming.

- **Communication redondante :** Mettre en place des canaux de communication redondants pour assurer la continuité du service en cas de brouillage.[9]

2.13.2.7 Sécurisation Physique et Mise à Jour Régulière :

- **Sécurisation physique :** Protéger physiquement les équipements de communication pour réduire le risque de manipulation et de sabotage.

- **Mise à jour régulière :** Mettre à jour régulièrement les logiciels et micrologiciels pour corriger les vulnérabilités connues.[9]

2.13.2.8 Gestion des Clés et Synchronisation Robuste :

- **Gestion des clés :** Implémenter des systèmes de gestion des clés robustes, incluant la rotation régulière et la révocation des clés compromises.

- **Synchronisation robuste :** Mettre en place des mécanismes de synchronisation robustes pour les numéros de séquence (SQN) entre les dispositifs et le réseau.[9]

2.13.2.9 Sauvegardes et Protection contre les Ransomwares :

- **Sauvegardes régulières :** Effectuer des sauvegardes régulières et sécurisées des données pour assurer une récupération rapide en cas d'attaque par ransomware.

Antivirus et anti-ransomware : Utiliser des logiciels antivirus et anti-ransomware à jour pour détecter et bloquer les menaces.[9]

2.13.2.10 Contrôles d'Accès et Surveillance :

- **Contrôles d'accès physiques :** Mettre en place des contrôles d'accès physiques stricts pour protéger les dispositifs médicaux et les installations critiques.

- **Surveillance et alarme :** Installer des systèmes de surveillance et d'alarme pour détecter et réagir rapidement aux tentatives d'accès non autorisé.[13]

2.13.2.11 Authentification Forte et Protocoles Sécurisés :

- **Authentification forte :** Mettre en place des méthodes d'authentification forte qui incluent des mécanismes de prévention des rejeu.

- **Protocoles sécurisés :** Implémenter des protocoles d'authentification résistants au rejeu pour assurer la sécurité des communications.[9]

2.13.2.12 Chiffrement de Bout en Bout et Vérification de l'Intégrité :

- **Chiffrement de bout en bout :** Utiliser des solutions de chiffrement de bout en bout pour protéger les communications entre les dispositifs de santé et les serveurs.

- **Vérification de l'intégrité :** Utiliser des mécanismes de vérification de l'intégrité des messages pour détecter toute altération par un attaquant.

Dans ce travail, nous nous appuierons sur le protocole EAP-AKA' pour assurer la sécurité et remédier aux attaques précédemment mentionnées.

2.14 Utilisation du Protocole EAP-AKA' pour l'Authentification des Dispositifs de Santé 5G :

Dans le cadre de l'authentification intelligente des dispositifs de santé 5G, le protocole EAP-AKA' (Extensible Authentication Protocol – Authentication and Key Agreement) se distingue comme unesolution particulièrement adaptée. EAP-AKA' offre des mécanismes de sécurité robustes, notamment [12] [23] [21] [19]

2.14.1 Authentification mutuelle :

EAP-AKA' assure l'authentification mutuelle entre les dispositifs de santé et le réseau, renforçant la sécurité des communications. Cela aide à contrer les attaques par rejeu et les attaques de l'homme du milieu (MiTM) en vérifiant les identités des deux parties et en garantissant que les messages ne sont pas interceptés ou altérés.

2.14.2 Protection contre les attaques par rejeu :

Le protocole intègre des mécanismes pour prévenir les attaques par rejeu, garantissant ainsi l'intégrité des sessions. EAP-AKA' utilise des jetons de session uniques et des horodatages pour empêcher qu'un message intercepté ne soit rejoué plus tard pour accéder au système.

2.14.3 Gestion sécurisée des clés :

EAP-AKA' utilise des méthodes sophistiquées de gestion des clés pour sécuriser les échanges et protéger les données sensibles. Cette gestion efficace des clés aide à prévenir la compromission de clé et à garantir que les données transmises sont toujours chiffrées de manière sécurisée.

2.14.4 Résistance aux attaques de canal latéral :

Grâce à des techniques avancées de sécurisation, EAP-AKA' offre une résistance accrue aux attaques de canal latéral, protégeant ainsi les informations confidentielles contre les méthodes d'extraction d'informations non conventionnelles.

2.14.5 Chiffrement de bout en bout :

Le chiffrement de bout en bout intégré dans EAP-AKA' assure que les communications restent sécurisées tout au long de leur transmission, ce qui est essentiel pour prévenir les attaques par écoute clandestine, interception et sniffing.[10]

2.14.6 Prévention des attaques par force brute et par dictionnaire :

En mettant en œuvre des mécanismes robustes de gestion des mots de passe et des politiques de sécurité strictes, EAP-AKA' aide à prévenir les attaques par force brute et par dictionnaire. L'utilisation de méthodes d'authentification multifactorielle (MFA) renforce encore la sécurité des dispositifs de santé.

En intégrant les mesures de sécurité et en utilisant le protocole EAP-AKA', les dispositifs de santé 5G peuvent bénéficier d'une protection renforcée contre les cybermenaces. Le protocole EAP-AKA' est une solution idéale pour renforcer la sécurité des dispositifs de santé 5G grâce à ses mécanismes de sécurité robustes, notamment l'authentification mutuelle, la protection contre les attaques par rejeu, la gestion sécurisée des clés et le chiffrement de bout en bout. Ces fonctionnalités permettent de contrer efficacement les diverses menaces et attaques. Ainsi, en combinant EAP-AKA' avec des mesures de sécurité supplémentaires, il est possible de créer un environnement de santé 5G sécurisé, garantissant la confidentialité,

l'intégrité et la disponibilité des services médicaux essentiels, et assurant la protection de l'ensemble de l'écosystème des dispositifs de santé 5G.

2.15 Conclusion :

Cette chapitre met en lumière l'importance de l'authentification intelligente, en particulier à travers le protocole EAP-AKA', dans la sécurisation des dispositifs de santé connectés sur les réseaux 5G. Elle souligne également l'importance d'étudier le protocole en profondeur pour identifier les points faibles et développer des stratégies efficaces pour faire face aux défis de sécurité.

En examinant les fondements de la technologie, en mettant en évidence ses caractéristiques et ses avantages, ainsi qu'en analysant son déploiement dans le contexte des dispositifs de santé 5G, vous avez clairement démontré son rôle essentiel dans la préservation de la confidentialité et de la sécurité des données médicales sensibles.

Le troisiéme chapitre de la recherche une étude plus approfondie du protocole EAP-AKA' et à la formulation de recommandations spécifiques pour renforcer la sécurité des données dans l'environnement de santé connecté à travers les réseaux 5G .

Chapitre 3

Étude de cas et applications dans la santé

3.1 Introduction

Dans un monde de plus en plus connecté, les appareils de soins de santé intelligents jouent un rôle crucial dans le suivi et l'amélioration de la santé des patients. Cependant, cette interconnexion expose également ces dispositifs à diverses menaces de sécurité, rendant la protection des données et la confidentialité des patients primordiales. Le protocole d'Authentification et de Key Agreement Extensible (EAP-AKA) est l'un des mécanismes de sécurité avancés conçus pour sécuriser ces appareils en réseau. La Protection protocole, basée sur le protocole EAP-AKA, offre une solution robuste pour garantir la sécurité et l'intégrité des communications des appareils de soins de santé intelligents.[8]

l'EAP-AKA est un protocole d'authentification largement utilisé dans les réseaux mobiles pour garantir une connexion sécurisée entre l'appareil et le réseau. Ce protocole est basé sur la technologie de carte SIM, qui offre une authentification mutuelle entre l'utilisateur et le réseau, ainsi qu'un échange sécurisé de clés cryptographiques. La Protection protocole utilise ces principes pour offrir une sécurité renforcée aux appareils de soins de santé intelligents[19] , Ce chapitre se concentre donc sur la vérification du protocole EAP-AKA et Scénario de fonctionnement.

3.2 Scénario de fonctionnement protocole EAP-AKA :

Le protocole EAP-AKA' est une méthode d'authentification qui fait partie du cadre plus large du protocole EAP (Extensible Authentication Protocol). Voici une explication détaillée des échanges de messages dans le processus EAP-AKA'

3.2.1 Explication des Éléments et Étapes :

- ▷ **Dispositif de Santé :** Collecte les mesures de santé et les envoie à l'UE (par exemple, via Bluetooth).

- ▷ **UE (User Equipment) :** L'équipement utilisateur, tel qu'un smartphone ou une tablette, utilisé par le patient pour interagir avec le réseau.
- ▷ **SEAF (Security Edge Protection Proxy) :** Assure la protection des communications entre l'UE et les fonctions internes du réseau.
- ▷ **AUSF (Authentication Server Function) :** Valide l'identité du patient en utilisant le protocole EAP-AKA' et génère les clés de session pour sécuriser les communications.
- ▷ **ARPF/UDM (Authentication and Key Management for Applications Function/User Data Management) :** Gère les données de l'abonné (patient) et les vecteurs d'authentification. Confirme l'authentification et les droits d'accès aux données médicales.
- ▷ **Hôpital/Clinique :** Stocke et gère les données médicales des patients. Valide les droits d'accès et fournit les données médicales nécessaires.
- ▷ **Médecin :** Reçoit les notifications d'accès aux données médicales du patient et peut surveiller ou analyser ces données.

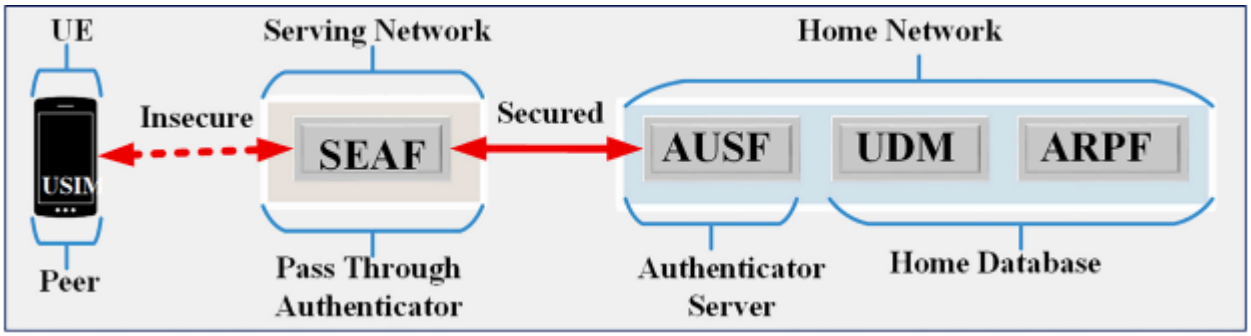

FIGURE 3.1 – : Architecture générale protocole EAP-AKA' Réseaux 5G [11]

Voici une explication détaillée des étapes impliquées dans la première phase du protocole EAP-AKA :

3.2.2 Etape 01 : Initialisation et demande d'identité

3.2.2.1 Message 01. Dispositif de Santé → UE :

Mesures de santé Les dispositifs de santé légers ne peuvent pas se connecter directement au réseau. Ainsi, les dispositifs de santé collecte des données de santé (comme la glycémie, la pression artérielle, etc.) et les transmet à l'UE (le téléphone du patient ,par exemple via Bluetooth).

3.2.2.2 Message 02. SEAF → UE : (EAP-Request/Identity) :

▷ Le SEAF (Security Edge Anchor Function) envoie un message EAP-Request/Identity à l'UE (User Equipment).

▷ Ce message demande à l'UE de fournir son identité afin de commencer le processus d'authentification.

3.2.2.3 Message 03. UE → SEAF : (SUCI) :

▷ L'UE répond au SEAF avec un message contenant le SUCI (Subscription Concealed Identifier).

▷ Le SUCI est une identité de l'utilisateur qui est cachée pour des raisons de confidentialité mais peut être utilisée pour l'authentification.

3.2.2.4 Message 04. SEAF → AUSF : (SUCI, SNN) :

▷ Le SEAF transmet le SUCI reçu de l'UE ainsi que le nom du réseau de sécurité (SNN) à l'AUSF (Authentication Server Function).

▷ Le SNN identifie le réseau de sécurité auquel l'UE tente de se connecter.

3.2.2.5 Message 05. AUSF → ARPF : (SUCI, SNN) :

▷ L'AUSF envoie un message à l'ARPF (Authentication and Routing Policy Function) ou à l'UDM (User Data Management) dans le domaine de l'opérateur avec le SUCI et le SNN.

▷ Avant de procéder, l'AUSF vérifie l'autorisation du SEAF.

▷ L'ARPF/UDM, lors de la réception du message, dévoile le SUCI en SUPI (Subscription Permanent Identifier) à l'aide du SIDF (Subscription Identifier De-Conceal Function) et sélectionne une méthode d'authentification appropriée.

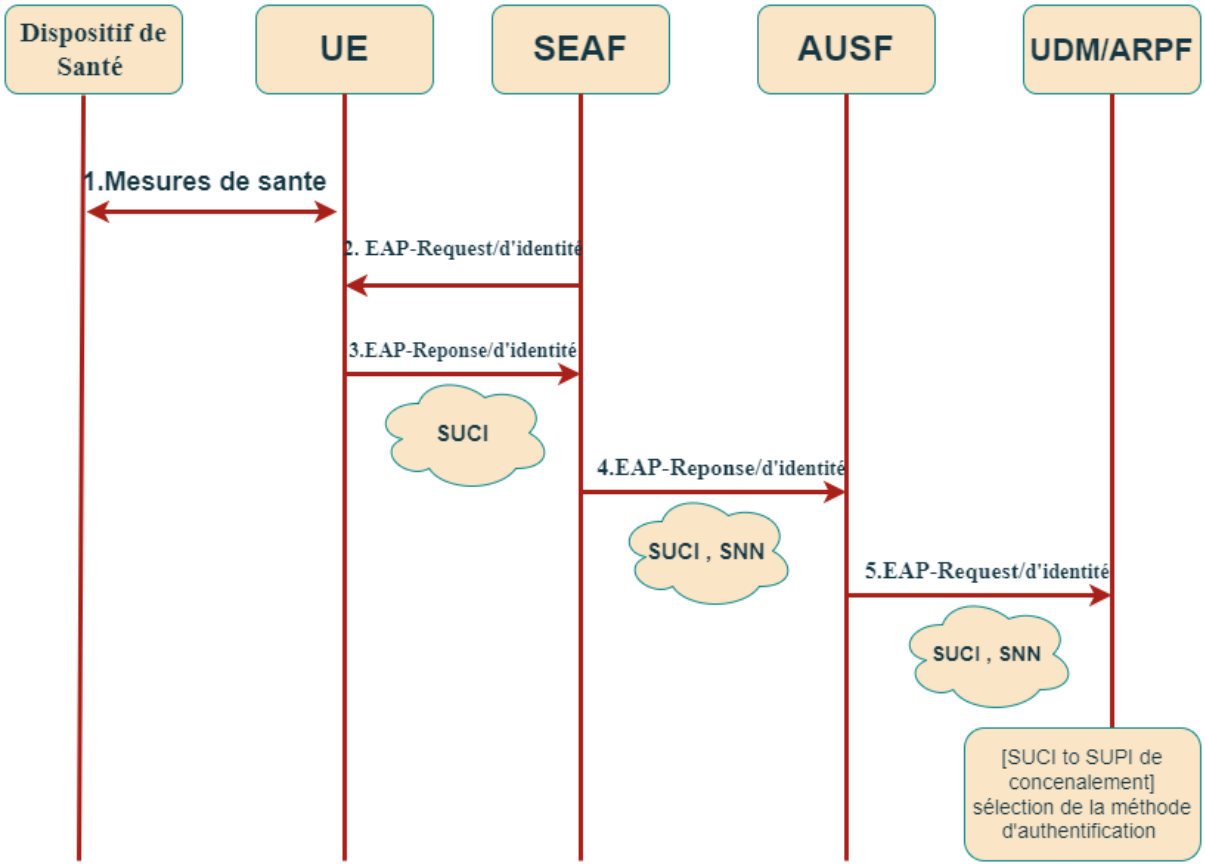

FIGURE 3.2 – EAP- AKA' Etape 01.

Ces étapes initiales établissent la communication entre l'UE et les fonctions d'authentification du réseau (SEAF, AUSF, ARPF/UDM) et permettent de commencer le processus d'authentification de l'utilisateur.

3.2.3 Etape 02 : Authentification et challenge

Voici une explication détaillée de la phase 2 du protocole EAP-AKA :

3.2.3.1 Message 06. ARPF → AUSF : EAP-AKA' AV (RAND, AUTN, XRES, SNN,MAC,SQN, CK' IK', SUPI) :

▷ L'ARPF envoie à l'AUSF les vecteurs d'authentification (AV) EAP-AKA' contenant le challenge RAND, le numéro de nonce AUTN, la réponse authentique XRES, le nom du réseau de sécurité SNN, la clé de chiffrement CK' et la clé d'intégrité IK', ainsi que l'identifiant permanent de l'utilisateur (SUPI).

▷ **RAND :** Un nombre aléatoire généré par l'ARPF.

▷ **AUTN :** Un numéro de nonce pour éviter les attaques par rejeu.

- ▷ **XRES :** La réponse authentique de l'UE calculée précédemment.
- ▷ **SNN :** Le nom du réseau de sécurité.
- ▷ **MAC :**(Message Authentication Code) : Ensures the integrity and authenticity of the message.
- ▷ **SQN :**Numéro de séquence
- ▷ **CK' et IK' :** Les clés de chiffrement et d'intégrité dérivées de l'identité permanente de l'utilisateur (SUPI).
- ▷ **KDF** : (Key Derivation Function Attribute)
- ▷ **KDF input** : (Key Derivation Function Input Attribute)
- ▷ **SUPI :** L'identifiant permanent de l'utilisateur.

3.2.3.2 7. Message 07. AUSF → SEAF : (RAND, AUTN, SNN)

- ▷ Lorsque l'AUSF reçoit le msg5, il stocke XRES et SUPI avant d'envoyer un message EAP-Request/AKA'-Challenge au SEAF. Ce message contient le challenge RAND, le numéro de nonce AUTN et le nom du réseau de sécurité SNN.

3.2.3.3 Message 08. SEAF → UE : (RAND, AUTN, ngKSI, ABBA) :

- ▷ Dans le message Auth-Request (Message 7), le SEAF envoie le challenge RAND et le numéro de nonce AUTN à l'UE. Le paramètre ABBA doit être inclus dans ce message pour activer la protection en aval.
  - ▷ **ngKSI :** L'identifiant de jeu de clés NAS (Non-Access Stratum), qui aide à gérer les clés de chiffrement pour l'interface NAS.
  - ▷ **ABBA :** Un paramètre supplémentaire pour améliorer la sécurité.

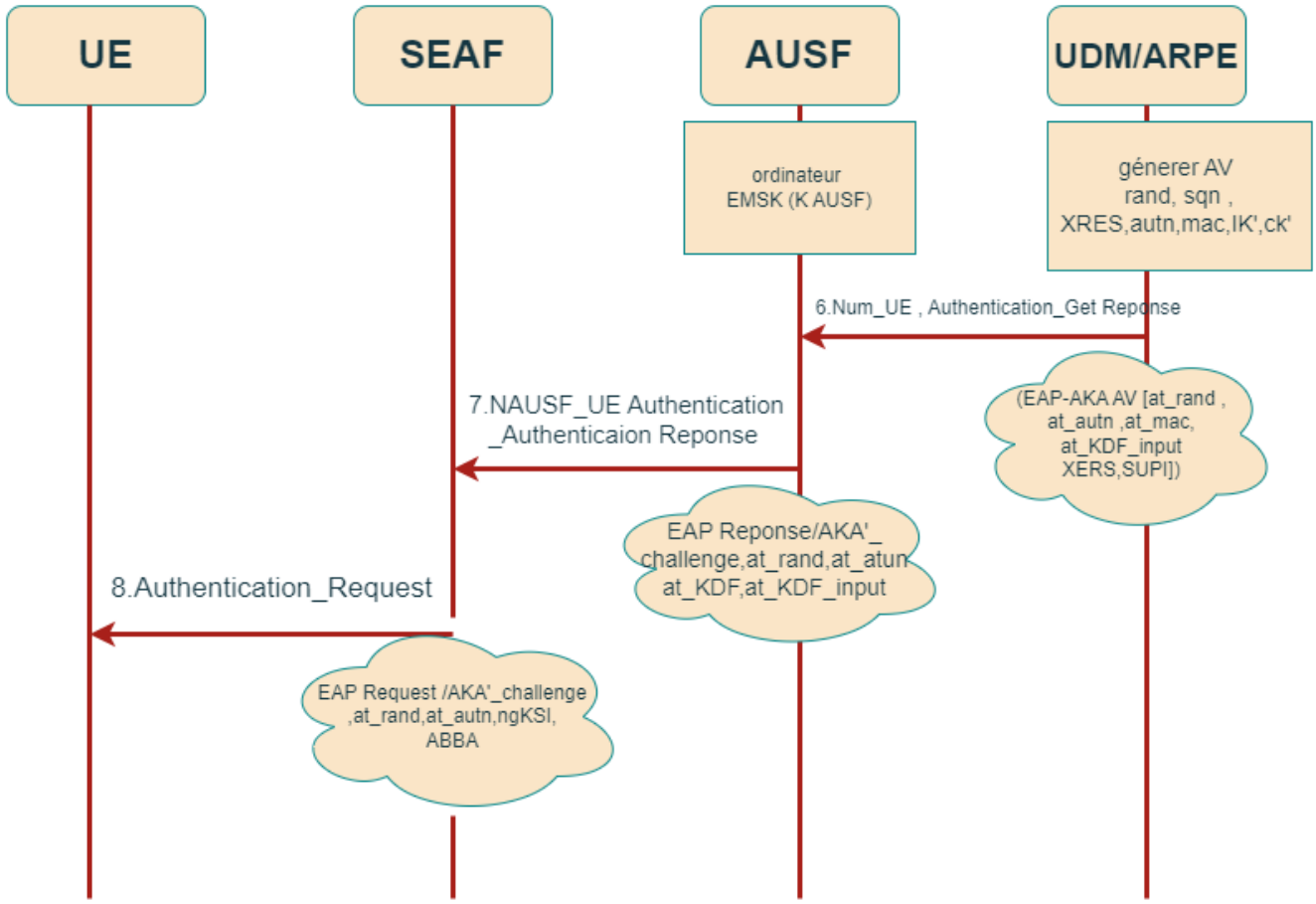

FIGURE 3.3 – EAP- AKA' Etape 02.

3.2.3.4 Message 09. UE → SEAF : (RES, MAC) :

▷ Lorsque l'UE reçoit le msg7, elle transmet le challenge RAND et le numéro de nonce AUTN à la USIM (Universal Subscriber Identity Module), qui vérifie l'authenticité du AV en vérifiant la fraîcheur du AUTN. L'UE génère alors la clé de session AK et obtient le numéro de séquence SQN. Elle génère ensuite le code d'authentification MAC2 et le compare au MAC reçu. Si MAC2 est égal à MAC et que SQN est dans la plage autorisée, l'UE calcule RES et renvoie le tout avec MAC2.

3.2.3.5 Message 10. SEAF → AUSF : (RES, MAC) :

▷ Le SEAF transfère transparentement le msg8 en msg9 à l'AUSF. Il peut y avoir un échange optionnel de messages EAP supplémentaires après le msg9.

3.2.3.6 11. Message 11. AUSF → SEAF : EAP-Success (KSEAF, SUPI) :

▷ Lorsque l'AUSF reçoit RES et MAC2, il les vérifie en les comparant à XRES. S'ils sont égaux, l'AUSF considère l'authentification comme réussie, informe l'UDM et dérive la clé de session KSEAF. Il envoie ensuite KSEAF au SEAF dans le message EAP-Success.

3.2.3.7 12. Message 12. SEAF → UE : EAP-Success (ngKSI, ABBA) :

▷ Le SEAF envoie un message de succès à l'UE avec ngKSI et le paramètre ABBA. L'UE génère la clé de session KSEAF de la même manière que l'AUSF.

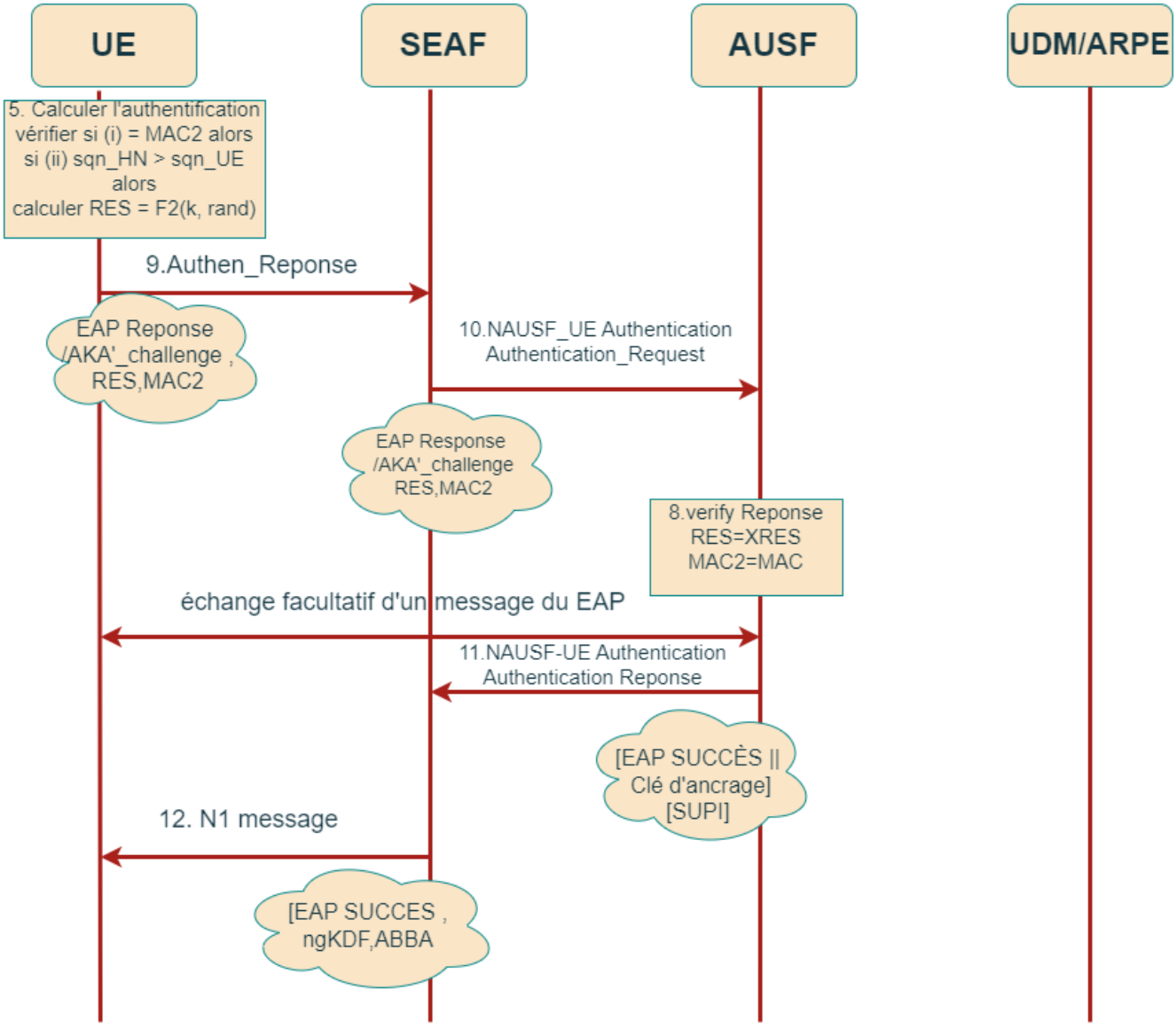

FIGURE 3.4 – EAP- AKA' Etape 02.

3.2.4 Etape 03 : Resynchronisation

La phase de resynchronisation est une procédure utilisée pour mettre à jour le numéro de séquence (SQN) sur le côté du réseau domestique (HN) lorsque celui-ci est désynchronisé avec l'USIM (Universal Subscriber Identity Module) de l'utilisateur. Voici les étapes détaillées de cette phase :

- ▷ **Échec de la vérification AUTN :** Lorsque l'USIM détecte un échec de vérification de l'AUTN (Authentication Token), il informe l'UE (User Equipment) s'il s'agit d'un échec de MAC (Message Authentication Code) ou de synchronisation. L'USIM envoie ensuite le paramètre AUTS (Authentication Synchronization) à l'UE.

3.2.4.1 Message 13 (UE → SEAF) :

L'UE envoie un échec de MAC (Mac failure) et de synchronisation (Synch failure) ainsi que l'AUTS au SEAF (Security Anchor Function).

3.2.4.2 Message 14 (SEAF → AUSF) :

Le SEAF peut demander à l'UE de se réidentifier en cas d'échec de MAC ou de lancer une nouvelle session d'authentification en cas d'échec de synchronisation. Le SEAF envoie ensuite le message 13 à l'AUSF (Authentication Server Function).

3.2.4.3 Message 15 (AUSF → ARPF) :

Avec le RAND (Random Number) transmis à l'UE dans le message 6, et l'AUTS reçu dans le message 13, l'AUSF envoie le message 14 au UDM/ARPF (Unified Data Management/Authentication Repository and Processing Function). L'ARPF obtient le SQNUE (SQN de l'UE) de l'AUTS, vérifie la plage du SQNHN (SQN du HN), et détermine si le SQN créé avec le SQNHN sera accepté par l'USIM.

Calcul de nouveaux vecteurs d'authentification (AV) : Après une vérification réussie, l'UDM/ARPF calcule de nouveaux AV, vérifie l'AUTS et réinitialise la valeur du compteur SQNHN à SQNUE. L'UDM/ARPF envoie ensuite les nouveaux AV à l'AUSF pour que l'UE puisse effectuer une nouvelle exécution du protocole d'authentification.

Cette procédure assure que l'UE et le HN sont synchronisés et que l'authentification peut se poursuivre de manière sécurisée. Comme indiqué sur la Figure 2.4.

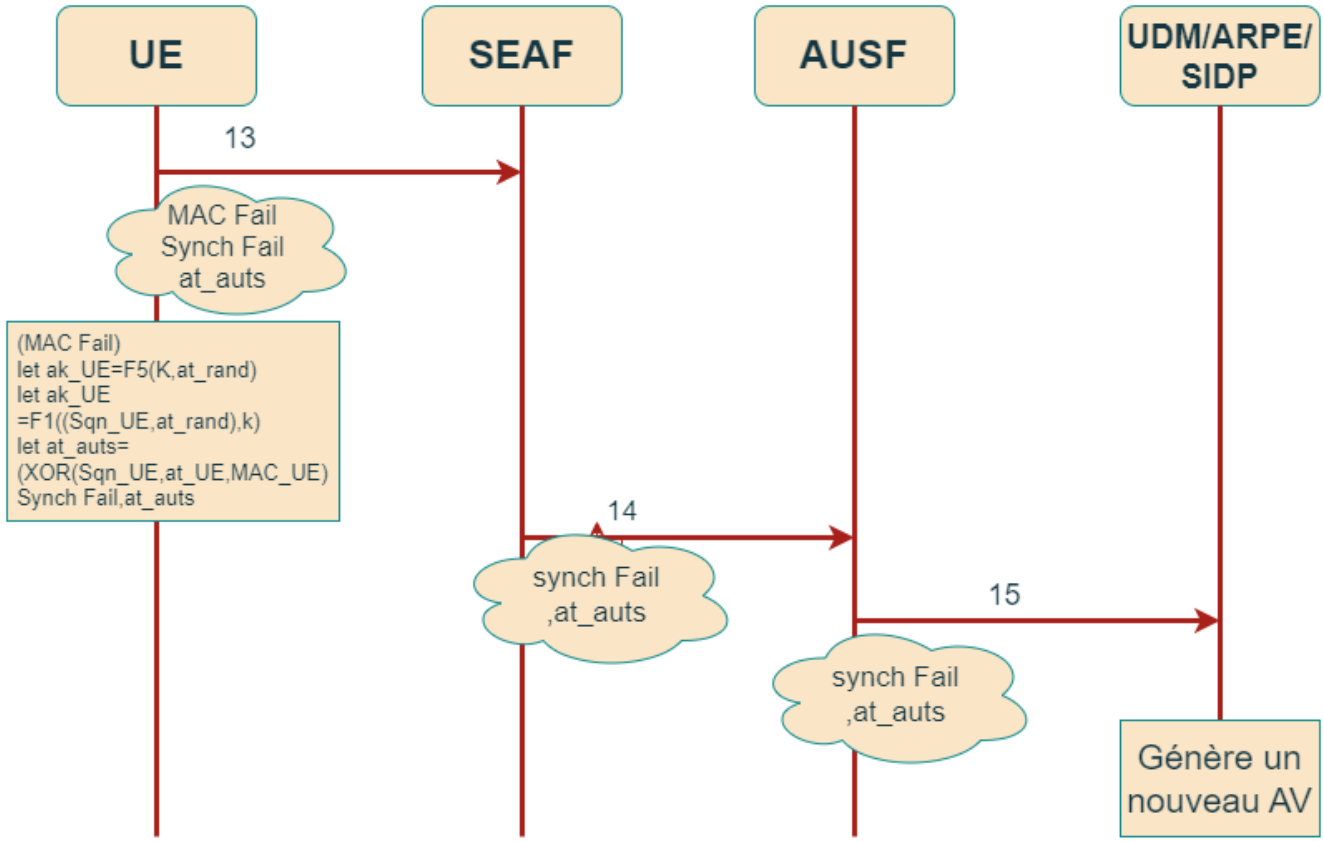

FIGURE 3.5 – EAP- AKA' Etape 03

3.2.5 Etape 04 : Accès aux données médicales

3.2.5.1 Message 16 (UE → Hôpital/Clinique) :

Demande de données médicales L'UE envoie une demande d'accès aux données médicales à l'hôpital ou la clinique.

3.2.5.2 Message 17 (Hôpital/Clinique → SEAF) :

Validation des droits d'accès L'hôpital ou la clinique demande au SEAF de valider les droits d'accès de l'utilisateur.

3.2.5.3 Message 18 (SEAF → Hôpital/Clinique) :

Confirmation de l'authentification et droits d'accès Le SEAF confirme l'authentification et les droits d'accès de l'utilisateur auprès de l'hôpital ou de la clinique.

3.2.5.4 Message 19 (Hôpital/Clinique → UE) :

Accès aux données médicales L'hôpital ou la clinique fournit les données médicales demandées à l'UE.

3.2.5.5 Message 20 (Hôpital/Clinique → Médecin) :

Notification d'accès Une notification est envoyée au médecin traitant informant que le patient a accédé à ses données médicales

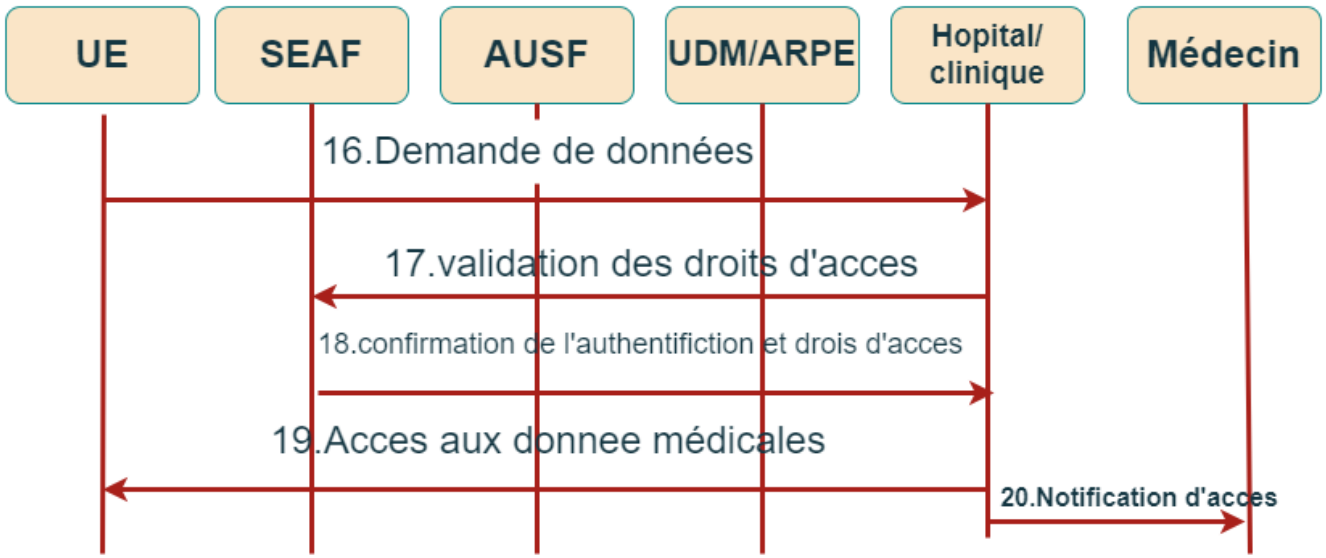

FIGURE 3.6 – EAP- AKA' Etape 04

3.3 Description des Attaques de Rejeu sur le Protocole EAP-AKA 5G :

Il présente certaines vulnérabilités aux attaques de rejeu qui peuvent compromettre la confidentialité des utilisateurs. Voici une description détaillée de l'attaque et de son impact potentiel :

3.3.1 Mécanisme de l'Attaque de Rejeu :

3.3.1.1 Capturer et Rejouer le Message de Challenge :

- ▷ Un acteur malveillant peut capturer le message de challenge (Message 8 : SEAF → UE : (RAND, AUTN, ngKSI, ABBA)) qui est envoyé de manière claire du SEAF à l'UE.

▷ L'attaquant enregistre ce message et le rejoue plus tard pour détecter la présence du UE ciblé dans une zone particulière.

3.3.1.2 Différence de Réponse entre UE Ciblé et Autres Dispositifs :

- **Dispositifs non ciblés :** Si le message rejoué est reçu par un dispositif qui n'est pas le UE ciblé, ce dispositif essaiera de vérifier la valeur MAC avec sa propre clé. Puisque la clé utilisée pour calculer le MAC du message rejoué est partagée uniquement entre le UE ciblé et le HN, cette vérification échouera, entraînant une réponse 'mac-failure'.

- **Dispositif ciblé :** Si le message rejoué est reçu par le UE ciblé, la vérification MAC réussira car le UE ciblé utilise la même clé que celle utilisée pour calculer le MAC. Cependant, le message contient un ancien numéro de séquence (SQN), ce qui entraînera une 'sync-failure' puisque le UE aura avancé son SQN.

3.3.1.3 Détection de Présence :

▷ L'attaquant peut détecter la présence du UE ciblé en surveillant les réponses aux messages rejoués. Une réponse 'sync-failure' indique que le UE ciblé est dans la zone, ce qui constitue une violation de la vie privée.

3.3.1.4 Analyse des Modèles de Connexion :

▷ En rejouant le même message de challenge plusieurs fois, l'attaquant peut obtenir des informations sur la fréquence de connexion du UE ciblé. Les réponses contiendront des valeurs SQN XORées avec une valeur dérivée du message de challenge. En analysant les différences entre ces valeurs, l'attaquant peut déduire les changements dans le numéro de séquence du UE, révélant ainsi des informations sur ses habitudes de connexion.

3.4 propositions d'amélioration le Protocole EAP-AKA 5G :

Supposons que nous choisissions d'implémenter le chiffrement et l'intégrité des messages

3.4.1 Chiffrement des Messages de Challenge :

- **Chiffrement des messages de challenge (RAND, AUTN) :** En chiffrer les messages de challenge pour que même s'ils sont interceptés, ils ne puissent pas être utilisés par un attaquant. Cela peut impliquer l'utilisation de clés de session temporaires ou de techniques de chiffrement symétrique.

- **Ajout d'un MAC (Message Authentification Code) aux messages sensibles :** Chaque message, y compris les réponses de l'UE, doit inclure un MAC calculé avec une clé partagée, garantissant ainsi l'intégrité des messages et rendant plus difficile la falsification par un attaquant.

3.4.2 Ajout de MAC aux Messages Sensibles :

▷ Chaque message échangé entre l'UE et le SEAF inclut un MAC calculé à partir du contenu du message et d'une clé partagée.

▷ L'UE et le SEAF vérifient le MAC à chaque réception de message. Si le MAC ne correspond pas, le message est rejeté.

3.4.3 Utilisation de Timestamps :

▷ Chaque message de challenge inclut un timestamp pour vérifier la fraîcheur du message.

▷ L'UE vérifie que le timestamp est dans une plage acceptable avant de traiter le message. Si le timestamp est trop ancien, le message est ignoré.

3.4.4 Synchronisation Sécurisée :

- **Mécanisme de resynchronisation sécurisé :** Améliorer le protocole de resynchronisation pour qu'il soit moins susceptible de révéler des informations lors des échecs de synchronisation. Par exemple, l'utilisation de nonces temporaires ou de séquences plus complexes pour masquer le véritable numéro de séquence.

- **Utilisation de timestamps :** Inclure des timestamps dans les messages de challenge pour vérifier la fraîcheur du message et empêcher la réutilisation de vieux messages. Si un message de challenge a un timestamp trop ancien, il peut être rejeté.

3.4.5 Détection et Réponse aux Attaques de Rejeu :

- **Surveillance des échecs de synchronisation :** Implémenter des mécanismes au niveau du réseau pour détecter les patterns d'échecs de synchronisation anormaux. Une augmentation soudaine des messages 'sync-failure' pourrait indiquer une attaque de rejeu.

- **Limitation du nombre de resynchronisations :** Restreindre le nombre de tentatives de resynchronisation autorisées dans une période donnée pour éviter les attaques par force brute.

3.4.6 Authentification Multi-Facteur :

Authentification multi-facteur : Introduire des éléments d'authentification supplémentaires qui ne sont pas vulnérables aux attaques de rejeu, comme des codes de confirmation envoyés via des canaux sécurisés (SMS, emails) ou l'utilisation de biométrie.

Ces contre-mesures, combinées, renforceraient la sécurité du protocole EAP-AKA et réduiraient considérablement les risques d'attaques de rejeu. En implémentant ces solutions, les réseaux mobiles peuvent offrir une meilleure protection de la confidentialité et de la sécurité des utilisateurs.

3.5 Conclusion :

Dans ce chapitre, nous avons exploré en détail le fonctionnement du protocole d'authentification EAP-AKA dans le contexte des applications de santé. Nous avons examiné chaque étape du processus d'authentification, en mettant en évidence les mécanismes de sécurité en place pour protéger les données sensibles des utilisateurs. Dans le chapitre qui suit, nous nous intéressons à la vérification de ces protocoles de sécurité EAP-AKA en utilisant une plateforme de validation automatique, SPAN AVISPA.

Chapitre 4

Vérification des protocoles de sécurité EAP-AKA' avec l'outil SPAN AVISPA

4.1 Introduction :

De nos jours, de nombreuses failles de sécurité ont été découvertes dans divers protocoles cryptographiques publiés. Il est donc crucial de vérifier automatiquement la sécurité de ces protocoles avant leur mise en service. La sécurité de ces protocoles ne repose pas uniquement sur l'utilisation de méthodes de chiffrement, mais également sur une vérification automatique et formelle.[18]

Dans ce chapitre, nous présentons les principales propriétés des protocoles cryptographiques ainsi que quelques notions relatives à leur vérification, en nous basant sur un modèle formel. Nous décrivons les caractéristiques, les méthodes et les outils de vérification automatique qui s'appuient sur ce modèle. Nous mettrons particulièrement l'accent sur l'outil AVISPA, qui permet la spécification, l'analyse et la validation des protocoles de sécurité. Nous soulignerons les principaux aspects de modélisation adoptés par cet outil.

4.2 Présentation de l'outil AVISPA :

AVISPA (Automated Validation of Internet Security Protocols and Applications) a été développé en 2004 par Basin et al. dans le cadre d'un projet européen. Cet outil d'analyse automatique est conçu pour aider à la validation des protocoles. Il vise à atteindre deux objectifs majeurs : offrir des performances élevées tout en restant accessible aux non-spécialistes du domaine. AVISPA peut être utilisé pour analyser des protocoles de petite et moyenne échelle (comme ceux disponibles dans la bibliothèque Clark/Jacob1), ainsi que des protocoles de sécurité Internet à grande échelle.[18]

4.3 Architecture logicielle de l'outil AVISPA (back-end AVISPA) :

AVISPA dispose de quatre back-ends différents, comme illustré sur la Figure , chacun implémentant des techniques d'analyse variées. Ces techniques vont de la falsification de protocole (découverte d'attaques sur le protocole d'entrée) à des méthodes de vérification basées sur des abstractions pour des nombres finis ou infinis de sessions. Si une propriété de sécurité est violée dans la spécification, l'analyseur produit une trace de séquence d'événements qui mène à la faille et indique quelle propriété a été violée.[18]

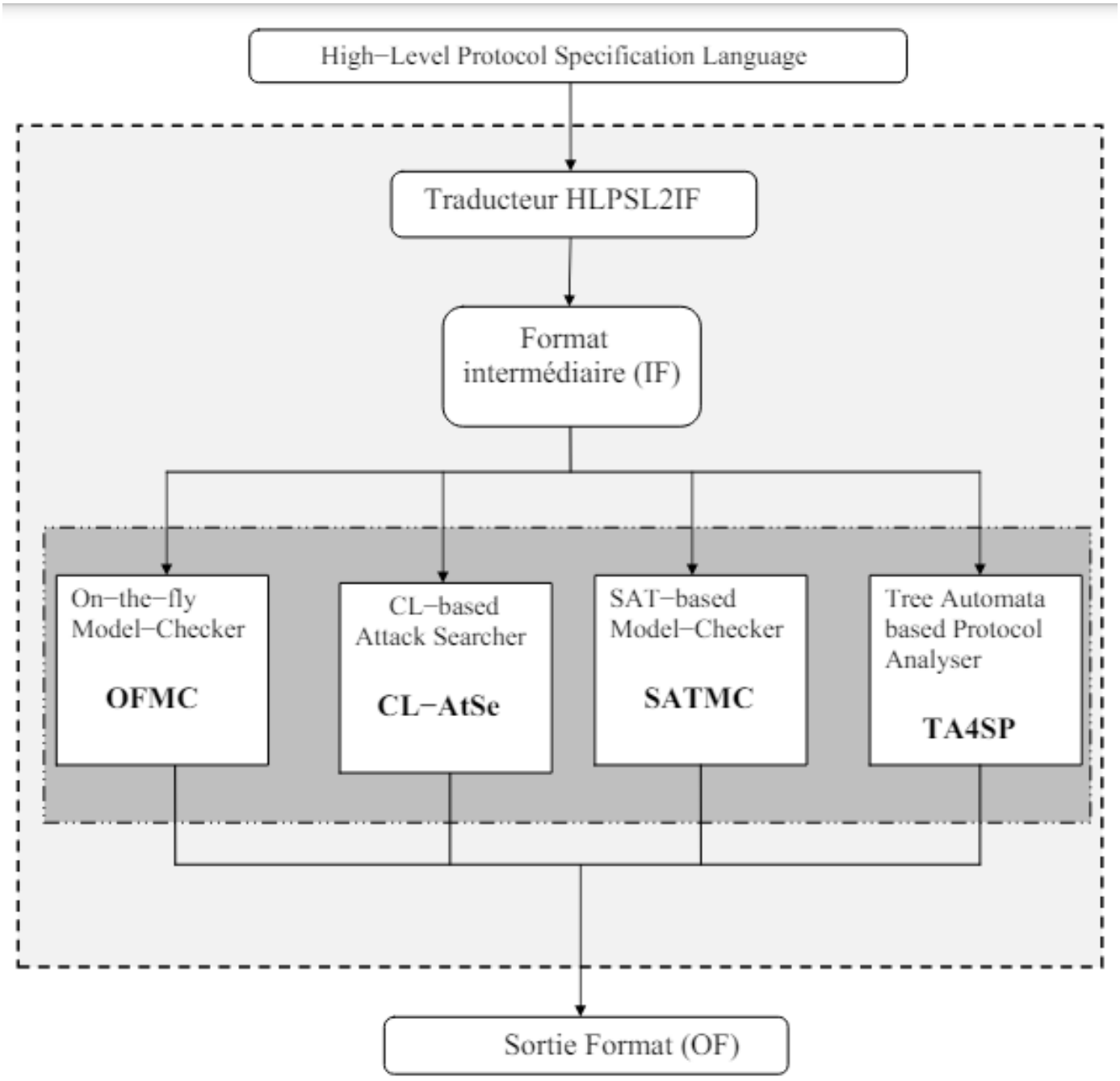

FIGURE 4.1 – Architecture d'AVISPA.[18]

4.4 Description des principaux Back-Ends de l'outil AVISPA :

L'outil AVISPA (Automated Validation of Internet Security Protocols and Applications) utilise plusieurs back-ends pour analyser et vérifier la sécurité des protocoles de communication. Voici une description des principaux back-ends de l'outil AVISPA [18][14] :

4.4.1 OFMC (On-the-Fly Model Checking) :

L'histoire d'OFMC a commencé avec le projet AVISS, avant de mûrir au sein du projet AVISPA. Cet outil effectue une vérification bornée en explorant le système de transition décrit par une spécification IF. OFMC implémente des techniques symboliques qui sont à la fois correctes et complètes. Il supporte la spécification des opérateurs avec des propriétés algébriques, tels que le OU exclusif (XOR) ou l'exponentiation. OFMC est particulièrement utile pour les protocoles où les propriétés algébriques des fonctions cryptographiques sont cruciales.

4.4.2 CL-AtSe (Constraint Logic-based Attack Searcher) :

CL-AtSe est un outil basé sur des techniques de résolution de contraintes et implémente une procédure de décision. Il traduit une spécification de protocole de sécurité sous forme de relations de transition au format IF en un ensemble de contraintes, permettant ainsi de trouver des attaques sur le protocole. La traduction et la vérification sont entièrement automatiques et prises en charge par CL-AtSe sans nécessiter d'outils externes. Les capacités de CL-AtSe ont été étendues lors du projet AVISPA pour supporter des opérateurs possédant des propriétés algébriques, comme le XOR et l'exponentiation. Il procède également à une simplification du protocole en éliminant les états redondants grâce à des propriétés heuristiques, et sa modularité permet d'intégrer facilement d'autres spécifications de fonctions cryptographiques.

4.4.3 SATMC (SAT-based Model Checker) :

Développé au laboratoire DIST à Gênes (Italie), SATMC construit une formule propositionnelle codant un déploiement borné du système de transition IF, l'état initial et l'ensemble des états représentant la violation des propriétés de sûreté spécifiées en IF (ou en HLPSL). Cette formule est ensuite résolue par un solveur SAT, parmi lesquels zCHAFF, mCHAFF, SIM, et SATO. Tout modèle satisfaisant cette formule est retourné sous forme d'attaque. SATMC utilise un état transitoire pour rechercher les éventuelles violations d'un protocole, générant une formule représentant la violation et la transformant en attaque.

4.4.4 TA4SP (Tree-Automata-based Protocol Analyzer) :

TA4SP se distingue par son approche utilisant des automates d'arbres pour effectuer soit une sur-approximation, soit une sous-approximation des connaissances de l'intrus à partir d'un état initial. Cette méthode permet de déterminer si un certain état est accessible ou non et si l'intrus peut acquérir certaines connaissances, concluant ainsi à l'absence d'attaque sur le secret pour des scénarios exécutés un nombre indéterminé de fois. En d'autres termes, TA4SP montre la vulnérabilité d'un protocole ou la prédit en faisant une estimation précise des capacités de l'intrus.

4.5 Présentation du langage de spécification des protocoles HLPSL :

Pour écrire des spécifications de protocoles de sécurité, AVISPA utilise un langage appelé HLPSL (High-Level Protocol Specification Language). HLPSL est inspiré des travaux de Lamport sur la logique temporelle des actions (TLA - Temporal Logic of Actions). La représentation des protocoles de sécurité dans HLPSL repose sur des systèmes d'états/transitions, permettant la vérification des propriétés de sûreté exprimées en logique temporelle linéaire.

L'analyse des protocoles nécessite des constructions syntaxiques (comme la structure du message) et des concepts sémantiques (comme la notion de l'intrus). Idéalement, modéliser des protocoles dans un langage intégrant ces éléments communs serait pratique. HLPSL a été développé avec les objectifs de conception suivants [14] :

4.5.1 Lisibilité et puissance :

HLPSL doit être lisible par l'homme, facile à utiliser, tout en étant assez puissant pour supporter la spécification des protocoles Internet modernes. Pour cela, HLPSL ressemble formellement à un langage de définition de transitions gardées dans un système de transitions d'états et est équipé de constructions permettant la spécification modulaire de protocoles.

4.5.2 Sémantique formelle :

HLPSL doit disposer d'une sémantique formelle. Pour atteindre cet objectif, HLPSL s'appuie sur la TLA de Lamport et sa sémantique est donnée par une traduction en un sous-ensemble de TLA.

4.5.3 Analyse formelle automatisée :

HLPSL doit se prêter à une analyse formelle automatisée. Cela est réalisé par une traduction de HLPSL dans un format intermédiaire (IF).

Les spécifications HLPSL représentent toutes les entités pouvant intervenir dans le protocole. Cette description est faite dans un fichier avec l'extension .hlpsl, qui sera ensuite traduit à l'aide du traducteur hlpsl2if pour générer un fichier .if. Les différents back-ends utilisent ce format pour vérifier le protocole spécifié.

4.6 Présentation du langage de spécification des protocoles CAS+ :

Le CAS+ (Community Adaptable Protocol Specification) est un langage de spécification de protocoles conçu pour modéliser et analyser les protocoles de communication de manière flexible et évolutive. Développé pour répondre aux besoins des communautés de recherche et de développement, CAS+ permet de décrire les interactions entre les différents participants d'un protocole, ainsi que les messages échangés et les conditions de sécurité à respecter. Il se distingue par sa capacité à s'adapter facilement à divers types de protocoles, y compris ceux nécessitant des mises à jour fréquentes ou des modifications pour s'adapter à de nouveaux environnements ou à des exigences changeantes. Grâce à une syntaxe claire et à des outils de vérification automatisés, CAS+ facilite l'identification et la correction des vulnérabilités potentielles dans les protocoles avant leur déploiement, garantissant ainsi des communications sécurisées et fiables.

4.7 Interface graphique de SPAN AVISPA :

Cette interface fournit une fonction pour écrire, traduire, vérifier et enregistrer les spécifications du protocole de sécurité, ainsi que d'afficher les résultats et les symboles dans différents formats. Comme indiqué dans la figure possible

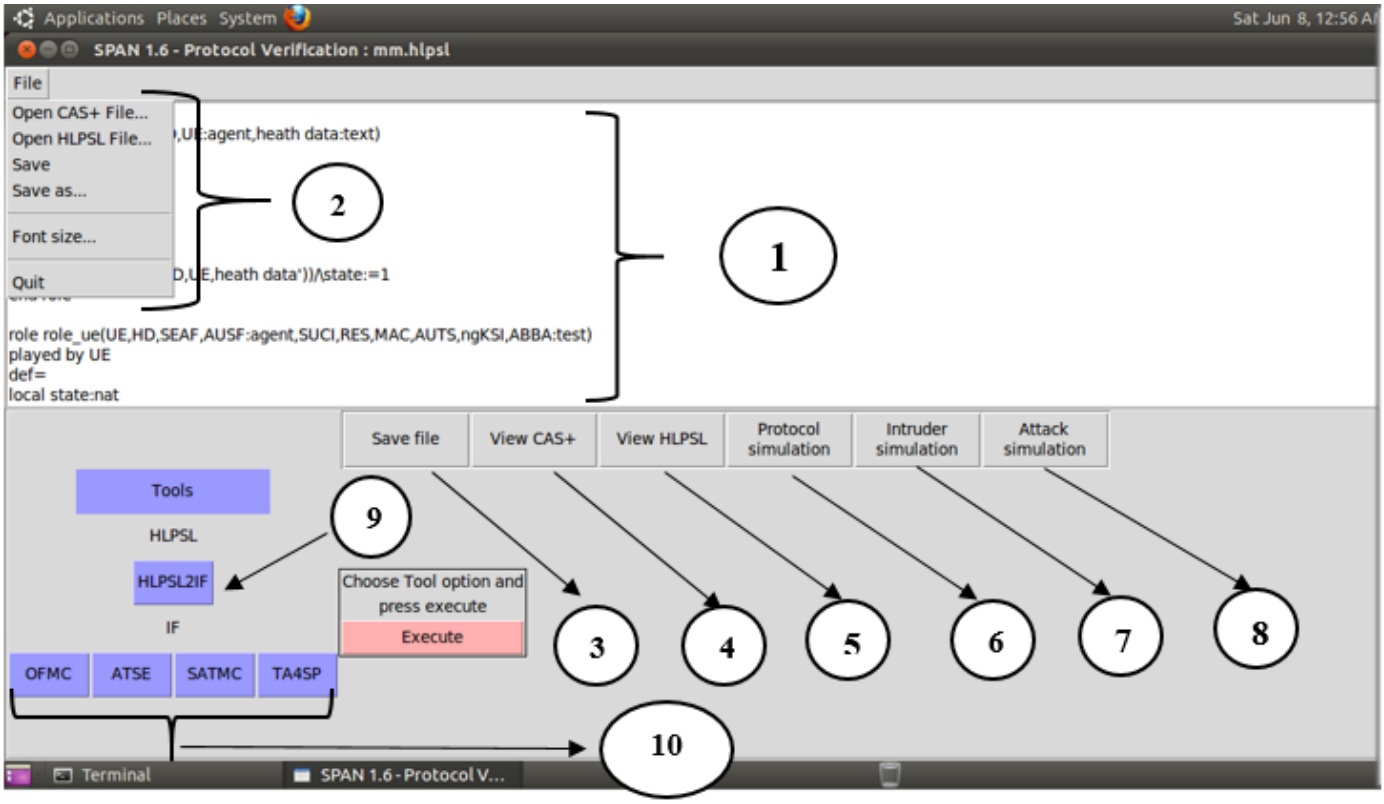

FIGURE 4.2 – Interface graphique de SPAN AVISPA

Voici une description des éléments numérotés dans l'interface : 1 : Zone de la spécification HLPSL

2 : Ouvrir ou enregistrer une spécification HLPSL ou quitter l'application

3 : Enregistrer le fichier modifie HLPSL ou CAS+ 4 : Outils de vérification

4 : Voir le code CAS+

5 : Voir le code HLPSL

6 : Trace du protocole en mode normal

7 : Trace du protocole en mode intrus

8 : Trace du protocole en mode Attack

9 : Translation de HLPSL a une forme intermédiaire

10 : Outils de vérification

4.8 Vérification formelle des protocoles de sécurité EAP-AKA :

Nous avons exécuté sur SPAN le code du programme protocole EAP-AKA écrit en HLPSL étaillé ci-dessus :

```
role ue(A,B,C,D: agent, M:text, SND, RCV: channel(dy)) played_by A
def=
  local
  AT_RAND          : text,
    NAI              : text,
    AT_MAC1 : hash(hash(text.hash(symmetric_key.text).hash(symmetric_key.text)).text.message),
    AT_MAC2 : hash(hash(text.hash(symmetric_key.text).hash(symmetric_key.text)).hash(symmetric_key.text)),
    AT_AUTN : message,
    AT_RES, IK, CK   : hash(symmetric_key.text),
 State:nat,
  SNN,SUCI,ABBA:text
  request_id,
    respond_id,
    SUCCESS    : text,
    sec_ck1, sec_ik1,
    at_rand,
    at_rand2    : protocol_id
  init State:= 1
  transition
        1. State = 1 /\ RCV(SUCI') =|> State':=3
        /\ SNN' := new()
        /\ SND(SUCI'.SNN')
       2.State = 1 /\ RCV(RAND'.ATUN'.SNN') =|> State' := 9
                    /\ SND(RES'.MAC')
        3.State = 1 /\ RCV(SUCCESS') =|> State' := 13


end role
```

FIGURE 4.3 – Code du UE (User Equipment)

```
role seaf(A,B,C,D: agent, M,SUCI:text, SND, RCV: channel(dy)) played_by B
def=
   local

  AT_RAND          : text,
    NAI              : text,
    AT_MAC1 : hash(hash(text.hash(symmetric_key.text).hash(symmetric_key.text)).text.message),
    AT_MAC2 : hash(hash(text.hash(symmetric_key.text).hash(symmetric_key.text)).hash(symmetric_key.text)),
    AT_AUTN : message,
    AT_RES, IK, CK   : hash(symmetric_key.text),
 State:nat,
  SNN,SUCI:text
  request_id,
    respond_id,
    SUCCESS     : text,
    sec_ck1, sec_ik1,
    at_rand,
    at_rand2    : protocol_id
   init State:= 0
   transition
        1. State = 0 /\ RCV(start)  =|> State' := 2 /\ SND(SUCI)
        2.State = 0 /\ RCV(SNN'.SUCI')  =|> State' := 4
                    /\ SND(SUCI'.SNN')
        3.State = 0 /\ RCV(RAND'.ATUN'.SNN') =|> State' := 8
                    /\ SND(RAND'.ATUN'.SNN')
      4.State = 0 /\ RCV(RES'.MAC') =|> State' := 10
                    /\ SND(RES'.MAC')
      5.State = 0 /\ RCV(SUCCESS') =|> State' := 12
                    /\ SND(SUCCESS')

end role
```

FIGURE 4.4 – Code du SEAF(Security Edge Protection Proxy)

```
role ausf(A,B,C,D: agent, M:text, SND, RCV: channel(dy)) played_by C
def=
  local

  AT_RAND          : text,
    NAI              : text,
    AT_MAC1 : hash(hash(text.hash(symmetric_key.text).hash(symmetric_key.text)).text.message),
    AT_MAC2 : hash(hash(text.hash(symmetric_key.text).hash(symmetric_key.text)).hash(symmetric_key.text)),
    AT_AUTN : message,
    AT_RES, IK, CK   : hash(symmetric_key.text),
 State:nat,
  SNN,SUCI:text
  request_id,
    respond_id,
    success     : text,
    sec_ck1, sec_ik1,
    at_rand,
    at_rand2    : protocol_id
State:nat,
  SUCI,SNN,AV:text
  init State:= 2
  transition
        1.State = 2 /\ RCV(SNN'.SUCI')  =|> State' := 5
                    /\SND(SUCI'.SNN')
        2.State = 2 /\ RCV(AV') =|> State' := 7
                    /\ SND(RAND'.ATUN'.SNN')
           3.State = 2 /\ RCV(RES'.MAC') =|> State' := 11
                    /\ SUCCESS':= new()
                    /\ SND(SUCCESS')
end role
```

FIGURE 4.5 – Code du AUSF(Authentication Server Function)

```
role arpf(A,B,C,D: agent, M,AV:text, SND, RCV: channel(dy)) played_by D
def=
 local
  AT_RAND            : text,
    NAI              : text,
    XRES             : text,
    AT_MAC1 : hash(hash(text.hash(symmetric_key.text).hash(symmetric_key.text)).text.message),
    AT_MAC2 : hash(hash(text.hash(symmetric_key.text).hash(symmetric_key.text)).hash(symmetric_key.text)),
    AT_AUTN : message,
    AT_RES, IK, CK   : hash(symmetric_key.text),
 State:nat,
  SNN,SUCI:text
  request_id,
    respond_id,
    SUCCESS : text,
    sec_ck1, sec_ik1,
    at_rand,
    at_rand2    : protocol_id
 State:nat,
  SUCI,SNN:text
  init Satate:= 3
  transition
        1.State = 3 /\ RCV(SNN'.SUCI')  =|> State' := 6
                    /\ AV' := new()
                    /\ AV'= RAND ,XRES, at_rand,sqn,ck'
                    /\ CK'  = F3(SK.AT_RAND')
                    /\ SND(AV')
end role
```

FIGURE 4.6 – Code du ARPF (Authentication and Routing Policy Function)

4.9 Résultat de la vérification par le back-end OFMC :

L'objectif de ce test est de détecter les vulnérabilités de sécurité dans le design proposé. L'outil AVISPA analyse et classe les résultats en deux catégories : "safe" pour les protocoles sécurisés, et "unsafe" pour ceux contenant des failles. AVISPA vérifie s'il existe une attaque pendant l'exécution du protocole. En cas de protocole non sécurisé, AVISPA fournira une trace détaillée de l'attaque et montrera comment des dommages peuvent être causés. Nos vérifications sont effectuées par le back-end OFMC, et le résultat obtenu est le suivant :

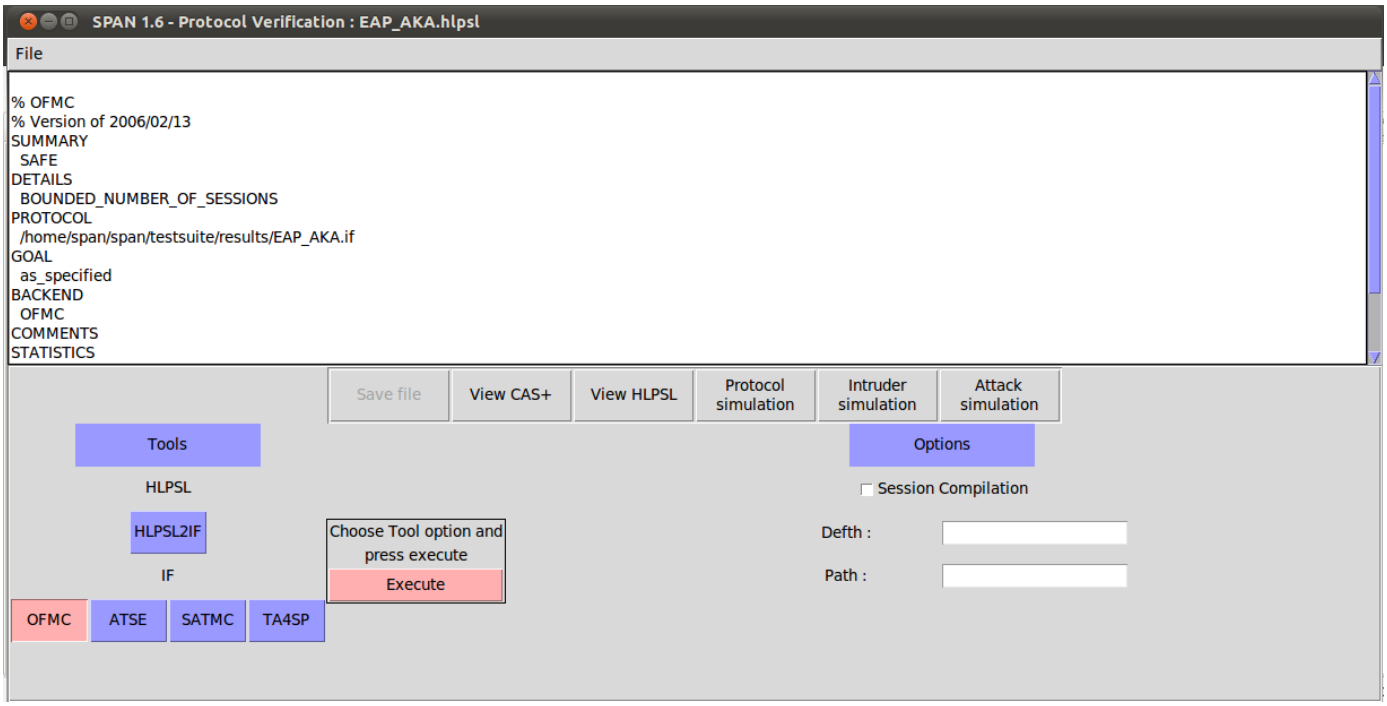

FIGURE 4.7 – Résultat de la vérification

- La première section, SUMMARY, indique si le protocole est sécurisé ou non, ou si l'analyse n'a pas été concluante. Dans notre cas, le résultat est SAFE.
- La deuxième section, DETAILS, décrit les conditions sous lesquelles le protocole est déclaré sûr ou non, les conditions sous lesquelles une attaque est trouvée, et les raisons pour lesquelles l'analyse n'a pas été concluante.
- La section PROTOCOL rappelle le nom du protocole analysé.
- La section GOAL présente l'objectif de l'analyse, comme par exemple la confidentialité de la clé de chiffrement des données.
- La section BACKEND désigne le traducteur des spécifications HLPSL.

Ainsi, l'outil AVISPA a démontré que notre solution ne contient pas de faille de sécurité. Les résultats confirment l'absence de brèche de sécurité, notamment en ce qui concerne la

confidentialité. Le rapport obtenu, présenté dans la figure, justifie que le protocole est sécurisé et bien protégé contre diverses attaques .

4.10 Code de vérification formelle des protocoles EAP-AKA'

Nous avons exécuté sur SPAN le code du programme protocole EAP-AKA écrit en CAS + étaillé ci-dessus :

```
protocol EAP-AKA;

identifiers
A,B,C,D         : user;
Suci,Request,Snn,Av,Rand,Autn,Ngksi,Abba,Res,Mac ,Success ,Macfail,Synchfail,Atauts : number;
IK, CK   : symmetric_key;
messages
1. B -> A       : Request
2. A => B       : Suci
3. B => C       : Suci,Snn
4. C => D       : Suci,Snn
5. D => C       : Av
6. C => B       :Rand , Autn , Snn
7. B => A       :Rand , Autn ,Ngksi,Abba
8. A => B       :Res,Mac
9. B => C       :Res,Mac
10. C => B      :Success
11. B => A      :Success
12. A => B      :Macfail,Synchfail,Atauts
13. B => C      :Synchfail,Atauts
knowledge
A       : A,B,C,D,Suci,Request,Rand,Autn,Ngksi,Abba,Res,Mac ,Success,Macfail,Synchfail,Atauts   ;
B       : A,B,C,D,Suci,Request,Snn,Rand,Autn ,Ngksi,Abba,Res,Mac ,Success,Macfail,Synchfail,Atauts   ;
C       : A,B,C,D,Suci,Request,Snn,Av,Rand,Autn,Res,Mac ,Success,Macfail,Synchfail,Atauts   ;
D       :A,B,C,D,Suci,Request,Av,Rand,Autn,Res,Mac  ;

session_instances
 [A:ue,B:seaf,C:ausf,D:arpf,Suci:suci
,Request:request,Snn:snn,Av:av,Rand:rand,CK:ck,Autn:autn,Ngksi:ngksi
,Abba:abba,Res:res,Mac:mac ,Success :success,Macfail:macfail,Synchfail:synchfail,Atauts:atauts  ];

intruder_knowledge
 ue,seaf,ausf,arpf,suci,request,snn,av,rand,autn,ngksi,abba,res,mac ,ck,success,macfail,synchfail,atauts
```

FIGURE 4.8 – Code du langage CAS+

4.11 Simulation du protocole EAP-AKA :

Tout d'abord, nous lançons le code source écrit en CAS+. Une fois l'exécution terminée sans erreurs, nous pouvons simuler le protocole entre les deux entités. La figure suivante présente les différentes étapes de cette simulation :

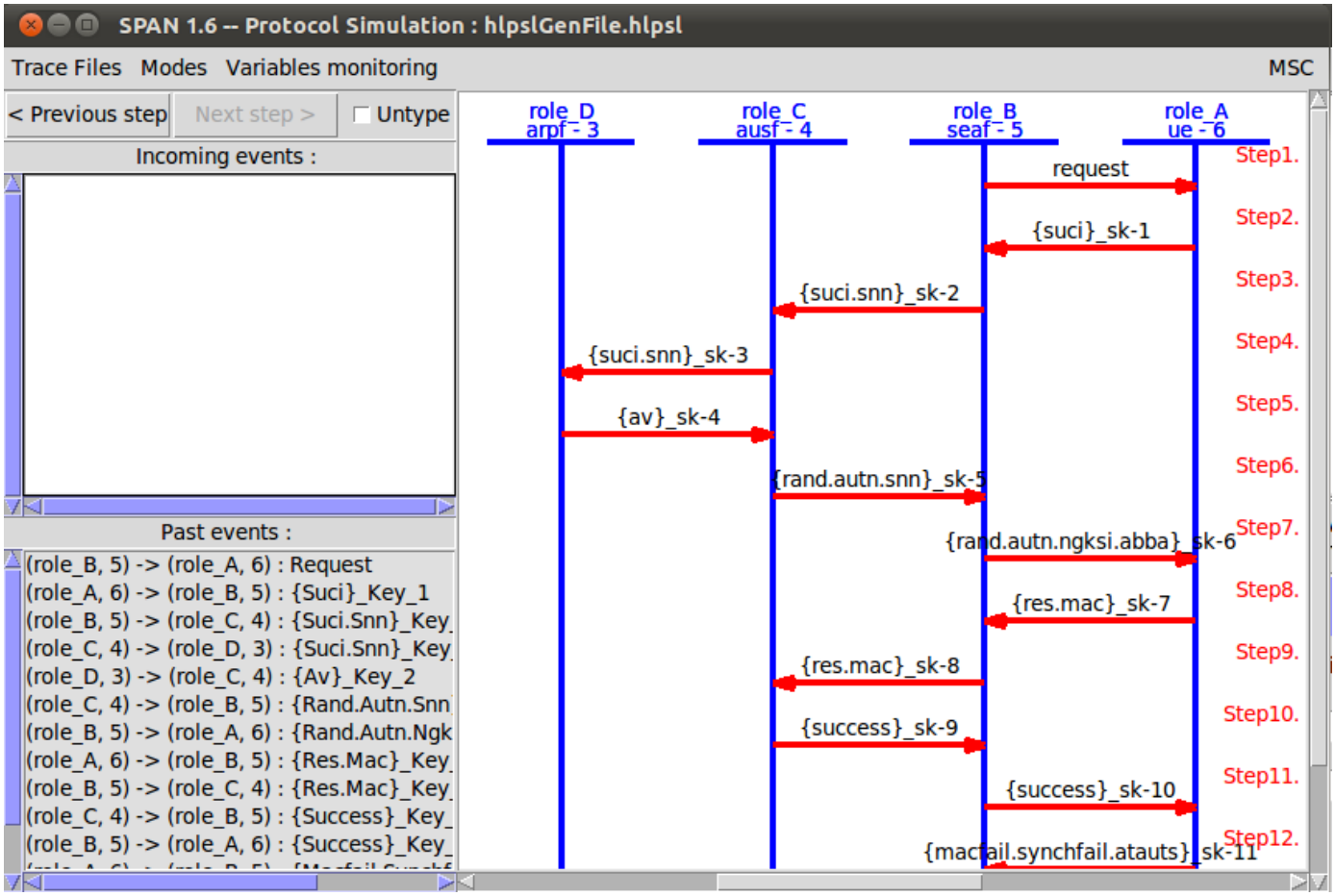

FIGURE 4.9 – Simulation du protocole EAP-AKA

4.12 Conclusion

Dans ce chapitre, nous avons exploré les notions fondamentales des outils de vérification SPAN AVISPA et du langage HLPSL et CAS+, ainsi que la vérification formelle des protocoles EAP-AKA'. Nous avons couvert la spécification formelle, la simulation et les résultats de vérification obtenus, en soulignant l'importance de cette vérification pour assurer la confidentialité des protocoles EAP-AKA'.

l'outil AVISPA, grâce à ses diverses fonctionnalités et à l'intégration de HLPSL et CAS+, a prouvé que les protocoles de sécurité EAP-AKA' sont exempts de failles majeures, garantissant la confidentialité et l'intégrité des communications. Cette vérification rigoureuse valide la fiabilité des protocoles dans des environnements critiques.

Conclusion et perspectives

La révolution numérique transforme de nombreux secteurs, et le domaine de la santé ne fait pas exception. L'émergence des réseaux de cinquième génération (5G) et de l'Internet des Objets (IoT) ouvre de nouvelles perspectives pour améliorer la qualité des soins, l'efficacité des services médicaux, et l'expérience des patients. Les technologies 5G et IoT permettent la connectivité en temps réel et la gestion des données à grande échelle, offrant ainsi des opportunités sans précédent pour les dispositifs médicaux connectés.

Cependant, cette interconnexion accrue et la dépendance aux technologies de l'information soulèvent des défis importants en matière de sécurité. Les dispositifs de santé 5G doivent non seulement être fiables et performants, mais aussi garantir la confidentialité et la protection des données médicales sensibles. L'authentification des dispositifs de santé devient ainsi une priorité cruciale pour prévenir les accès non autorisés et les cyberattaques potentielles.

Ce mémoire s'inscrit dans cette dynamique en explorant les mécanismes d'authentification adaptés aux dispositifs de santé connectés à des réseaux 5G. Notre objectif est de proposer des solutions robustes et sécurisées qui répondent aux exigences spécifiques du domaine médical. Nous aborderons les différentes caractéristiques des réseaux 5G et de l'IoT dans le contexte de la santé, les protocoles de sécurité existants, et les défis liés à leur mise en œuvre.

Nous commencerons par une revue des réseaux 5G et de leurs applications dans le secteur de la santé, en soulignant les avantages et les opportunités qu'ils offrent. Ensuite, nous analyserons les protocoles d'authentification actuels, notamment le protocole EAP-AKA', et évaluerons leur adéquation pour les dispositifs de santé 5G. Enfin, nous présenterons des études de cas et des scénarios d'application pour illustrer l'implémentation pratique des solutions proposées et nous avons exploré les notions fondamentales des outils de vérification SPAN AVISPA et du langage HLPSL et CAS+,.

Bibliographie

[1] A Comparative Introduction to 4G and 5G Authentication https ://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication, 2019.

[2] Définition de la 5G tout ce que vous devez savoir sur la 5g https ://actualiteinformatique.fr/internet-of-things-iot/definition-de-la-5g, January 2021.

[3] Télésanté : connecter la ville et l'offre de santé grâce à la 5G https ://www.orange-business.com/fr/magazine/5g-telesante-connecter-ville-et-offre-sante, 2023.

[4] Chronique de Viswanathan Ramaswamy Tata Communications . Quels avantages de la 5G privée pour le secteur de la santé ? https ://www.journaldunet.com/economie/sante/1525155-quels-avantages-de-la-5g-privee-pour-le-secteur-de-la-sante/, September 2023.

[5] Abdul Ahad, Mohammad Tahir, Muhammad Aman Sheikh, Kazi Istiaque Ahmed, Amna Mughees, and Abdullah Numani. Technologies trend towards 5g network for smart health-care using iot : A review. *Sensors*, 20(14) :4047, 2020.

[6] Shams Forruque Ahmed, Md Sakib Bin Alam, Shaila Afrin, Sabiha Jannat Rafa, Samanta Binte Taher, Maliha Kabir, SM Muyeen, and Amir H Gandomi. Towards a secure 5g-enabled internet of things : A survey on requirements, privacy, security, challenges, and opportunities. *IEEE Access*, 2024.

[7] Victor Hugo Costa de Albuquerque Akash Kumar Bhoi, editor. *5G IoT and Edge Computing for Smart Healthcare.* 2022.

[8] Jari Arkko and Henry Haverinen. Extensible authentication protocol method for 3rd generation authentication and key agreement (eap-aka). Technical report, 2006.

[9] CYBER COVER contact@cyber cover.fr. 5G : quels sont les enjeux de cybersécurité ?https ://www.cyber-cover.fr/cyber-documentation/cyber-securite/quels-sont-les-veritables-enjeux-de-cybersecurite-poses-par-larrivee-de-la-5g.

[10] Ed Kamya Kiyemba Edris, Mahdi Aiash, and Jonathan Loo. Formalization and evaluation of eap-aka'protocol for 5g network access security. *Array*, 16 :100254, 2022.

[11] Ed Kamya Kiyemba Edris, Mahdi Aiash, and Jonathan Loo. Formalization and evaluation of eap-aka'protocol for 5g network access security. *Array*, 16 :100254, 2022.

[12] Ed Kamya Kiyemba Edris, Mahdi Aiash, Jonathan Kok-Keong Loo, and Mohammad Shadi Alhakeem. Formal verification of secondary authentication protocol for 5g secondary authentication. *International Journal of Security and Networks*, 16(4) :223–234, 2021.

[13] flaunay. La sécurité des réseaux mobiles – Part 6 | Frédéric Launay https ://blogs.univ-poitiers.fr/f-launay/2021/06/29/la-securite-des-reseaux-mobiles-part-6/, June 2021.

[14] Y Glouche, T Genet, and E Houssay. Span : A security protocol animator for avispa. *IRISA/Université de Rennes 1 : Rennes, France, September*, 2008.

[15] AB Feroz Khan, Mohammed Muzaffar Hussain, S Kalpana Devi, and MA Gunavathie. Ddos attack modeling and resistance using trust based protocol for the security of internet of things. *Journal of Engineering Research*, 11(2) :100058, 2023.

[16] Bektas-C. Dorsch N. & Wietfeld Kurtz, F. Network Slicing for Critical Communications in Shared 5G Infrastructures - An Empirical Evaluation. In Proceedings of the Conference on Network Softwarization and Workshops. 2018.

[17] F Launay. Les réseaux de mobiles 4G et 5G. Université de Poitiers.TEHTRIS. (n.d.). Le monde de la santé face aux cyberattaques. Retrieved from. June 2021.

[18] Mohamedi Malika and Ikerbane Samia. *Vérification automatique d'un protocole de sécurité dans les systèmes RFIDs à base d'outils AVISPA & SPAN.* PhD thesis, Université Mouloud Mammeri, 2016.

[19] Avijit Mallik. Man-in-the-middle-attack : Understanding in simple words. *Cyberspace : Jurnal Pendidikan Teknologi Informasi*, 2(2) :109–134, 2019.

[20] Kaspersky. (n.d.). La technologie 5G est-elle dangereuse ? Les avantages et les inconvénients du réseau 5G. Retrieved from https ://www.kaspersky.fr/resource-center/threats/5g-pros-and-cons, 2023.

[21] Laurent Oudot. Le monde de la santé face aux cyberattaqueshttps ://tehtris.com/fr/blog/le-monde-de-la-sante-face-aux-cyberattaques/, April 2022.

[22] Radiator. Open System Consultants Pty. Ltd. (16 juin 2016). "Radiator EAP-SIM, EAP-AKA and EAP-AKA' Support." White paper. Version 2.0. page 17, June 2016.

[23] P. Richard. 5G : un déploiement à haut risque ? Informatique et Numérique. November 2020.

RÉSUMÉ

Ce mémoire explore l'intégration des technologies 5G et de l'Internet des objets (IdO) dans le domaine de la santé, se concentrant sur l'authentification des appareils de santé connectés. Il analyse le protocole EAP-AKA', utilisé pour sécuriser les communications dans les réseaux 5G, offrant des avantages tels que l'authentification mutuelle et l'échange sécurisé de messages. Malgré ces fonctionnalités, des vulnérabilités subsistent, nécessitant des améliorations contre les attaques de rejeu et de désynchronisation. L'outil de vérification formelle SPAN AVISPA est utilisé pour évaluer et valider la sécurité du protocole EAP-AKA', confirmant sa robustesse pour les applications de santé connectée.

Mots clés : 5G, IdO, santé, protocoles de sécurité, EAP-AKA', vérification formelle, SPAN AVISPA.

ABSTRACT

This thesis explores the integration of 5G technologies and the Internet of Things (IoT) in the healthcare sector, focusing on the authentication of connected medical devices. It analyzes the EAP-AKA' protocol, used to secure communications in 5G networks, offering benefits such as mutual authentication and secure message exchange. Despite these features, vulnerabilities persist, necessitating improvements against replay and desynchronization attacks. The formal verification tool SPAN AVISPA is used to evaluate and validate the security of the EAP-AKA' protocol, confirming its robustness for connected healthcare applications.

Key words : 5G, IoT, healthcare, security, EAP-AKA', formal verification, SPAN AVISPA.