وزارة البحث العلمي والتعليم العالي
MINISTERE DE L'ENSEIGNEMENT SUPEREUR ET DE LA RECHERCHE SCIENTIFIQUE
جامعة عبد الحميد بن باديس مستغانم
Université Abdelhamid Ibn Badis de Mostaganem
كلية العلوم والتكنولوجيا
Faculté des Sciences et de la Technologie
DEPARTEMENT DE GENIE ELECTRIQUE

N° d'ordre : M ...../GE/2020

MEMOIRE

Présenté pour obtenir le diplôme de

MASTER EN ELECTRONIQUE

Option : électronique des systèmes embarqués

Thème

Gestion intelligente et contrôle de l'accès aux salles de cours

(Par carte RFID suivant un emploi du temps)

Présenté par :

DIARRA Pierre Dit Prince

Mohamed Ghaly Ould ELBOU

Soutenu le /12/2019 devant le jury composé de :

Président :	M. CHAOUACH Abdallah	MC	Université de Mostaganem
Examinateur :	M. BENTOUMI Mohamed	MC	Université de Mostaganem
Encadreur :	M. AZZEDINE Mohammed	MC	Université de Mostaganem

Année Universitaire 2019/2020

Remerciements

Nous rendons grâce en premier lieu au ***Seigneur****, de nous avoir assisté durant toute notre étude et de nous avoir donné le courage et la force nécessaire d'accomplir ce travail de mémoire de fin d'étude.*

Nous tenons à remercier toutes les personnes qui, de près ou de loin ont participé à l'élaboration de ce mémoire, à commencer par notre encadreur ***Mr. Azzedine*** *pour sa disponibilité, ses idées, ses conseils et encouragements. Nous remercions très vivement tous nos professeurs, ami(e)s et tous nos proches qui ont contribué à la réalisation de ce projet.*

Dédicaces

Je dédie ce modeste travail aux personnes qui me sont chères :

Ma grand-mère ***Hortense Diallo*** *et mon grand-père* ***Joachim Sidibé*** *paix à son âme sans qui, je ne serais pas là où j'en suis. Ils ~~Qui~~ ont su me donner les bonnes bases nécessaires depuis ma tendre enfance.*

Mes parents*, pour leurs amours, leurs soutiens, leurs sacrifices, leurs conseils, leurs prières, leurs aides tant émotionnelles que financières. Ils n'ont cessé de me guider et sans qui je ne serai pas à ce niveau.*

A mes ***Oncles*** *et* ***Tantes****.*

Mes ***Ami(e)s*** *ainsi que toutes les personnes qui m'ont aidé et soutenu tout au long de mon cursus.*

Diarra Pierre dit Prince

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma reconnaissance.

Je dédie d'abord et avant tout ce travail réussi à mon ***père ELBOU OULD BOUH*** *et ma mère* ***FATIMETOU BABA*** *pour leurs soutiens, leurs amours et leurs prières ininterrompues.*

Mes frères, oncles et tantes et à toute ma famille, mes amies et tous ceux qui ont contribué de près ou de loin à la réussite de ma cursus universitaire.

Mohamed Ghaly Ould Elbou

Résumé

Notre projet consiste à la réalisation d'un système de contrôle d'accès physique basé sur la technologie des cartes sans contact. Plus concrètement de la gestion de l'accès aux salles de cours par carte RFID suivant un emploi du temps, avec une plateforme de suivi des accès (application web) nommée gateSecurAccess.

Notre mémoire est subdivisé en quatre principaux chapitres. Le premier chapitre intitulé **Contrôle d'accès physique**, portera sur une étude générale des systèmes de contrôle d'accès physiques basés sur la technologie des cartes sans contacts. Il décrira les propriétés, les fonctions, les caractéristiques d'un tel système et les avantages de son utilisation. Le second chapitre intitulé **La technologie RFID** se consacre à une étude générale des cartes RFID, leur principe de fonctionnement, les différents types de tags RFID, leurs caractéristiques, les fréquences d'utilisation. Le troisième chapitre intitulé **Réalisation de la carte d'accès et de l'application web**, portera sur la réalisation pratique du mémoire. Il se compose de deux parties :

- Une première partie consacrée à la réalisation de la carte d'accès. Elle décrira le principe de fonctionnement du système, les schémas électriques de l'ensemble du système et des sous blocs, le rôle des différentes cartes composant le système, l'organigramme des algorithmes du système.

- Une deuxième partie consacrée à la réalisation de l'application web. Cette dernière décrit le processus de réalisation de l'application web à savoir : les différentes technologies utilisées pour sa réalisation, la présentation de l'application, la description (fonctionnement et algorithmes) des différentes pages de l'application, la fonction de chaque page.

Un quatrième et dernier chapitre intitulé **Tests de fonctionnement et implémentation sur maquette**, dans ce chapitre nous ferons des tests. Ces tests porteront sur la lecture des cartes, l'identification et l'authentification de la carte, la transmission des informations d'accès au module wifi et à l'application web, l'affichage du suivi dans l'application web.

Summary

Our project consists of the realization of a physical access control system based on contactless card technology. More specifically, the management of access to classrooms by RFID card according to a schedule, with an access monitoring platform (web application).

Our study thesis is subdivided into four main chapters. The first chapter, entitled **Physical Access Control**, will cover a general study of physical access control systems based on contactless card technology. It will describe the properties, functions, characteristics of such a system and the advantages of its use. The second chapter entitled **The RFID technology** is devoted to a general study of RFID cards, their operating principle, the different types of RFID tags, their characteristics, and the frequencies of use. The third chapter entitled **Realization of the access card and the web application**, will focus on the practical realization of the thesis. It consists of two parts :

- A first part devoted to the realization of the access card. It will describe the operating principle of the system, the electrical diagrams of the entire system and the sub-blocks, the role of the various cards making up the system, the flowchart of the system algorithms.
- A second part devoted to the realization of the web application. The latter describes the process of making the web application, namely : the different technologies used for its realization, the presentation of the application, the description (operation and algorithms) of the different pages of the application, the function of each page.

A fourth and last chapter entitled Functional tests and implementation on a model, in this chapter we will do some tests. These tests will cover the reading of the cards, the identification and the authentication of the card, the transmission of access informations to the wifi module and to the web application, and the display of the tracking in the web application.

Tables des matières

Liste des figures

Liste des tableaux

Introduction Générale

Depuis la sédentarisation de l'homme et l'apparition des premières constructions, la question de la protection du bien et de sa famille ont été au centre des préoccupations de l'homme.

Pour cela il fallait trouver des moyens ou techniques pour restreindre l'accès aux habitations et par conséquent aux biens. De ce fait les premières habitations étaient fait avec de petites ouvertures faisant office de porte sans portail, donc une personne étrangère cherchant à pénétrer chez autrui devrait s'accroupir, cette position d'inconfort laissait le temps au propriétaire de se défendre face à l'intrus.

Il faut dire que l'homme a évolué depuis et les techniques avec.

Il y'a 7000 ans les égyptiens inventèrent le verrou à loquet tombant qui est une simple tige de bois (le pêne) poussée dans une ouverture dans le montant fixe (la gâche) pour sécuriser les portes et ainsi contrôler l'accès. L'invention du verrou a été suivie par celle de la serrure. Le verrou étant facilement manipulable, ils ont eu l'idée de bloquer celui-ci par une cheville mobile en bois : c'est la naissance de la serrure. Pour déverrouiller cette cheville, on fabriqua un outil comportant une dent (tige de fer) qui permettait de soulever la cheville. Puis, par déduction, on comprit alors que si cette tige avait plusieurs dents, elle pourrait soulever plusieurs tiges : c'est la naissance de la clé [7].

Plus les techniques se sophistiquaient, plus était rude l'accès pour un individu mal intentionné ou non autorisé.

La révolution technologique que nous avons connu dans le siècle dernier et l'apparition des cartes électroniques vers les années 1950, ont poussé encore loin la sophistication et la complexification des systèmes de contrôle d'accès physique ; avec l'apparition de nouvelles technologies des systèmes de contrôle d'accès comme les cartes à puces sans contact (badge RFID).

Ce mémoire s'inscrit dans le cadre du contrôle d'accès physique. De nos jours, il existe plusieurs solutions pour le contrôle d'accès physique comme les systèmes électroniques basés sur les cartes sans contact ou encore la biométrie.

Néanmoins la solution proposée dans ce mémoire s'oriente vers la conception d'une carte d'accès connectée basée sur la technologie RFID (cartes sans contact). L'objectif est de contrôler l'accès aux salles de cours suivant un emploi du temps, cela permettra de garantir l'intégrité de l'emploi du temps tant pour les salles que pour les horaires. La solution proposée dans ce mémoire est couplée à une application web faisant office d'intergiciel de suivi et de gestion centralisée des accès que nous avons nommé gateSecurAccess permettant le suivi des accès. Elle permettra un audit en temps réel des salles permettant de savoir qui est entré où et quand, d'avoir des informations sur l'état de chaque salle (attente, occupée ou libre) et sur la personne occupant la salle.

Le présent mémoire est hiérarchisé sur quatre chapitres. Une première partie propose une étude des systèmes de contrôle d'accès physique en présentant leurs caractéristiques et fondements. Une deuxième partie propose des généralités sur la technologie RFID. La troisième partie porte sur la réalisation pratique du mémoire à savoir la réalisation de la carte d'accès et de l'application web. Une dernière et quatrième partie proposant des tests de fonctionnements et une implémentation sur maquette.

Chapitre I : Le contrôle d'accès

I.1 Introduction

Ce premier chapitre portera sur une étude théorique des systèmes de contrôle d'accès physique en générale tout en restant focaliser sur la solution des cartes sans contact. Il traitera des fondements et caractéristiques d'un système de contrôle d'accès physique.

I.2 Définition du contrôle d'accès physique

Le contrôle d'accès physique désigne les différentes solutions techniques qui permettent de sécuriser, de contrôler et de gérer les accès à un bâtiment, un local ou un site [1][2].

I.3 Fondements du contrôle d'accès physique

I.3.1 Systèmes de contrôle d'accès physique

Lorsque nous parlons d'un système de contrôle d'accès physique nous faisons généralement référence à un système de sécurité électronique. Ainsi ils permettent de créer, de gérer et de surveiller des droits d'accès. Ils gèrent l'identification des autorisations, l'authentification, l'approbation des accès et la responsabilité des entités grâce à des identifiants, notamment des mots de passe, des codes PIN, des analyses biométriques et des clés physiques ou électroniques. Et, comme ils sont capables d'enregistrer qui est entré où et quand, ils peuvent fournir par la suite des données précieuses pour le suivi et l'utilisation du local ou du bâtiment [3][4].

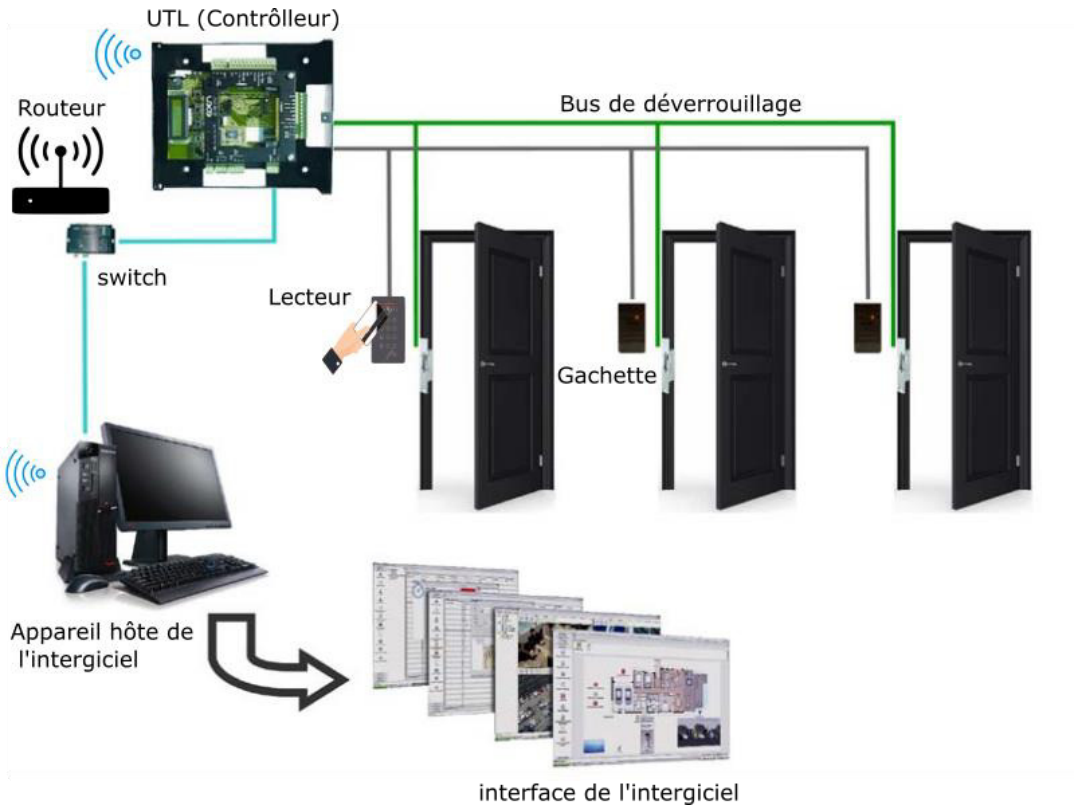


Figure 1. 1 : Système de contrôle d'accès basée sur carte sans contact

I.3.2 Techniques de contrôle d'accès physique

Les techniques de contrôle d'accès physique sont basées sur les critères suivants :

- Ce que l'on sait : un code PIN ou un mot de passe ;
- Ce que l'on possède : comme une carte, un badge d'accès ou tout autre type d'étiquette d'identification ;
- Ce que l'on est : il s'agit de données biométriques comme l'empreinte digital, l'iris.

Ou une combinaison de ces trois critères. Chaque méthode d'identification présente des avantages et des inconvénients, de sorte à ce que la méthode à choisir dépend de la situation. La combinaison de deux ou plus de critères augmente le niveau de sécurité, c'est ce que l'on appelle la vérification : une méthode pour s'identifier et une autre pour valider l'identité. Par exemple, la personne peut présenter son badge pour s'identifier et un code PIN ou son empreinte digitale lui sera demandé pour la validation [3][5].

I.3.3 Fonctions d'un système de contrôle d'accès

Un système de contrôle d'accès physique assure trois fonctions primaires [5] :

- L'identification et l'authentification ;
- Le traitement des données ;
- Le déverrouillage.

Ces fonctions sont assurées en chaque point où l'accès est contrôlé. L'image ci-dessous représente le schéma fonctionnel d'un système de contrôle d'accès physique

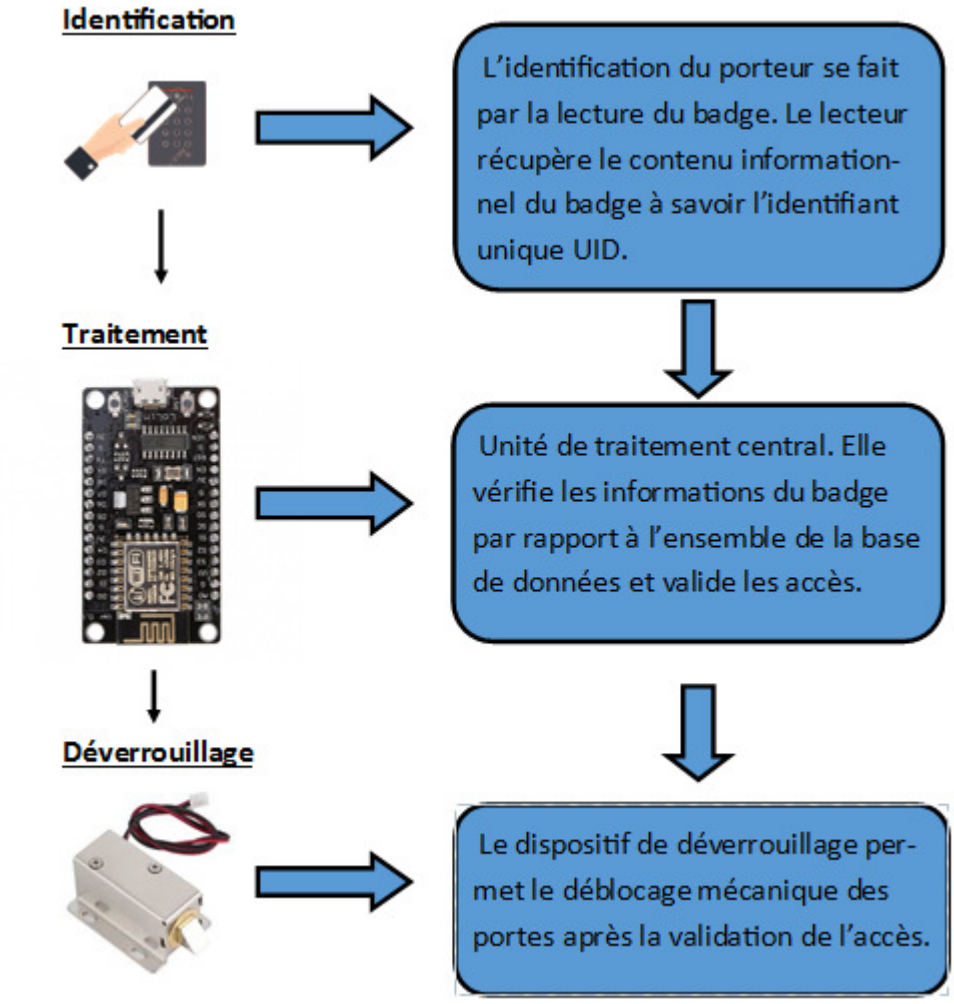


Figure 1. 2 : Schéma fonctionnel d'un système de contrôle d'accès

Dans le cas d'un système de contrôle d'accès utilisant des technologies sans contact, quatre éléments supports principaux interviennent :

- Le badge ;
- Le lecteur ;

- L'unité de traitement et de contrôle local ;
- Le serveur de gestion du système.

I.3.3.1 Phase d'identification et d'authentification

Tout d'abord il est important de définir les termes employés.

S'identifier, c'est le fait de communiquer son identité ;
S'authentifier, c'est apporter la preuve de son identité ;

Il est rappelé que l'identité d'un d'individu est l'ensemble des données de fait et de droit qui permettent d'individualiser une personne. Ainsi :

- La vérification de l'identité conduit à l'identification ;
- La preuve de l'identité conduit à l'authentification.

Dans le contexte des systèmes de contrôle d'accès physique et dans le cadre des technologies sans contact. La phase d'identification/d'authentification peut se réduire à l'identification du badge, ou à l'identification et l'authentification du badge seulement.

a. Identification

Dans un système reposant sur une technologie sans contact, l'identification est la présentation d'un badge à un lecteur.

b. Authentification du badge

L'authentification consiste à prouver qu'il est valide. Pour un système de contrôle d'accès reposant sur les cartes sans contact, l'authentification du badge se fait le plus souvent par échange cryptographique permettant au badge de prouver qu'il détient des éléments secrets sans les révélés.

c. Authentification du porteur

Le badge étant préalablement authentifié, il s'agit pour le porteur du badge de prouver qu'il est le détenteur légitime. L'authentification du porteur se fait par l'usage d'un second élément sélectionné parmi « ce que l'on est et ce que l'on sait ». Elle se fait par exemple par la saisie d'un mot de passe ou par l'usage de la biométrie.

I.3.3.2 Traitement des données

Le traitement des données est assuré en premier lieu par l'unité de traitement et de contrôle local (UTL). Cette unité assure la gestion de toutes les demandes d'accès, compare ces demandes par rapport à un ensemble de droit d'accès stockés dans sa base de données et délivre les commandes de libération des verrouillages.

I.3.3.3 Verrouillage et déverrouillage

Le dispositif de verrouillage permet de réaliser le blocage mécanique du point d'accès pour empêcher le passage des personnes non autorisées. Le contrôle d'accès autorise le déverrouillage.

I.4 Solutions de contrôle d'accès physique

Des solutions de contrôle d'accès physiques peuvent être, par exemple :

- Lecteur de proximité(badge) ;
- Clavier à codes ;
- Lecteur biométrique ;
- Serrure classique ;
- Cadenas ;
- Interphone et interphone ;

Nous pouvons regrouper ces solutions en deux catégories, les solutions classiques et les solutions à niveau de sécurité élevé.

I.4.1 Solutions classiques

I.4.1.1 La serrure classique

La serrure est un mécanisme de fermeture qui ne peut être ouvert que par une clef ou une combinaison correspondante. Ils existent différents types de serrures :

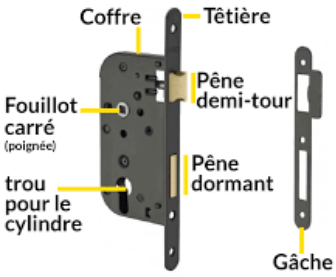


Figure 1. 3 : Mécanisme d'une serrure classique

- La serrure à garnitures
- La serrure à gorges ;
- La serrure à goupilles ;
- La serrure tubulaire ;
- La serrure à pompe ;
- La serrure à crémone ;
- La serrure biométrique ;
- La serrure à secret [7].

I.4.1.2 Le cadenas

Un cadenas est un objet qui permet de verrouiller une porte ou de boucler une chaine il se compose d'un boitier dans lequel se trouve un mécanisme de serrure et d'un anneau métallique qui peut être ouvert ou fermé. Le mécanisme est commandé par une clef, soit par un système de roues chiffrées

Ils existent différents modèles de cadenas : cadenas à anse pivotante, cadenas à anse coulissante et cadenas mono-point.

Un cadenas de haute sécurité est un cadenas composé d'acier trempé, de matière blindée, avec ou sans protecteur d'anse, non perçable, non crochetable et livré avec une carte de propriété brevetée [8].

Figure 1. 4 : Cadenas

I.4.2 Solutions à niveau de sécurité élevé

I.4.2.1 Clavier à code

Un clavier à code est un clavier de sécurité pour saisir un code de sécurité, par exemple pour ouvrir une porte [9]. En tapant un code sur un clavier à code, autrement appelé « Digicode », chaque utilisateur franchit le contrôle d'accès. La personnalisation des codes et des privilèges sur un clavier est possible dans une certaine mesure [9][10].

Figure 1. 5 : Clavier à code

On trouve plusieurs types de clavier à code :

- Clavier codé DK85 : il est indépendant à double sortie, les codes sont mémorisés dans une EPROM (Erasable programmable Read Only Memory) permettant la sauvegarde lors de coupure d'alimentation ;
- Clavier codé DK85BL : il est indépendant à double sortie à rétroéclairage, les codes sont mémorisés dans une EPROM ;
- Clavier étanche DK9610 ;

- Clavier à clé DK80 ;
- Clavier étanche anti-vandale SU-N ;
- Clavier anti vandale SU2TM ;
- Clavier et lecteur de proximité SU2PM.

I.4.2.2 Le lecteur biométrique

Ce type de contrôle d'accès s'appuie sur la biométrie.

Figure 1. 6 : Lecteur d'empreinte digitale

I.4.2.2.1 Biométrie

Le mot biométrie signifie littéralement (mesure du vivant) et désigne dans un sens très large l'étude quantitative des êtres vivant.

L'usage de ce terme se rapporte de plus en plus à l'usage de ces techniques à des fins de reconnaissance, d'authentification et d'identification.

La biométrie est la vérification de l'identité d'un individu par ce qu'il est c'est-à-dire en utilisant des caractéristiques physiques ou comportementales. Pour cela on effectue des analyses qui peuvent être : morphologique, comportementale, voir même biologique [11].

I.4.2.2.2 Analyse morphologique

L'analyse morphologique peut se pratiquer avec :

- Les empreintes digitales : une empreinte digitale est le dessin formé par les lignes de la peau des doigts, des paumes des mains, des orteils ou de la plante des pieds. Une empreinte complète contient en moyenne une centaine de points caractéristiques mais les contrôle ne sont effectués qu'à partir de 12 points. Il est

quasiment impossible de trouver deux individus présentant 12 points caractéristiques identiques, même dans une population de plusieurs millions de personnes [11].

Figure 1. 7 : Technologie d'empreinte digitale

- La reconnaissance de l'iris : se base sur l'observation de l'iris (contour et texture de l'iris, dilatation des pupilles) [11].

Figure 1. 8 : Iris d'un œil

- Les réseaux veineux de la rétine : la lecture des caractéristiques de la rétine est une technologie utilisée pour des applications de sécurité très élevée, par exemple dans des applications militaires ou nucléaires. Les caractéristiques de la rétine sont liées à la configuration géométrique des vaisseaux sanguins [11][12].

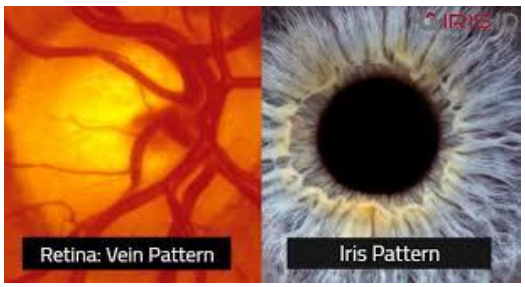


Figure 1. 9 : Réseaux veineux de la rétine

- Les réseaux veineux de la paume de la main

- La morphologie de la main
- La reconnaissance de visage : se base sur les caractéristiques faciales en effectuant des mesures (écartement des yeux, arêtes du nez, commissures des lèvres, oreilles, menton) [11][12].

Figure 1. 10 : Technologie de reconnaissance faciale

I.4.2.2.3 Analyse comportementale

Un individu possède plusieurs éléments liés à son comportement qui lui sont propre [11] :

- Dynamique des frappes au clavier : pour identifier une personne grâce à son style de frappe, en effectuant des mesures de paramètres comme le temps de pression sur chaque touche, le temps de relâchement, le temps de vol entre deux touches, ou encore le nombre de doigts utilisés.
- Reconnaissance vocale : utilise les données liées à la voie. Ces caractéristiques de la parole sont constituées par une combinaison de facteurs comportementaux (vitesse, rythme, etc…) et physiologiques (tonalité, âge, sexe, fréquence, accent, harmoniques…).

Figure 1. 11 : Technologie de reconnaissance vocale

- Dynamiques des signatures : se base sur la mesure de plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total etc. pour pouvoir identifier la personne.

Figure 1. 12 : Technologie de reconnaissance de signature

- La démarche de la personne

I.4.2.2.4 Analyse biologique

Elle fait recours aux analyses biologiques (odeur, groupe sanguin, salive, urine test ADN) [11].

I.4.2.3 Interphone et vidéophone

Un interphone en anglais (intercom) est un téléphone qui utilise un réseau interne ; il n'est donc pas connecté au réseau téléphonique, il est souvent équipé d'un haut-parleur et permet des communications sur de courtes distances, en général à l'intérieur d'un même bâtiment. Il peut notamment être placé à l'entrée d'un immeuble afin d'en contrôler l'accès. Il est souvent équipé d'un système permettant l'ouverture d'une porte à distance, appelé (portier) [13].

Le visiophone est l'association de la téléphonie et de la télévision permettant ainsi aux interlocuteurs de se voir, cela ajoute un niveau de sécurité supplémentaire au contrôle d'accès par cette méthode car il permet de voir la personne souhaitant avoir l'accès donc de l'identifier [14].

Figure 1. 13 : Interphone

Figure 1. 14 : Vidéophone

I.4.2.4 Lecteur de proximité ou badge

Un lecteur de proximité est un dispositif permettant la lecture d'une puce RFID à distance. Ce terme peut être associé à des applications de :

- Sécurité électronique (**contrôle d'accès**, identification sur un système électronique ou informatique) ;
- Suivi de stock /inventaire ;
- Antivol ;

Figure 1. 15 : Badge d'accès de chez Mifare

Avec ce type de contrôle d'accès, un badge est fourni à chaque utilisateur, pour avoir l'accès il faut présenter devant un lecteur fixe son badge. En approchant le badge à la borne, le lecteur détecte le badge individualisé et autorise l'accès.

Ce type de lecteur est capable de mémoriser les évènements : qui a accédé et quand. Un des avantages de ce système est sa simplicité d'utilisation et de paramétrage : un nouveau badge, un nouveau privilège, une nouvelle suppression se font en quelques clics. Nous développerons plus en détail cette partie dans le chapitre suivant car c'est l'élément central du thème de ce mémoire de fin d'étude [10][15].

I.5 Critères de choix d'un système de contrôle d'accès

L'abondance de dispositif de système de contrôle d'accès pose un inconvénient : celui de rendre le choix du meilleur système significativement plus complexe ; pour cela il faut se référer à certains critères.

- L'installation est-elle simple et économique ;
- Faut-il prévoir des coûts considérables ;
- Quelles sont les entreprises qui fournissent ce genre d'appareil ou dispositif ;
- Où trouver des informations sur les coûts et les tarifs de dispositif de contrôle d'accès ;
- La facilité de la documentation sur le dispositif ;
- La fiabilité ;
- La flexibilité ;
- Le niveau de sécurité ;

I.6 Pourquoi utiliser un système de contrôle d'accès plutôt qu'une clé

Les clés physiques sont la forme la plus simple de contrôle d'accès physique et la méthode utilisée par de nombreuses organismes. Cependant même pour une petite structure l'utilisation de clé mécanique présente plusieurs défauts et limites [3][16].

I.6.1 Inconvénients liés à l'utilisation de clé mécanique

- Les gens perdent leurs clés : si quelqu'un perd sa clé, il faut remplacer la serrure pour s'assurer que la clé perdue ne puisse être utilisée à de mauvais escients. Il

faut ensuite distribuer de nouvelles clés à toutes les personnes qui ont besoin d'accéder à cette porte.

- Les clés ne laissent pas de traces d'audit : il ne sera pas possible de savoir qui a utilisé une clé, où il est entré et à quelle heure.
- Les clés sont difficiles à gérer : si une personne doit entrer dans plusieurs salles il lui faut un grand nombre de clés qui ne sont pas pratiques à transporter et à utiliser. Il peut être difficile de se rappeler quelles clés correspond quelles portes et il est risqué de les étiqueter
- Le niveau de sécurité laisse à désirer car les clés sont facilement reproductibles : il est facile d'en faire des copies [3][16].

I.6.2 Avantages des systèmes de contrôle d'accès

Avec un dispositif de contrôle d'accès nous aurons : un renforcement de la sécurité.

- Qui a accès ;
- Quelles sont les portes auxquelles ils ont accès ;
- A quelle heure ils peuvent accéder ;
- Dans quelles conditions ils sont autorisés d'accéder [3].

I.7 Conclusion

La sécurité des biens et des données étant une question préoccupante pour tous organismes (entreprises, établissements publics, résidences collectives ou privées). Le contrôle d'accès devient un outil incontournable pour gérer la question de sécurisation de biens et de données. Du plus simple (serrure classique, cadenas) aux plus complexes (système biométrique, badge), ces systèmes ou techniques n'ont cessé de facilité le quotidien des structures qui les utilisent. Ces techniques ou technologies ne cessent d'évoluer avec les progrès technologiques grandissantes auxquelles nous assistons ces dernières années rendant certains des systèmes de contrôle d'accès presque infaillible. Outre tous ces systèmes nous nous concentrerons sur les cartes à puces sans contact (badge RFID), qui feront l'objet de développement dans le chapitre suivant.

Chapitre II : La technologie RFID

II.1 Introduction

La RFID n'est pas une nouvelle technologie. Elle fait son apparition pour la première fois durant la seconde guerre mondiale lorsque « ROBERT WATSON-WATT » développe une application pour l'armée britannique pour identifier les avions qui entraient dans l'espace aérien britannique afin de différencier les avions ennemis de ceux des alliés : c'est le système d'identification IFF « identification friend or foe » qui reste le principe de base utilisé de nos jours pour le control du trafic aérien [17].

Jusqu'aux années 70, l'utilisation de la technologie RFID reste assez confidentielle. Elle est principalement utilisée par l'armé pour contrôler les accès des sites sensibles, comme le nucléaire

Dans les années 80-90, avec notamment les avancées technologiques du tag passif, la RFID se repend peu à peu dans le civil (pour l'identification du bétail ou encore dans les chaines de fabrication des constructions automobiles), jusqu'à connaitre un véritable essor dans les années 2000.

On trouve de nos jours les technologies RFID dans la plupart des secteurs industriels (aéronautique, agroalimentaire, transport, sécurité, santé…). Mais aussi sans toujours le savoir dans notre quotidien (cartes de transport, étiquettes antivols, clés sans contact pour le contrôle d'accès, badges autoroutes…).

Ce chapitre traitera d'une étude générale des RFID.

II.2 Définition de la RFID

La radio-identification appelée RFID « Radio Frequency Identification », est l'ensemble des techniques et méthodes permettant d'échanger des données à distance à l'aide d'onde électromagnétique en utilisant des transpondeurs (tag RFID).

II.3 Principe de la RFID

La technologie RFID se base sur les ondes électromagnétiques. Elle est composée de deux entités qui communiquent entre elles :

- Un transpondeur (tag RFID). Celui contient les données numériques utilisées pour l'identification. Les données du tag peuvent être lues sans ligne de vue

directe. Le transpondeur est détectable à des distances relativement grandes mais dépend du type de puce.

- D'une station de base (lecteur RFID ou encore interrogateur).
- Un intergiciel ou application hôte permettant la collecte, le stockage et le traitement des données issues de la station de base.

Le principe étant basé sur l'émission d'onde électromagnétique, la station de base (lecteur) émet un signal électromagnétique. Ce signal est détectable par les étiquettes (tag RFID) se trouvant dans son champ de lecture. Une fois activée, un dialogue s'établie entre l'étiquette et la station de base selon un protocole de communication défini et des données sont échangées [17].

Le principe d'identification repose sur le fait que chaque transpondeur (étiquette) possède son identifiant unique UID (Unique Identifiant) et qui est stocké en zone mémoire à lecture seule.

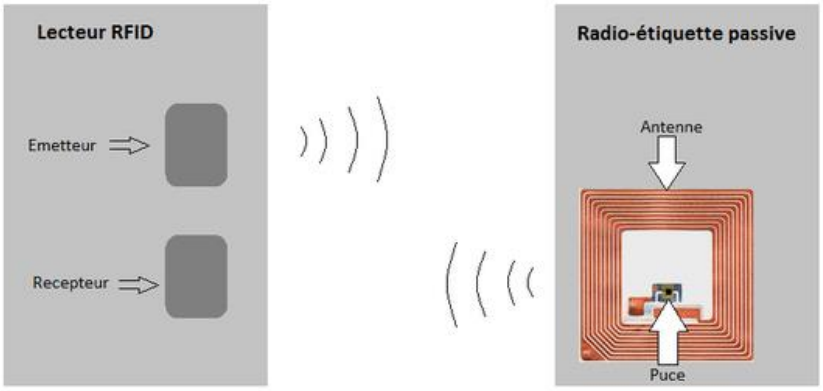


Figure 2. 1 : principe de fonctionnement de la RFID

II.4 Les composants d'un système RFID

Une application RFID comprend les étiquettes (tag), les lecteurs (station de base) ou enregistreurs et un intergiciel pour la collecte et le traitement des informations.

II.4.1 Le tag (étiquette)

Le transpondeur ou tag RFID contient les informations (par exemple l'identifiant unique UID pour le contrôle d'accès) utilisées pour l'identification de la personne ou

de l'objet qui le porte. Il se compose d'une puce électronique qui stocke des données et d'une antenne pour la transmission de l'information vers le lecteur par ondes électromagnétiques, le tout encapsulé dans un substrat ou support.

La capacité d'information d'une étiquette RFID est de l'ordre de 2kB, mais la plupart ne contient qu'un numéro d'identification de 32 à 128 bits.

Son principe est le suivant, il répond à la requête de l'interrogateur (signal d'interrogation du lecteur). L'une des réponses les plus simples possibles est le renvoie d'un numéro d'identification UID, par exemple celui du standard EPC-96 qui utilise le 96 bits (EPC pour Electrical Product Code) [17].

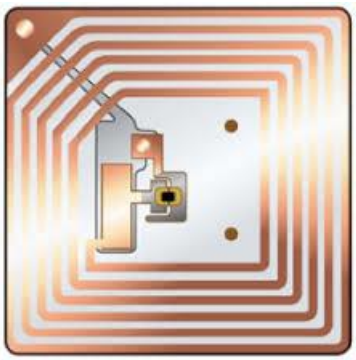


Figure 2. 2 : Structure interne d'un tag

II.4.1.1 Classification des tags (transpondeur)

Les tags RFID peuvent être classés en fonction de leur mode d'alimentation, de leurs propriétés en lecture/écriture (mode de fonctionnement) et selon la technologie du support.

II.4.1.1.1 Mode d'alimentation

Nous distinguons trois types de tags selon leur mode d'alimentation à savoir : le tag passif, le tag semi-passif ou semi-actif et le tag actif [17].

a. Tags passifs

Ils ne disposent pas de source d'alimentation externe (sans batterie ni piles), les tags passifs sont alimentés par l'énergie des ondes électromagnétiques issues du signal d'interrogation du lecteur.

b. Tags semi-passifs (semi-actifs)

Les tags semi-passif ou encore BAP (Batterie-Assisted Passive Tag, en français marqueurs passifs assistés par batterie), sont alimentés à l'aide d'une petite batterie ou pile. Ils utilisent également l'énergie du lecteur pour répondre à une requête de celui-ci.

Ces tags sont robustes et plus rapide en lecture et en transmission que les tags passifs mais sont aussi plus chers.

c. Tags actifs

A des fréquences élevées et en particulier à partir de 2,45 GHz, il devient difficile d'alimenter le tag à partir de l'énergie issue du rayonnement du lecteur, car la puissance d'émission requise pour alimenter le transpondeur devient trop forte, comme c'est le cas des systèmes de péages autoroutier qui opèrent de plus en plus dans les bandes DSRC (Dedicated Short Range Communications) à 5,8 ou 5,9 GHz.

Il devient indispensable d'utiliser une batterie embarquée. Du fait qu'ils sont équipés d'une batterie, cela leur permet d'émettre des signaux, ils peuvent être lu à une plus grande distance (100 m environ). Ils sont plus coûteux que les autres tags (passifs et semi-passif) [27].

d. Remarque

Les étiquettes sans puce font leur apparition. Ils ne disposent pas de puces électroniques dans le transpondeur. C'est l'impression de l'étiquette basée sur des principes physiques ou chimiques, qui engendre un identifiant unique. Ne coûtant pas cher, elles peuvent être une alternative aux codes-barres. Un exemple de t'étiquette sans puce est le tag SAW (Surface acoustic Wave, onde acoustique de surface) [17].

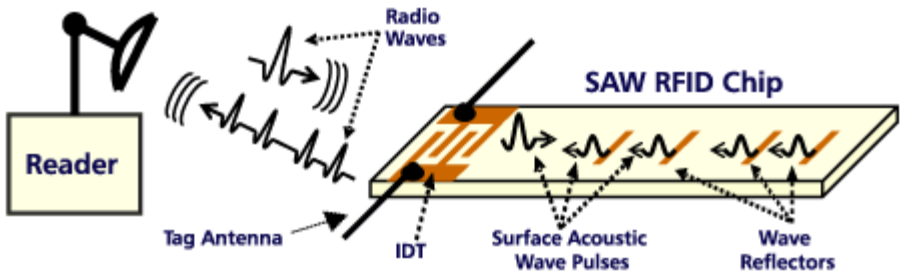


Figure 2. 3 : Etiquette RFID utilisant la technologie SAW

II.4.1.1.2 Mode de fonctionnement (propriété de lecture/écriture)

Nous distinguons trois types d'étiquettes (tags) selon le mode écriture/lecture à savoir : les étiquettes en lecture seule, en écriture une fois et lecture multiple et enfin en lecture/écriture multiples. L'information peut être stockée de deux manières :

- Soit on mémorise un pointeur (une clé d'accès) dans l'étiquette, en indiquant un chemin vers une base de données où trouver cette information nécessaire au traitement : l'application est dite centralisée.
- Soit l'information est mémorisée dans l'étiquette : l'application est dite décentralisée.

Les étiquettes à lecture seule permettent la réalisation de système appartenant à la première catégorie : systèmes centralisés.

Les étiquettes à écriture unique et lecture multiple permettent la réalisation de systèmes pouvant appartenir aux deux catégories : systèmes centralisés ou décentralisés.

Les étiquettes à écriture et lecture multiples permettent plus spécifiquement la réalisation de systèmes appartenant à la deuxième catégorie : systèmes décentralisés [6].

a. Lecture seule

Il est uniquement possible de lire l'étiquette. Les données sont préalablement inscrites dans l'étiquette par le fabricant, et ne peuvent pas être modifiées ni complétées par la suite.

b. Ecriture une fois, lecture plusieurs fois

L'étiquette est fournie à l'utilisateur vierge. Dans la majorité des cas le fournisseur l'a déjà équipé d'un numéro d'identification. Lors de sa mise en place sur l'objet à tracer, l'utilisateur peut y inscrire des informations qui lui seront utiles par la suite. Ces informations pourront être lues mais ne pourront pas être modifiées ni complétées par suite. On les appelle également WORM (Write Once Read Multiple).

c. Lecture et écriture multiple

L'étiquette est fournie vierge dans les mêmes conditions que les WORM, mais elle pourra être écrite, modifiée, complétée et lue plusieurs fois. Le nombre de répétition de ces opérations peut dépasser 500 000. L'objectif est la réutilisation de l'étiquette et ou la mise à jour de son contenu.

II.4.1.1.3 La technologie du support (substrat)

- La première catégorie de transpondeur est la plus classique. Il s'agit de tags simples, dont l'antenne de cuivre est disposée en carré ou circulaire et plate. La partie interne représente la puce, qui constitue le cœur du transpondeur. Ici les tags peuvent être contenus dans des films plastiques transparents, dans des polymères, dans des bracelets, dans des portes clés ou dans des badges.

Figure 2. 4 : Tag RFID en porte clé

- Le second type de transpondeur s'apparente à un croisement entre les tags et les codes-barres. Ce sont en fait des étiquettes (souvent autocollantes) contenant un tag RFID et un code-barre sur une de ses faces.

Figure 2. 5 : Combinaison étiquette RFID et code à barres

- La troisième et dernière catégorie de transpondeur est une gamme coûteuse et destinée à des usages spécifiques. Ici les tags sont composés d'une antenne en bobine de cuivre cylindrique et son enfermés dans des capsules de verre. Cette catégorie de tag est destinée à l'implantation sous-cutané, pour l'identification animalière.

Figure 2. 6 : Etiquette RFID pour l'implantation cutanée

II.4.1.2 Avantages et contraintes des étiquettes RFID

II.4.1.2.1 Avantages des étiquettes RFID (tags)

Les avantages des étiquettes radios par rapport aux codes à barres sont :

- La capacité de mise à jour du contenu ;
- Une plus grande capacité de contenu ;
- La vitesse de marquage ;
- Une sécurité d'accès au contenu ;
- Une plus grande durée de vie ;
- Une plus grande souplesse de positionnement ;
- Une meilleure protection aux conditions environnementales.

II.4.1.2.2 Les contraintes des étiquettes radiofréquences (tags)

Les avantages décrits plus hauts ne vont pas sans contraintes :

- Le coût ;
- La perturbation par l'environnement physique ;
- Les perturbations induites par les étiquettes entre elles ;
- La sensibilité aux ondes magnétiques parasites.

II.4.2 Le lecteur (interrogateur)

Le lecteur est l'élément qui coordonne la communication dans une application RFID, il assure la télé-alimentation des tags dans le cas des tags passifs. Il est composé d'un module radio fréquence pour la transmission et la réception, d'une unité de contrôle (microcontrôleur), et d'une interface pour transmettre les données vers un terminal.

La communication entre le lecteur et les étiquettes s'effectue en quatre temps [6] :

- Le lecteur transmet par onde électromagnétique l'énergie nécessaire pour activer les tags ;
- Il lance une requête interrogeant les étiquettes se trouvant dans son voisinage ;
- Il écoute les réponses et élimine les doublons ou les collisions entre réponses ;
- Et pour finir, il envoie les résultats obtenus aux applications concernées.

Figure 2. 7 : Lecteur de badge

II.4.2.1 Les différents types de lecteur

Les lecteurs peuvent être de différents types, on peut distinguer :

- Les lecteurs mobiles : sont généralement montés sur les chariots élévateurs, offrent une mobilité et une flexibilité accrues dans les applications de type gestion d'entrepôt ;
- Les lecteurs fixes : servent majoritairement dans les configurations de types portiques ou convoyeurs ;
- Les lecteurs portatifs : sont en général utilisés dans les applications de recherche et localisation de produits dans les entrepôts et dont les antennes intégrées sont incorporées directement dans le dispositif [17].

Figure 2. 8 : Lecteur de badge portatif

II.4.3 L'intergiciel (middleware)

Un middleware est un ensemble de couches logicielles assurant l'interface entre plusieurs applications, qu'elles soient matérielles ou logicielles. Dans le cas des applications RFID, le middleware assurera l'interface entre les données collectée sur le terrain (contenues dans la mémoire des tags RFID) et le logiciel de gestion de l'entreprise ou de la structure exploitant ces données. Quelque soit l'application RFID, une couche logicielle est nécessaire pour interfacer les modules de gestion de la structure avec les données issues des tags RFID. Elle peut faire l'objet d'un développement spécifique, ou peut être sélectionnée parmi les solutions « prêt à l'emploi » présentes sur le marché. Un développement spécifique peut parfois s'avérer pertinent notamment en cas de projet à petite échelle, où les solutions du marché peuvent être surdimensionnées.

La fonctionnalité minimum d'un middleware étant de communiquer avec les équipements de capture de données (lecteur RFID), d'autres caractéristiques plus étendues peuvent être proposées par les produits sur le marché. On peut citer notamment :

- Une gestion plus poussée des lecteurs RFID : paramétrage RF, définitions d'alertes ;
- Une gestion des tags RFID déployés : lecture, écriture, formatage ;
- Une gestion des données issues d'autres technologies : code à barres, réseaux de capteurs ;
- Une gestion directe de processus métiers « matures en RFID : logistique et chaîne d'approvisionnement, production et contrôle de qualité, traçabilité des produits et maintenance, contrôle d'accès et suivi des personnes, cartes de fidélités et de paiements.

On peut classer les fonctionnalités principales des middleware RFID du marché en 5 catégories :

- Catégorie 1 : fonctionnalités natives de la gestion des technologies RFID ;
- Catégorie 2 : fonctionnalités de gestion des tags ;
- Catégorie 3 : fonctionnalités de traitement de données contenues dans les tags ;
- Catégorie 4 : fonctionnalités de gestion de processus métiers ;
- Catégorie 5 : fonctionnalités de gestion de postes de travail pour les opérateurs finaux.

II.5 Fréquences utilisées

La fréquence est la caractéristique qui permet d'établir la communication entre la puce et l'antenne. Cette fréquence est variable selon le type d'applications visées et les performances recherchées [17].

Le lecteur et le tag sont équipés d'antenne et doivent par conséquent s'adapter à l'environnement. De plus la RFID doit coexister d'un point de vue spectral avec d'autres technologies sans fil et doit donc s'assurer à ne pas perturber le fonctionnement

de celles-ci. Aussi les fréquences utilisées sont contraintes par les données réglementaires, qui sont spécifiques selon chaque pays, à savoir la puissance de rayonnement autorisée. La solution est donc en général d'utiliser les fréquences ouvertes à tous, c'est-à-dire celles réservées aux applications industrielles, scientifiques et médicales appelées bandes ISM (Industriel-Scientifique-Medical) [27].

Fréquence	Vitesse	Distance	Informations
Basses fréquences			
125 kHz	< 10 kb/s	Jusqu'à 1m	
134,2 kHz			Charge du transpondeur
Haute fréquence			
13,56 MHz	< 100kb/s	Limitation de puissance autorisée	ISO 14443A 1-4, ISO 14443B 1-4, ISO 15693-3, ISO 18000-3, …
Ultra hautes fréquences			
915 MHz	< 200 kb/s	Jusqu'à 5-7m	Etats-Unis
865 - 868 MHz			Union Européenne
2,45 – 5,8 GHz	< 200 kb/s	Jusqu'à 10m	Micro-ondes

Figure 2. 9 : Fréquences d'utilisation autorisées pour la technologie RFID

II.6 Conclusion :

Dans ce chapitre, nous avons fait une étude de vue générale sur la technologie des cartes sans contacts « RFID ». En décrivant son principe de fonctionnement, les différentes composantes (tag, lecteur, intergiciel) d'un tel système, ses caractéristiques, ses avantages et ses inconvénients et aussi les fréquences autorisées par les réglementations des différents pays. Dans le chapitre suivant, nous nous concentrerons sur les réalisations pratiques du mémoire.

Chapitre III : Réalisation de la carte d'accès et de l'application web

III.1 Introduction

Dans les chapitres précédents nous avons abordé des notions relatives aux contrôle d'accès physique et à la technologie RFID dans un but d'introduction pour mieux aborder ce chapitre.

Dans ce chapitre nous allons nous concentrer sur la réalisation pratique du mémoire, pour rappel l'objectif de ce travail est de réaliser un système de gestion intelligente et de contrôle de l'accès par RFID aux salles de cours suivant un emploi du temps, à savoir la réalisation de la carte d'accès et de l'application web de gestion des salles. Ainsi il sera divisé en deux parties :

- Une première partie dédiée à la réalisation de la carte d'accès selon le cahier des charges établi ;
- Une deuxième partie pour l'application web de gestion des salles suivant un cahier des charges de fonctionnalités bien défini.

III.2 Partie A : La carte d'accès

III.2.1 Schéma synoptique du système

L'image ci-dessous Figure 3.1 représente le schéma synoptique du système. Il se compose de deux parties.

- La première partie représente la carte d'accès : elle assure la lecture et l'authentification des badges ainsi que la communication des informations d'accès avec l'application web ;
- La deuxième partie concerne l'application web gateSecurAccess pour le suivi des accès : elle permet de connaitre l'état de chaque salle ;
- Les deux parties communiquent par connexion wifi.

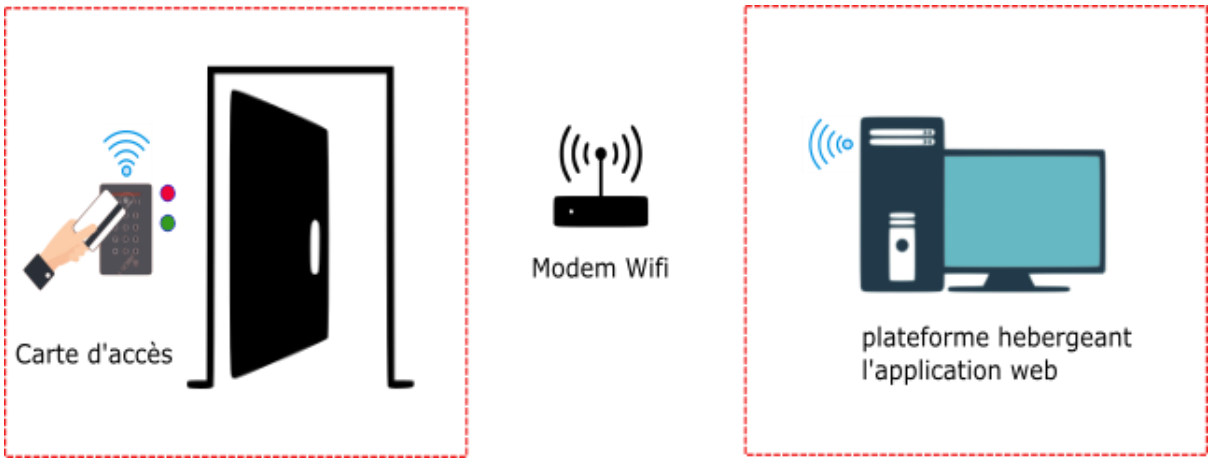


Figure 3. 1 : Schéma synoptique du système

III.2.2 Cahier des charges

Tout bon système nécessite un cahier des charges afin de répondre aux exigences souhaitées.

- Pour accéder à la salle, seuls les enseignants sont habilités ;
- L'accès se fait suivant un emploi du temps (jour et heure), une personne se présentant devant une salle dont il n'y figure pas dans l'emploi du temps suivant le jour et l'heure se verra se refuser l'accès ;
- Pour accéder à une salle, la personne concernée devra se présenter devant la porte avec son badge ;
- L'emploi du temps est défini au préalable et stocké dans la base de données du système (jour et heure pour chaque enseignant) ;
- Les informations (identifiant) de la carte sont associées à l'emploi du temps ;
- Si l'accès est validé une led verte s'allume sinon une led rouge ;
- Après chaque accès les informations devront être envoyées au site de gestion et stockées dans la base de données.

III.2.3 Les principaux composants électroniques

La liste ci-dessous regroupe l'ensemble des composants de base. Ces composants sont décrits dans l'annexe.

- Arduino nano ;
- Le module Wemos (ESP8266) D1 R2 à base d'Arduino uno ;

- Le solénoïde 12V ;
- La Carte RFID MFRC522 ;
- Le module d'horloge RTC DS1302 ;
- Des fils de connexions ;

III.2.4 Principe de fonctionnement du système

III.2.4.1 Schéma électrique du montage de la carte d'accès

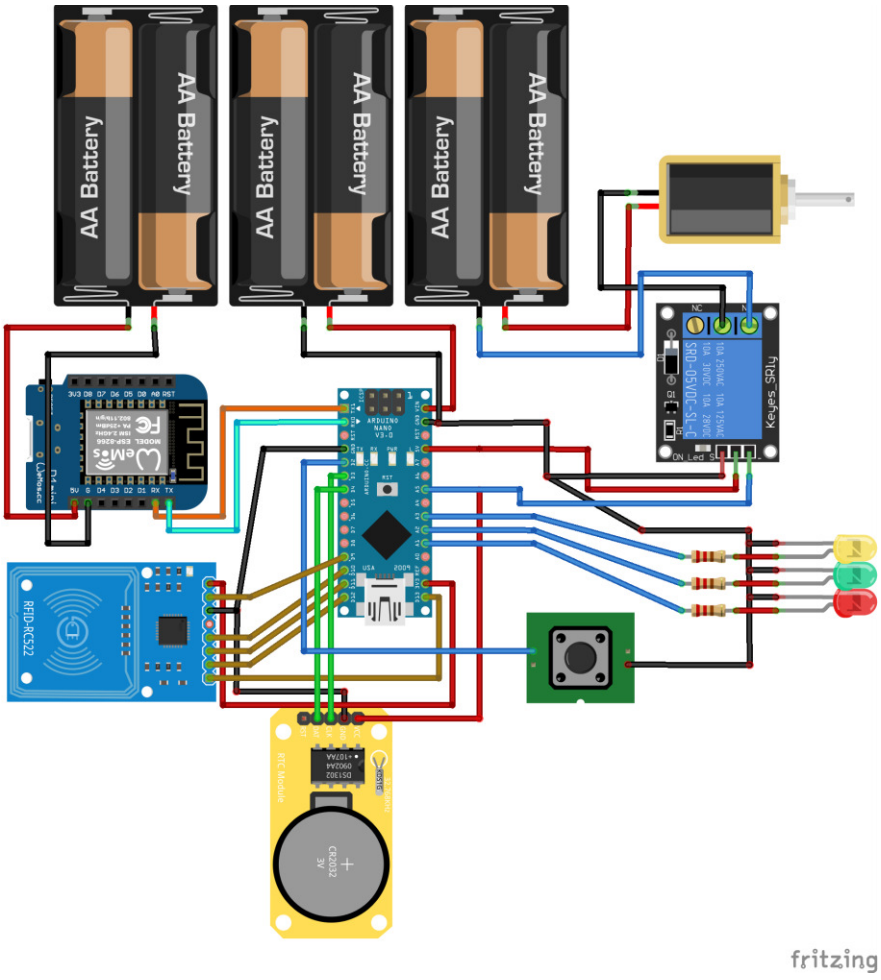


Figure 3. 2 : Schéma électrique du système

III.2.4.2 Principe du système

Le principe de fonctionnement se présente comme suit :

Le but étant de restreindre l'accès aux salles suivant l'emploi du temps des cours (jour et heure) et dont seuls les professeurs possèdent l'habilitation.

Pour accéder à la salle, l'enseignant se présente devant la salle avec son badge (tag RFID) qui contient un identifiant unique UID permettant son identification. Les informations de chaque tag (UID) sont stockées préalablement dans la base de données ici il s'agit de la mémoire interne de la carte Arduino et celle de l'application web. L'emploi du temps pour chaque jour ouvrable et horaire est également défini et stocké en mémoire. L'identifiant de chaque tag est associé à l'emploi du temps relatif à chaque enseignant. Une fois devant la porte, le système lit les informations du badge et récupère l'identifiant qui s'y trouve puis le compare aux identifiants qui sont déjà dans sa base de données.

Si l'identifiant existe, alors il récupère son index qui est l'indice de l'identifiant dans le tableau où sont stockés les identifiants, pour illustré voyons un cas concret :

Soit l'identifiant =1450 comme exemple de l'information lue par le système.
Tab_idenfiant= {1524 ; 4785 ; 1450 ; 7851 ; 7862} ;
Ici nous pouvons voir que l'identifiant lue correspond au troisième élément du tableau des identifiants alors c'est cet index qui est récupéré par le système. Cet index est associé à l'emploi du temps. Le système récupère également la date du jour et l'heure actuelle. Le système vérifie alors si dans le tableau des emplois du temps, il existe une section contenant l'index de l'identifiant et deux valeurs qui doivent correspondre à la date du jour et l'heure actuelle. Si ces trois informations sont correctes, alors le processus d'identification est validé et l'accès est autorisé. Une led verte s'allume pour confirmer l'autorisation. Un courant de 5V est délivré à travers une sortie numérique de la carte Arduino à un relais qui le transforme en 12V pour faire fonctionnement le solénoïde afin de débloquer la porte. L'identifiant du badge est envoyé à travers une connexion wifi à l'application web de gestion pour le suivi et la supervision par un administrateur et est également stocké dans une carte SD avec la date et l'heure d'accès au cas où il y aurait une coupure d'internet. Si l'identification échoue une led rouge s'allume pour signaler la personne.

III.2.4.3 Description des différents blocs

III.2.4.3.1 Bloc de la carte RFID

Le bloc « carte RFID » est la partie permettant l'identification à travers la lecture du tag RFID et ce en récupérant son UID. Il est composé principalement du module **MRF-RC522**. D'abord nous récupérons l'UID de chaque tag dans un petit programme afin de pouvoir leur faire des traitements (enregistrement sur la mémoire de la carte Arduino, comparaison lors de l'identification) dans le programme principal.

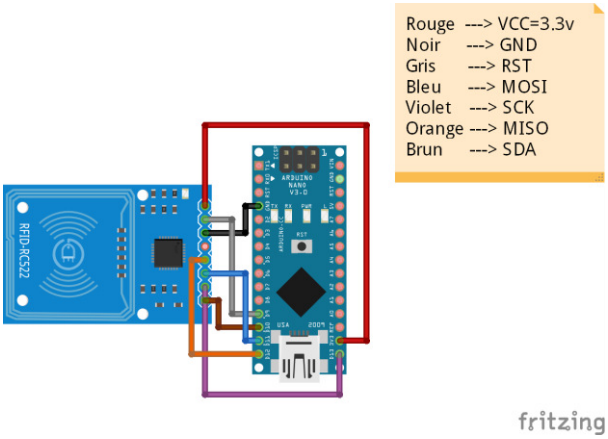


Figure 3. 3 : Schéma électrique de la carte de lecture du tag

III.2.4.3.2 Bloc du module d'horloge

Le bloc d'horloge est la partie du système qui permet d'avoir la date (jour et heure). Il est composé principalement d'un module RTC (**Real Time Clock**) à base du circuit intégré **DS1302** relié au microcontrôleur Arduino Nano. Le circuit intégré DS1302 est détaillé dans l'annexe. L'avantage de ce module est qu'il permet de garder la date une fois celle-ci définie et enregistrée, car le module dispose d'une petite pile de 3.3V ayant une durée de vie pouvant atteindre deux ans et demi. Pour pouvoir l'utiliser, il faut le bon « **driver** » à savoir la bibliothèque Arduino correspondante. Cette bibliothèque n'est pas disponible par défaut dans l'IDE d'Arduino il faut la télécharger sur internet.

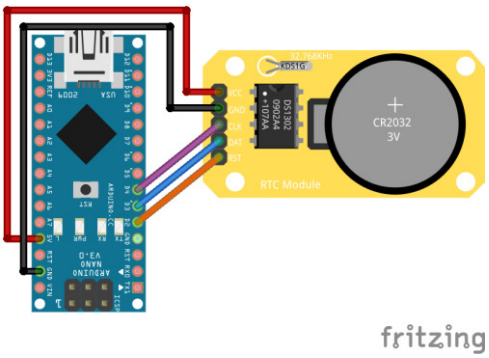


Figure 3. 4 : Schéma électrique du module d'horloge

```
Fichier  Édition  Croquis  Outils  Aide

DS1302_Serial_Easy §

#include <DS1302.h>
// Créer un objet rtc de la classe DS1302
DS1302 rtc(2, 3, 4);
void setup()
{
  Serial.begin(9600);
  // Initialisation du DS1302
  rtc.halt(false);
  rtc.writeProtect(false);

  rtc.setDOW(FRIDAY);        // On defini le jour de la semaine
  rtc.setTime(12, 0, 0);     // On defini l'heure (24hr format)
  rtc.setDate(6, 8, 2020);   // On defini la date ( 6 Août 2020)
}

void loop()
{}
```

Figure 3. 5 : Code d'initialisation du module d'horloge

III.2.4.3.3 Bloc Wifi

Le bloc Wifi est celui qui assure la transmission des données vers l'application web. Il se compose du module **Wemos ESP8266** relié à la carte Arduino par deux connexions. Cette connexion sert de support de communication entre les deux cartes. La communication s'effectue par voie série.

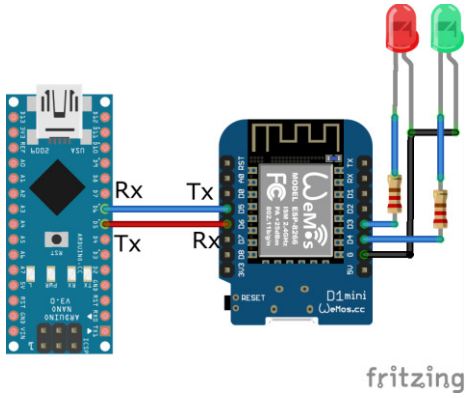


Figure 3. 6 : Schéma électrique du module wifi

III.2.4.3.4 Bloc de déverrouillage des portes (solénoïde)

Cette partie permet le déverrouillage des portes. Il est composé d'un relais, d'un solénoïde et d'une alimentation de 9-12V. Lorsque le système identifie la personne cherchant l'accès, un signal d'impulsion est envoyé sur l'entrée « **signal** » du relais. Cela permet d'activer le solénoïde et déverrouille la porte par l'occasion.

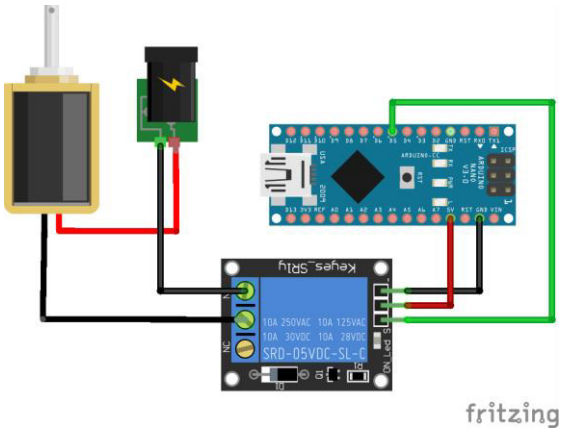


Figure 3. 7 : Schéma électrique du bloc de déverrouillage des portes

III.2.4.3.5 Bloc de déverrouillage interne (bouton poussoir)

Ce bloc se compose d'un bouton poussoir relié à la carte Arduino. Il permet de déverrouiller la porte de l'intérieur. Ce bouton est géré par interruption interne. Ainsi une action sur ce bouton permet de déclencher une routine d'interruption afin de gérer l'évènement conduisant donc au déverrouillage de la porte depuis l'intérieure de la salle

III.2.5 Organigrammes

Nous avons trois organigrammes : un organigramme pour la lecture et l'authentification des cartes, un organigramme pour le module wifi et un organigramme pour la sous-routine du bouton poussoir de déverrouillage interne.

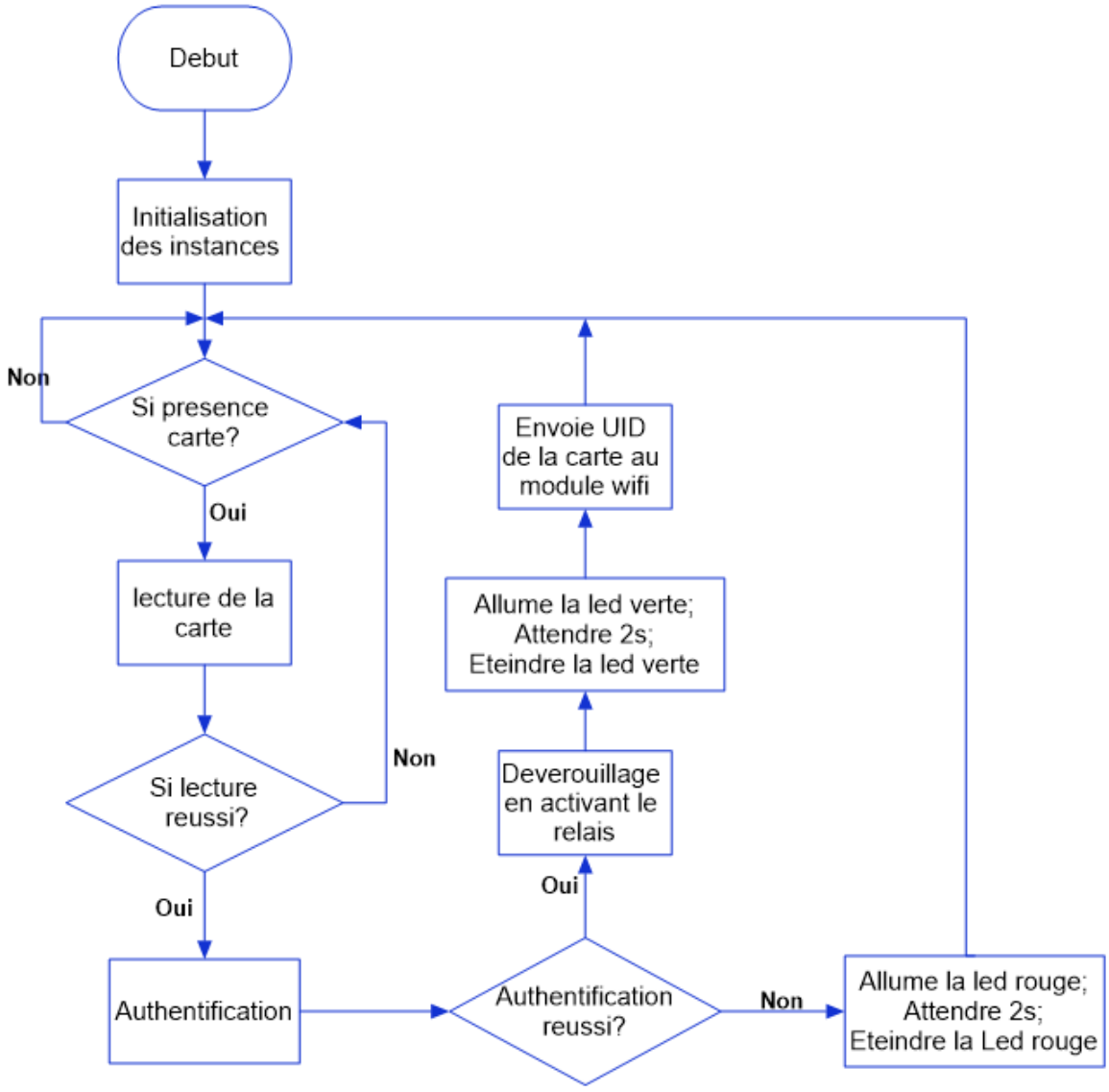


Figure 3. 8 : Organigramme de la carte de lecture du tag RFID

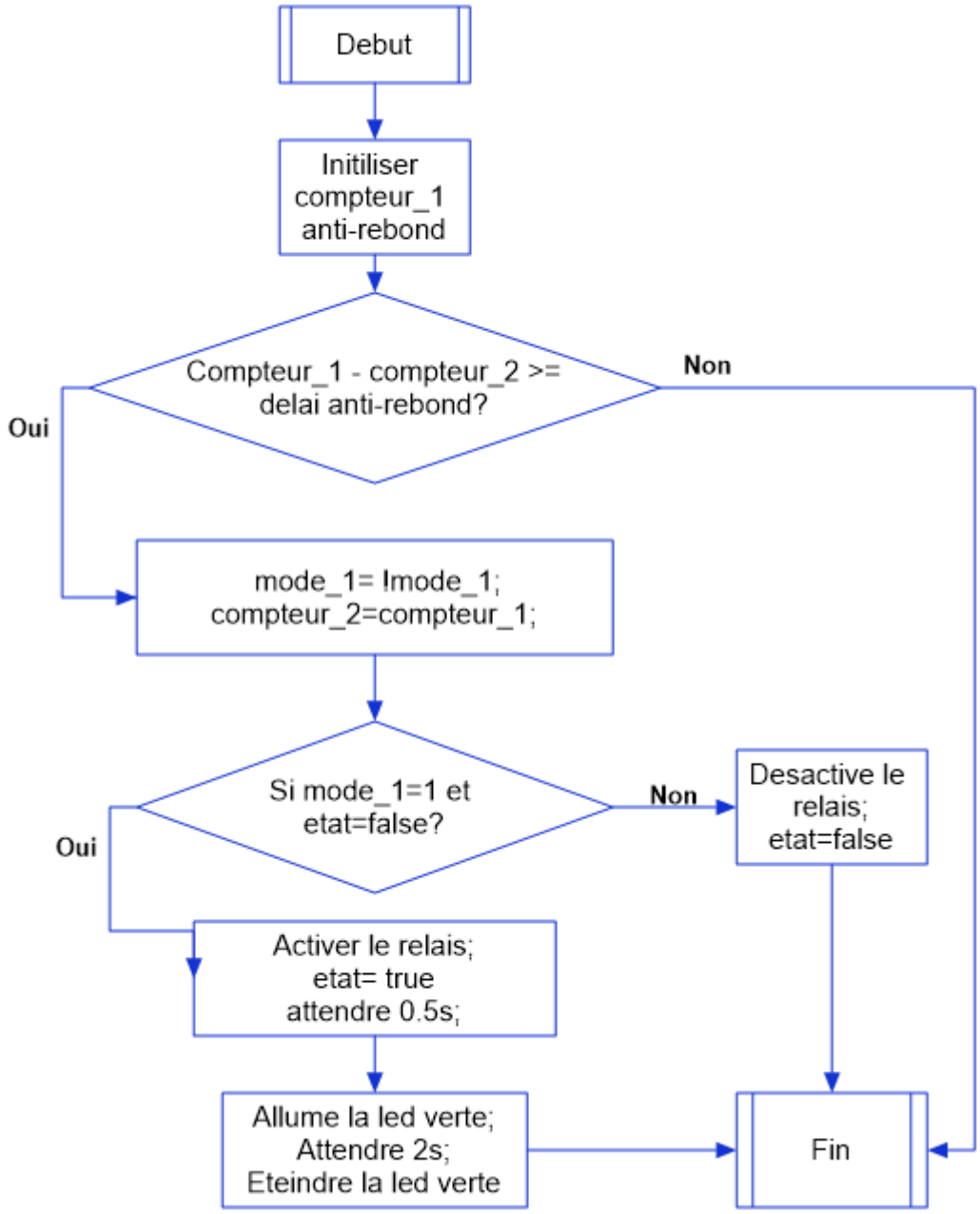


Figure 3. 9 : Organigramme de la sous-routine du bouton de déverrouillage interne

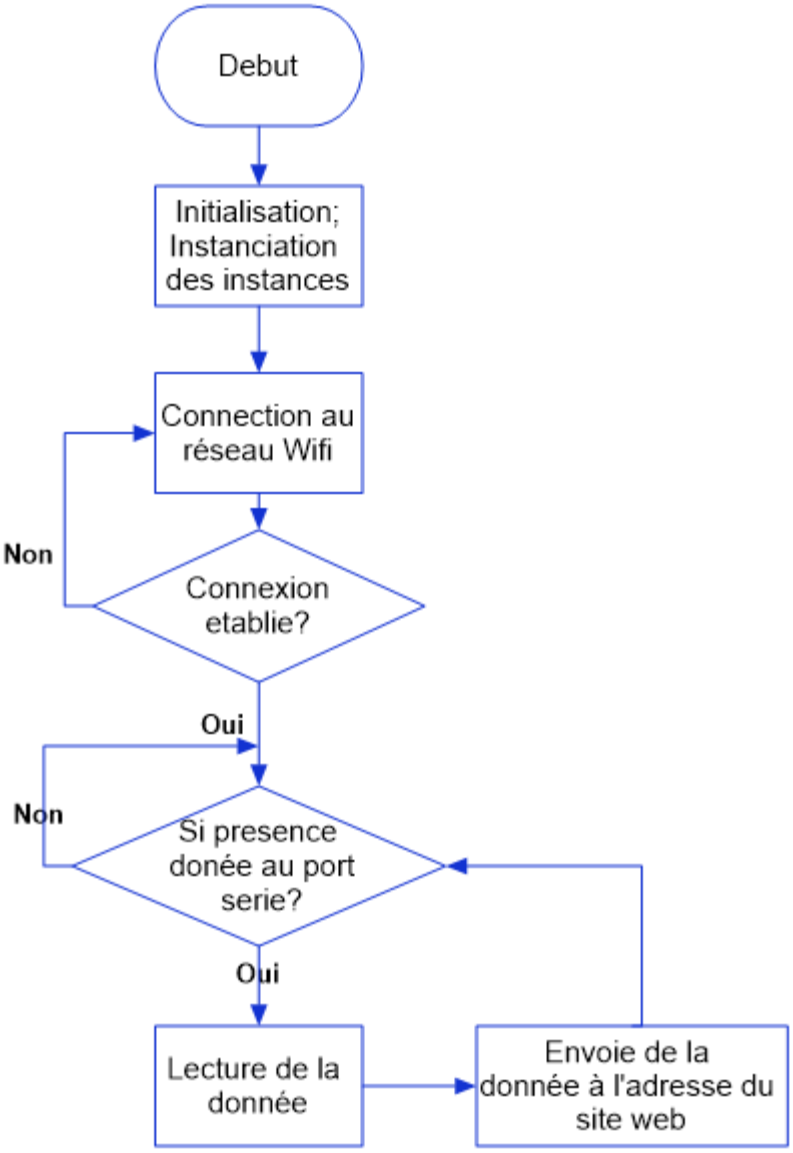


Figure 3. 10 : Organigramme du module Wifi

III.3 Partie B : Le site « application » web de gestion et de suivi des portes

Tout système de contrôle d'accès physique nécessite un intergiciel (middleware) ou application pour une gestion centralisée des accès et ceci pour une supervision. Dans ce projet nous avons opté pour une application web. Pour cette réalisation, un cahier des charges de fonctionnalité est nécessaire.

III.3.1 Cahier des charges du site web

- Le site doit disposer d'une page de connexion pour des questions de sécurité ;

- Seul, les enseignants et l'administrateur du site doivent pouvoir y accéder ;
- Les identifiants de connexion de chaque enseignant (email, mot de passe) sont définis et stockés préalablement dans la base de données du serveur ;
- La possibilité de faire une demande de salle pour une séance de rattrapage ;
- La possibilité d'afficher l'état de la salle (occupée, libre ou en attente) ;
- La possibilité d'afficher les informations relatives à l'occupant (nom, prénom…) ;
- La possibilité d'afficher les informations relatives aux salles : type de salle (amphi, TD, TP), capacité de place, département rattaché ;
- Des liens vers les sites web de l'université (plateforme e-learning, site de la fst, site central de l'université de Mostaganem).

III.3.2 Présentation du site web gateSecurAccess

Certains termes clés du thème de ce mémoire étant accès et salle ; alors nous avons choisi « gateSecurAcces » comme nom du site web pour mieux faire référence à ces termes et rester original.

Le site web « gateSecurAcces » permettra aux enseignants de se connecter dessus et de faire une demande de salle libre s'il en existe pour des séances de rattrapage. Il permettra à l'administrateur central du système de connaitre l'état de chaque salle (libre, occupée ou en attente), d'avoir des informations sur l'heure d'accès et la personne qui occupe la salle.

III.3.3 Outils et technologies de conception de l'application web gateSecurAcces

Tout site ou application web nécessite des langages de développement web pour sa conception. Dans notre cas nous avons utilisé les langages : HTML, CSS, PHP, SQL, JavaScript ; ces cinq langages sont nécessaires pour tout projet de développement web. Aussi nous avons utilisé les Framework CSS de Bootstrap et JavaScript de JQuery. Une base de données est également nécessaire et nous avons utilisé Xampp (constitué de deux logiciels principaux : Apache et PhpMyAdmin) pour émuler un serveur en local « intranet » (c'est-à-dire tout appareil connecté sur le même réseau que celui sur lequel l'application Xampp est installée et lancée peut accéder à notre site) et qui offre une

interface PhpMyAdmin permettant de gérer des bases de données à base du langage SQL. Un éditeur de code est également nécessaire pour la saisie des différents codes, nous avons utilisé SublimText qui est un excellent éditeur.

III.3.3.1 Le HTML

HTML pour HyperText Markup Langage (langage de balisage d'hypertexte) est un langage de balisage qui fait partie de la catégorie des langages interprétés ou de description de document (sa fonction est de donner du sens, structurer ou formater le contenu des documents) conçu pour représenter les pages web et permettant d'écrire de l'hypertexte. Sa dernière version en vigueur est le HTML5 [18].

III.3.3.1.1 Langage de balisage

Dans le jargon informatique, les langages de balisage représentent une classe de langages spécialisés dans l'enrichissement d'information textuelle et ceci en utilisant des balises (unités syntaxiques délimitant une séquence de caractères ou marquant une position précise à l'intérieur d'un flux de caractères comme un fichier texte). L'image ci-dessous illustre la structure d'une balise html.

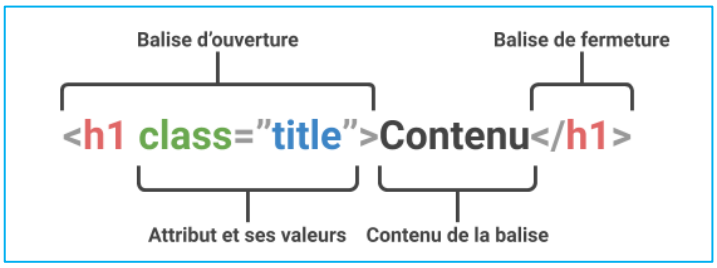


Figure 3. 11 : Structure d'une balise html

III.3.3.1.2 Structure d'une page web en HTML

La structure de base de toute page html se présente comme suit :

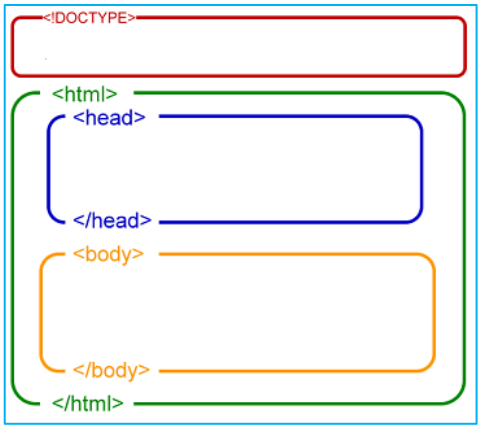


Figure 3. 12 : Structure d'une page html

- < ! DOCTYPE> correspond au type du document, ici un document html ;
- <html> correspond à l'ensemble de la page ;
- <head> est l'en-tête du document contenant des informations qui ne sont pas affichées sur la page mais, sont exploitées par les navigateurs et autres outils de statistique de google pour le référencement du site ;
- <body> est l'élément qui contient tout le contenu visible de la page.

III.3.3.2 Le CSS

CSS pour Cascading Style Sheets (feuilles de style en cascade) est un langage informatique décrivant la présentation et la mise en forme du contenu (couleur ; taille ; position des textes, couleur de fond…) des documents HTML en leur donnant des styles [19].

III.3.3.3 Le PHP

PHP pour **PHP Hypertext Preprocesso**r est un langage de script utilisé le plus souvent **« server side »** (coté serveur). Il a été conçu pour permettre la création de site ou d'applications web dynamiques. Il est généralement couplé à un serveur HTTP ou Apache. Lorsqu'un visiteur demande à consulter une page web, son navigateur envoie une requête au serveur http correspondant. Si la page est identifiée comme un script PHP grâce à l'extension (**.php**), le serveur interprète le code PHP des pages demandées et génère du code HTML pouvant être interprété et rendu par le navigateur web, à ce processus s'ajoute généralement un dialogue entre PHP et la base de données [20].

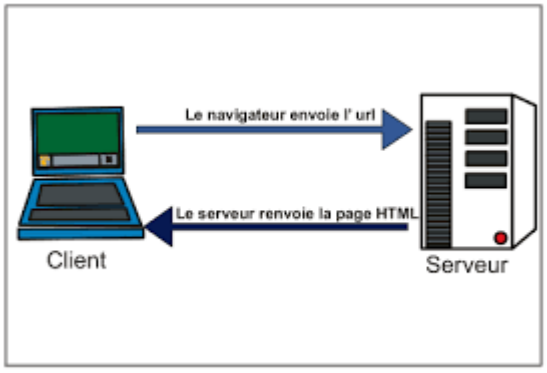


Figure 3. 13 : Processus de communication entre serveur et client

III.3.3.4 Le SQL

SQL pour **Structured Query Langage** (langage de requête structurée) est un langage informatique destiné à exploiter des bases de données relationnelles. Le SQL s'utilise de trois manières mais nous retiendrons la deuxième manière qui est celle que nous avons utilisé à savoir la technique dite **Embedded SQL** : elle consiste à incorporée dans le code source d'un programme écrit dans un autre langage des instructions en SQL [21].

III.3.3.5 La base de données

Une base de données « **database** », permet de stocker et de trouver des données brutes. Elle est au centre des dispositifs informatiques de collecte, mise en forme, stockage et utilisation d'informations. Les données peuvent être stockées sous une forme très structurées : on parle alors de base de données relationnelles [22].

Une base de données relationnelle est une base de données où l'information est organisée dans des tableaux à deux dimensions appelés des « **relations ou tables** », les lignes des tables sont appelées « **enregistrements** » et les colonnes « **attributs** » [23].

III.3.3.6 Le serveur

Figure 3. 14 : Image de serveur d'une centrale de calcule

III.3.3.6.1 Définition

Un serveur est un dispositif informatique (matériel et logiciel) semblable à un ordinateur (équipé de processeurs et de mémoires) mais en plus puissant, performant et tournant 24h/24, 7j/7 destiné à offrir des services à des clients en réseau internet ou intranet. Ces services peuvent être un accès au *WWW* (World Wide Web), le stockage et la gestion de base de données et autres [24].

III.3.3.6.2 Fonctionnement

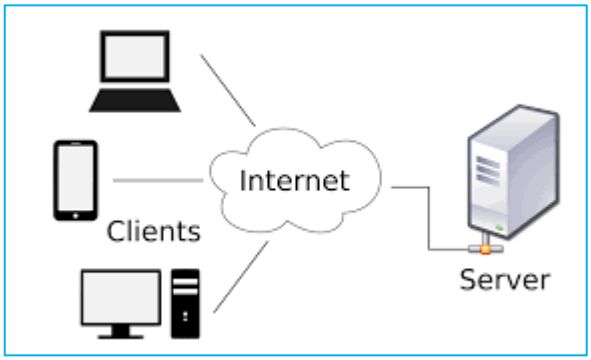


Figure 3. 15 : Relation serveur client

Un serveur fonctionne le plus souvent en environnement client-serveur. Les traitements sont effectués par l'exécution conjointe de deux logiciels différents et complémentaires placés sur des ordinateurs différents : le client et le serveur. Le client étant l'ordinateur ou la machine virtuelle qui envoie les requêtes via une interface utilisateur (logiciel client) le plus souvent un navigateur web et le serveur l'ordinateur ou le dispositif informatique qui traite les requêtes et génère leurs réponses. En réponse à une demande, le serveur peut envoyer un document le plus souvent en format HTML qui est stocké en

tant que fichier dans les mémoires de masses du serveur ou exécuter un traitement. Le client affiche les réponses par exemple à l'écran comme dans la plupart des navigateurs web. La communication entre le client et le serveur s'effectue suivant le protocole HTTP ou HTTPS [24][25].

III.3.3.6.3 Protocole HTTP et HTTPS

HTTP pour HyperText Transfert Protocol (protocole de transfert hypertexte) est un protocole de communication client-serveur basé sur la couche application du modèle OSI. HTTPS (avec S pour Secured) est la variante sécurisée par l'usage des protocoles Transfert Layer Security (TLS) [26].

III.3.3.6.4 Caractéristiques d'un programme serveur [25]

- Il écoute une connexion entrante sur un ou plusieurs ports réseaux locaux ;
- A la connexion d'un client sur le port en écoute, il ouvre un socket local au système d'exploitation ;
- Une fois la connexion établie, le processus serveur communique avec le client suivant le protocole prévu par la couche application du **modèle OSI**.

III.3.4 Structure de l'application web gateSecurAccess

Notre site se compose de 5 pages principales à savoir :

- Une page de connexion ;
- Une page d'accueil ;
- Une page pour réserver des salles ;
- Une page pour voir les demandes de réservation ;
- Une page à propos.

III.3.4.1 Préparation de l'environnement de travail

L'ensemble des codes de notre application web est écrit en PHP embarquant du SQL car du contenu est généré suivant différente situation. Le navigateur seul ne peut pas le traité et l'interprété car PHP est un langage qui s'exécute coté serveur et que SQL nécessite un serveur de base de données. De ce fait il nous a fallu faire recours à un logiciel de serveur web pouvant exécuter des scripts PHP à savoir celui « d'**Apache**

http server » et d'un logiciel de serveur de base de données ici **MySQL**. Ces deux logiciels sont disponibles sur une même application : **XAMPP**.

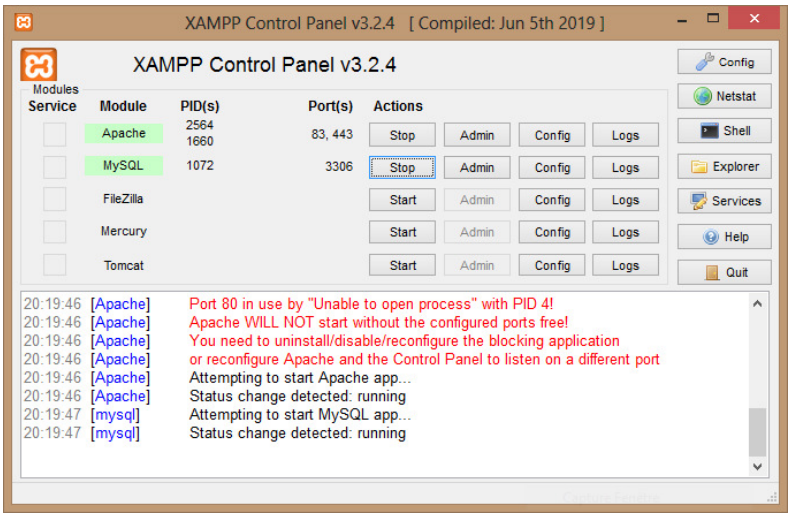


Figure 3. 16 : Panel de contrôle de l'application XAMPP

Une fois installée celle-ci crée un répertoire xampp dans la racine C de l'ordinateur. On lance l'application et on obtient l'interface ci-dessus puis on lance les services Apache et MySQL.

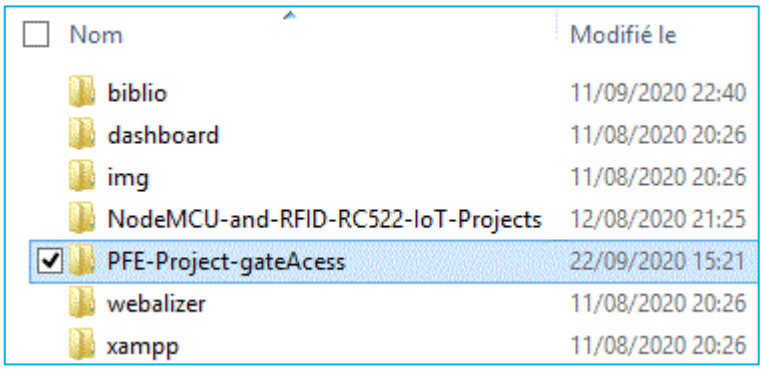


Figure 3. 17 : Répertoire de création du projet PFE-Project-gateAccess

Dans le répertoire xampp se trouve un dossier appelé htdocs, on y crée un répertoire nommé PFE-Project-gateAccess et ce dernier contiendra tous nos script PHP, JavaScript et CSS.

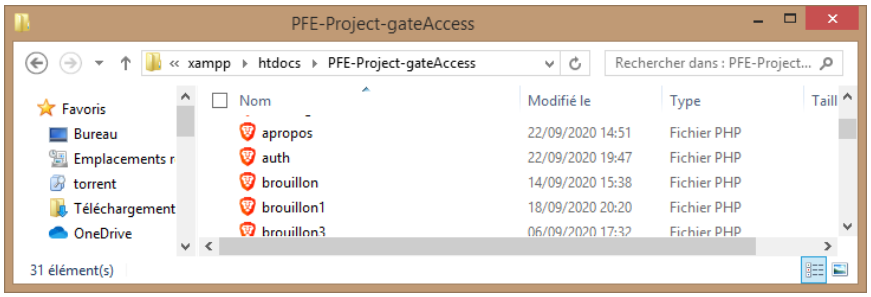


Figure 3. 18 : Contenu du dossier PFE-Project-gateAccess

Ensuite on lance les services Apache et MySQL depuis le panel de gestion de XAMPP et on obtient les images ci-dessous.

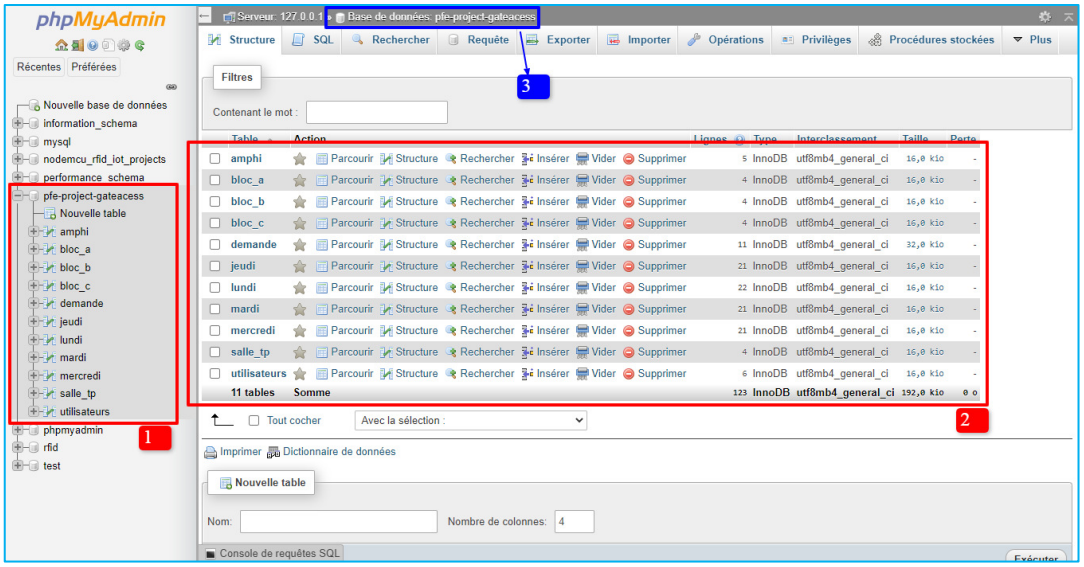


Figure 3. 19 : Page de lancement phpMyAdmin

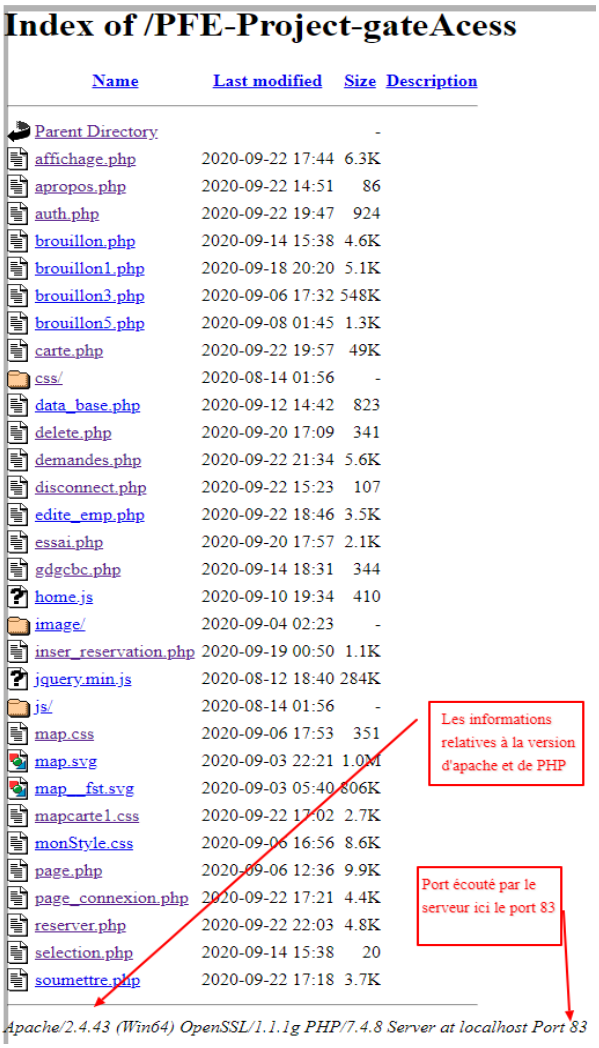


Figure 3. 20 : Page d'accueil du répertoire du projet

III.3.4.2 Structure de la base de données

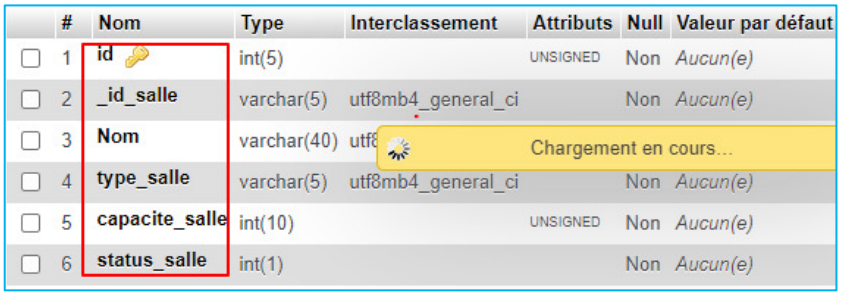
Notre base de données se compose de 11 tables, chaque table regroupe un ensemble de données relationnelles.

Table	Action	Lignes	Type	Interclassement	Taille	Perte
amphi	Parcourir Structure Rechercher Insérer Vider Supprimer	5	InnoDB	utf8mb4_general_ci	16,0 kio	-
bloc_a	Parcourir S Chargement en cours...	4	InnoDB	utf8mb4_general_ci	16,0 kio	-
bloc_b	Parcourir Structure Rechercher Insérer Vider Supprimer	4	InnoDB	utf8mb4_general_ci	16,0 kio	-
bloc_c	Parcourir Structure Rechercher Insérer Vider Supprimer	4	InnoDB	utf8mb4_general_ci	16,0 kio	-
demande	Parcourir Structure Rechercher Insérer Vider Supprimer	11	InnoDB	utf8mb4_general_ci	32,0 kio	-
jeudi	Parcourir Structure Rechercher Insérer Vider Supprimer	21	InnoDB	utf8mb4_general_ci	16,0 kio	-
lundi	Parcourir Structure Rechercher Insérer Vider Supprimer	22	InnoDB	utf8mb4_general_ci	16,0 kio	-
mardi	Parcourir Structure Rechercher Insérer Vider Supprimer	21	InnoDB	utf8mb4_general_ci	16,0 kio	-
mercredi	Parcourir Structure Rechercher Insérer Vider Supprimer	21	InnoDB	utf8mb4_general_ci	16,0 kio	-
salle_tp	Parcourir Structure Rechercher Insérer Vider Supprimer	4	InnoDB	utf8mb4_general_ci	16,0 kio	-
utilisateurs	Parcourir Structure Rechercher Insérer Vider Supprimer	6	InnoDB	utf8mb4_general_ci	16,0 kio	-
11 tables	Somme	123	InnoDB	utf8mb4_general_ci	192,0 kio	0 o

Figure 3. 21 : Structure de notre base de données

Les tables peuvent être groupées en 4 classes à savoir :

- Les tables **amphi**, **bloc_a**, **bloc_b, bloc_c** et **salle_tp** (classe 1) : elles contiennent les informations des salles de chaque bloc. Ces informations sont les suivantes :
    - Numéro de la salle ;
    - Nom de la personne qui occupe la salle ;
    - Type de salle ;
    - Capacité de place de la salle ;
    - Statut de disponibilité de la salle ;

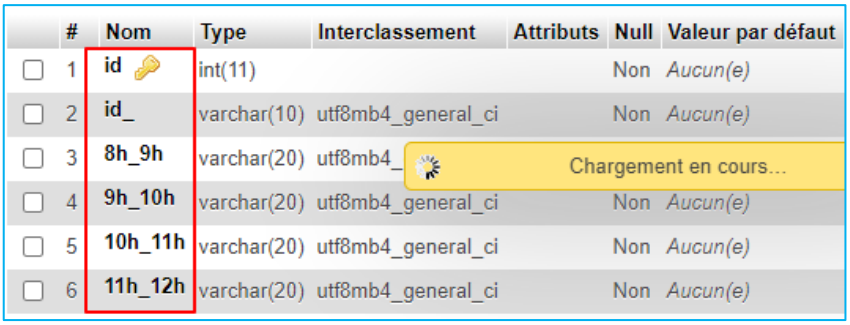


#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut
1	id	int(5)		UNSIGNED	Non	*Aucun(e)*
2	_id_salle	varchar(5)	utf8mb4_general_ci		Non	*Aucun(e)*
3	Nom	varchar(40)	utf Chargement en cours...			
4	type_salle	varchar(5)	utf8mb4_general_ci		Non	*Aucun(e)*
5	capacite_salle	int(10)		UNSIGNED	Non	*Aucun(e)*
6	status_salle	int(1)			Non	*Aucun(e)*

Figure 3. 22 : Structure des tables « salles » de la base de données

- Les tables **lundi**, **mardi**, **mercredi**, **jeudi** (classe 2) : elles contiennent les informations de l'emploi du temps de chaque salle par rapport aux jours de la semaine. Ces informations sont les suivantes :
    - Les différents horaires (**8h, 9h ,10h et 11h**) : ceux-ci contiendront le nom de l'enseignant ;

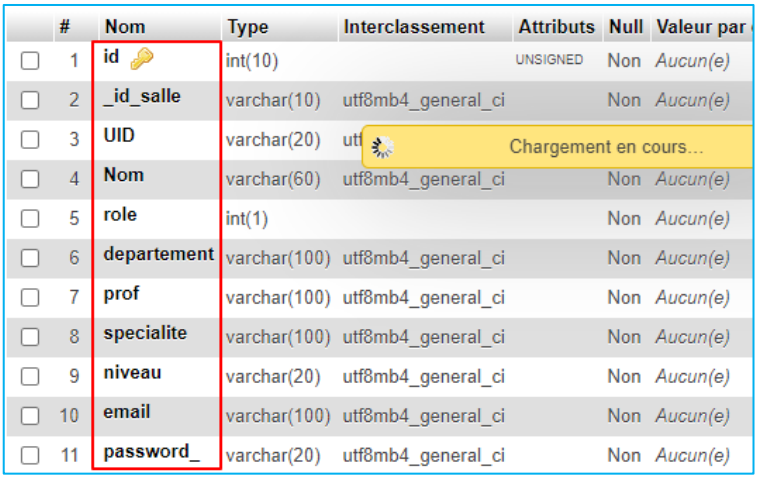
- L'identifiant de la salle pour faire le lien.



	#	Nom	Type	Interclassement	Attributs	Null	Valeur par défaut
☐	1	id	int(11)			Non	*Aucun(e)*
☐	2	id_	varchar(10)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	3	8h_9h	varchar(20)	utf8mb4_			Chargement en cours...
☐	4	9h_10h	varchar(20)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	5	10h_11h	varchar(20)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	6	11h_12h	varchar(20)	utf8mb4_general_ci		Non	*Aucun(e)*

Figure 3. 23 : Structure des tables « emploi du temps » de la base de données

- La table **utilisateurs** (classe 3) : elle contient les informations relatives aux utilisateurs.
  - **ID :** identifiant unique pour identifier chaque utilisateur ;
  - Nom de l'utilisateur ;
  - Le département auquel il est rattaché ;
  - Le module qu'il enseigne ;
  - Le niveau universitaire enseigné ;
  - La spécialité enseignée ;
  - Le mot de passe ;
  - L'email ;
  - Le rôle : celui-ci permet de définir le niveau de privilège de l'utilisateur. Il est soit 1 ou 0 ;
  - L'identifiant de la salle du jour de l'emploi du temps : celui-ci permet de faire le lien entre la salle et le nom de la personne dans un but d'affichage ;
  - **UID** : correspond à l'identifiant du tag RFID de l'utilisateur. Elle permet de savoir qui a accédé à la salle lorsque les informations d'accès (UID du tag) de la salle sont reçues par l'application web provenant de la carte d'accès.

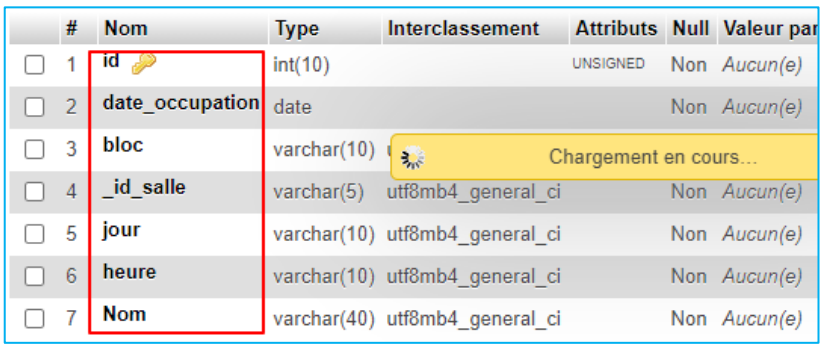


	#	Nom	Type	Interclassement	Attributs	Null	Valeur par
☐	1	id	int(10)		UNSIGNED	Non	*Aucun(e)*
☐	2	_id_salle	varchar(10)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	3	UID	varchar(20)	utf			
☐	4	Nom	varchar(60)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	5	role	int(1)			Non	*Aucun(e)*
☐	6	departement	varchar(100)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	7	prof	varchar(100)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	8	specialite	varchar(100)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	9	niveau	varchar(20)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	10	email	varchar(100)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	11	password_	varchar(20)	utf8mb4_general_ci		Non	*Aucun(e)*

Chargement en cours...

Figure 3. 24 : Structure de la table « utilisateurs » de la base de données

- La table **demandes (classe 4) :** elle contient les informations de réservation de salle pour des séances de rattrapage.
    - La date d'occupation ;
    - Le Nom de la personne qui a fait la réservation ;
    - Le jour et l'heure de l'emploi du temps ;
    - L'identifiant de la salle réservée.



	#	Nom	Type	Interclassement	Attributs	Null	Valeur par
☐	1	id	int(10)		UNSIGNED	Non	*Aucun(e)*
☐	2	date_occupation	date			Non	*Aucun(e)*
☐	3	bloc	varchar(10)				
☐	4	_id_salle	varchar(5)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	5	jour	varchar(10)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	6	heure	varchar(10)	utf8mb4_general_ci		Non	*Aucun(e)*
☐	7	Nom	varchar(40)	utf8mb4_general_ci		Non	*Aucun(e)*

Chargement en cours...

Figure 3. 25 : Structure de la table « demandes » de la base de données

Ces informations seront manipulées (modifications, insertion et lecture) par nos différents scripts PHP pour l'affichage des différentes pages de l'application web.

III.3.4.3 Analyse Fonctionnelle et Algorithmique de l'application web

III.3.4.3.1 La page de connexion

La page de connexion sert de portail d'entrée pour accéder aux restes du site, la personne doit saisir ses identifiants email et mot de passe via un formulaire. Ces informations sont envoyées à un script PHP d'authentification. Le script vérifie ces informations en les comparant à celles de la table utilisateurs de la base de données.

a. Structure de la table utilisateurs de la base de données

#	Nom	Type	Interclassement	Attributs	Null	Valeur par
1	id	int(10)		UNSIGNED	Non	*Aucun(e)*
2	_id_salle	varchar(10)	utf8mb4_general_ci		Non	*Aucun(e)*
3	UID	varchar(20)	utf	Chargement en cours...		
4	Nom	varchar(60)	utf8mb4_general_ci		Non	*Aucun(e)*
5	role	int(1)			Non	*Aucun(e)*
6	departement	varchar(100)	utf8mb4_general_ci		Non	*Aucun(e)*
7	prof	varchar(100)	utf8mb4_general_ci		Non	*Aucun(e)*
8	specialite	varchar(100)	utf8mb4_general_ci		Non	*Aucun(e)*
9	niveau	varchar(20)	utf8mb4_general_ci		Non	*Aucun(e)*
10	email	varchar(100)	utf8mb4_general_ci		Non	*Aucun(e)*
11	password_	varchar(20)	utf8mb4_general_ci		Non	*Aucun(e)*

Figure 3. 26 : Table utilisateurs de la base de données

Ici ce sont les colonnes 10 (email) et 11 (password_) qui nous intéresse pour faire l'authentification. Elles contiennent l'email et le mot de passe de chaque utilisateur. Si les informations saisies (email et mot de passe) correspondent à une ligne de la table « utilisateurs » contenant le même email et mot de passe alors l'accès est autorisé et la personne est redirigée vers la page d'accueil sinon un message d'erreur s'affiche pour lui signaler que les informations saisies sont incorrectes.

id	_id_salle	UID	Nom	role	departement	prof	specialite	niveau	email	password_
0			Administrateur	1					admin@mail.com	admin
			Chargement en cours...							
1	am1		Azzeddine	0	Geni-électrique	Système RFID	Electronique des systèmes embarqués	Master 2	azzeddine@mail.com	user
2	am5		Abdellaoui	0	Geni-électrique	Système Embarqué	Electronique des systèmes embarqués	Master 2	abdellaoui@mail.com	user
3	am2		Rebi	0	Geni-électrique	Microprocesseur	Télécom	Master 1	rebi@mail.com	user
4	am4		Reddouane	0	Geni-mécanique	Mécanique des Fluides	Conversion énergenitique	Licence 3	reddouanemail.com	user
5	am3		Abdou	0	Geni-civil	Matériaux de construction	Construction	Licence 1	abdou@mail.com	user

Figure 3. 27 : Information des utilisateurs dans la base de données

b. Organigramme du Script PHP d'authentification

Nom variable	Description
$email	Variable contenant l'email
$mdp	Variable contenant le mot de passe
$_POST	Tableau contenant les informations saisies dans le formulaire de connexion
$_POST['email']	Contenu du tableau $_POST relatif à l'email
$_POST['password']	Contenu du tableau $_POST relatif au password
Userexist	Contient le nombre de ligne retourné du résultat de la requête faite à la base de données
$_SESSION	Tableau associatif global dans lequel sont stockés des informations relatives à la session actuelle
$_SESSION['Nom']	Contenu du tableau $_SESSION relatif au nom de la personne connectée à la plateforme
$_SESSION['Role']	Contenu du tableau $_SESSION relatif au rôle de la personne connectée à la plateforme
$_SESSION['id']	Contenu du tableau $_SESSION relatif à id (identifiant unique crée lors de l'enregistrement des informations dans la base de données) de la personne connectée à la plateforme
$result	Tableau associatif contenant les résultats de la requête faite à la base de données

Tableau 3. 1 : table des variables du script d'authentification

En PHP un tableau associatif est un tableau de clé et de valeur : la « **clé** » correspond à l'indice de la ligne et la « **valeur** » son contenu. Ainsi dans le l'image ci-dessous, la syntaxe **$result1['Nom']** renvoie le contenu de la première ligne du tableau **$result1.**

```
$result1=array("Nom" => '---',
               "prof" => '---',
               "departement" => '---',
               "specialite" => '---',
               "niveau" => '---');
```

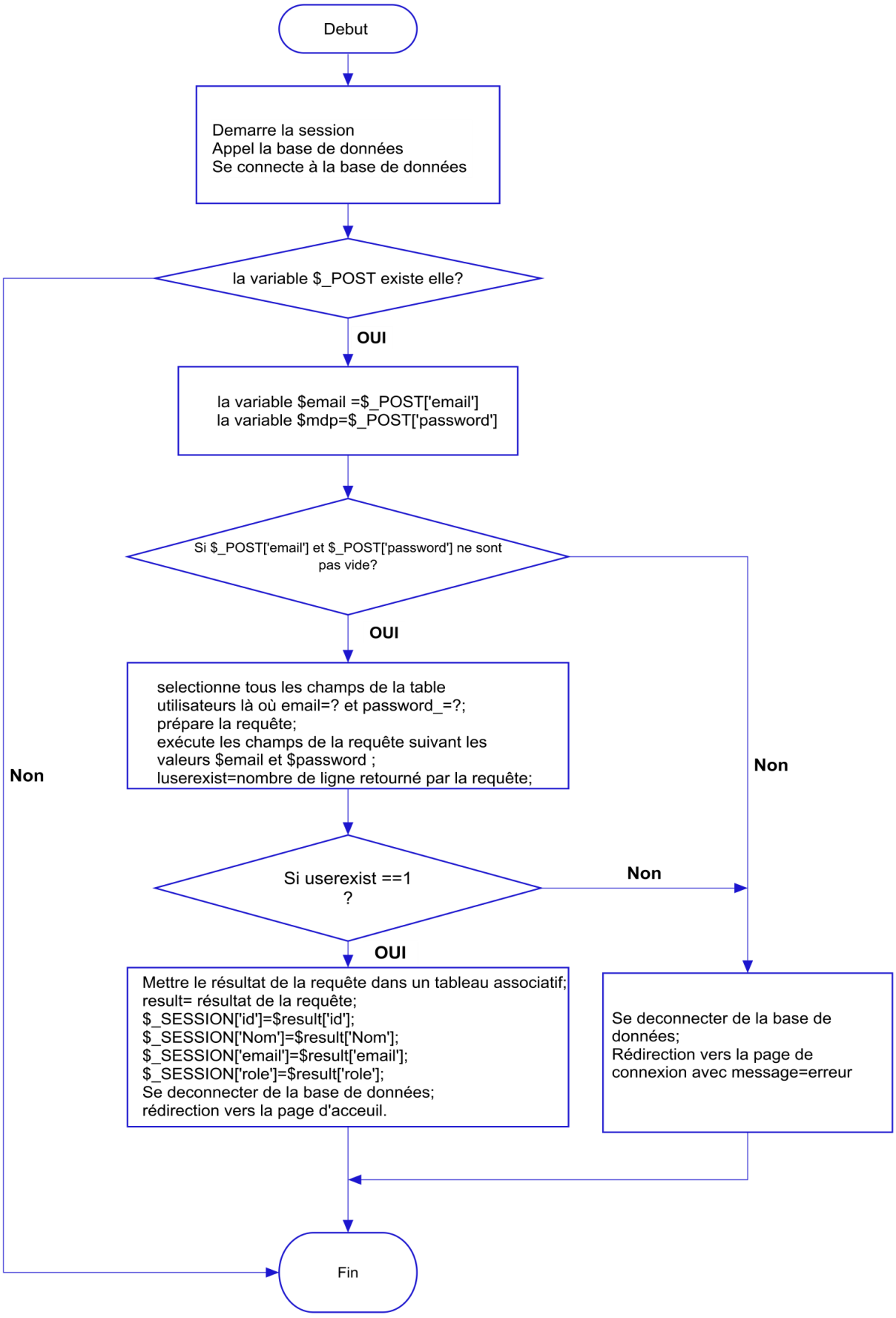


Figure 3. 28 : Organigramme du Script php d'authentification

III.3.4.3.2 La page d'accueil

La page d'accueil se compose de 2 sections principales et d'une section d'en-tête commune à toutes les pages.

a. Section en-tête

Elle permet de se déplacer d'une page à une autre, elle fait office de barre de navigation. A gauche nous avons un bouton déconnexion permettant de se déconnecter.

b. Section Carte de la faculté

Dans cette section nous avons une carte interactive en format SVG (c'est-à-dire dont les différents éléments sont cliquables par l'utilisateur, ici les blocs) de la faculté des sciences et techniques de Mostaganem. Les autres formats d'images (jpg, png, jpeg…) sont justes des représentations de couleurs de pixels, ils ne permettent pas de créer de l'interactivité sur l'image par contre le format SVG décrit l'image avec des formes mathématiques. Ce format SVG est décrit avec le langage de balisage XML (Extensible Markup Langage) permettant d'exploiter les différentes formes. N'ayant pas besoin de rendre tous les blocs cliquables. Ainsi les blocs A, B et C, Hall amphi, Salle TP, Amphi 4 et 5 peuvent être cliqués par l'utilisateur. Un clic sur chacun de ces blocs permet l'affichage de la section information relative à ce bloc.

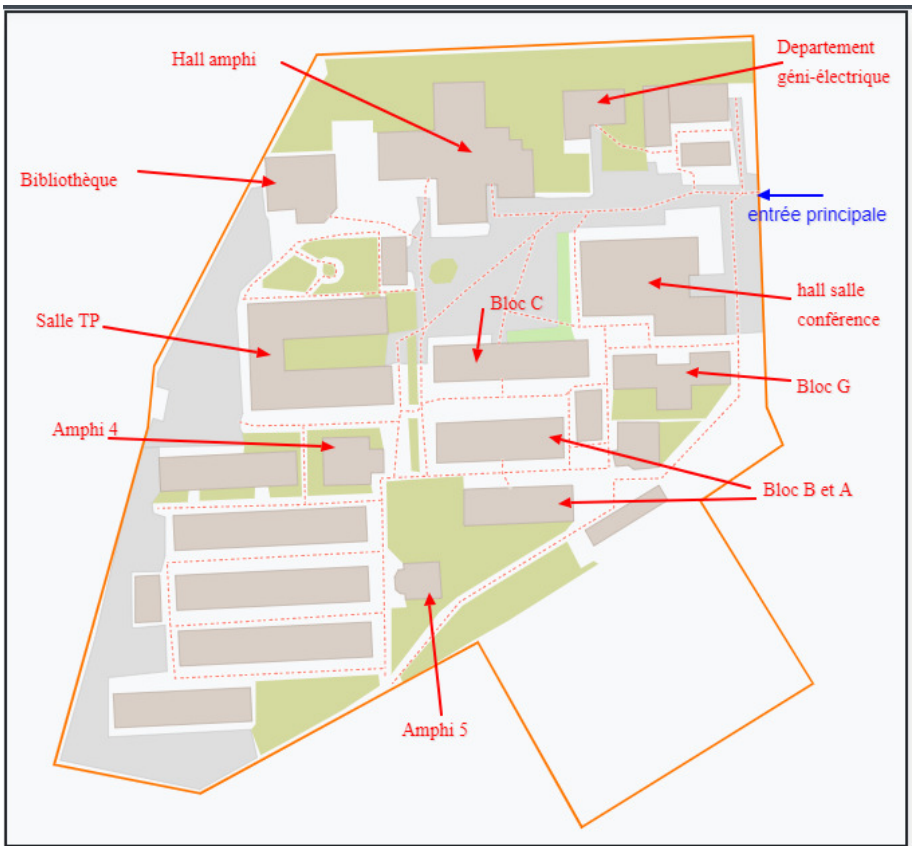


Figure 3. 29 : Carte du site de fst de Mostaganem

c. Exemple d'illustration de l'interactivité de la carte

Le clic sur un bloc entraine automatiquement son activation, celui-ci passe en bleu, et la désactivation des autres blocs qui sont actifs. La couleur des blocs inactifs ou désactivés reste inchangée. Nous avons lié tous les amphithéâtres ensemble, ainsi le clic sur l'un d'entre eux active simultanément les autres amphis.

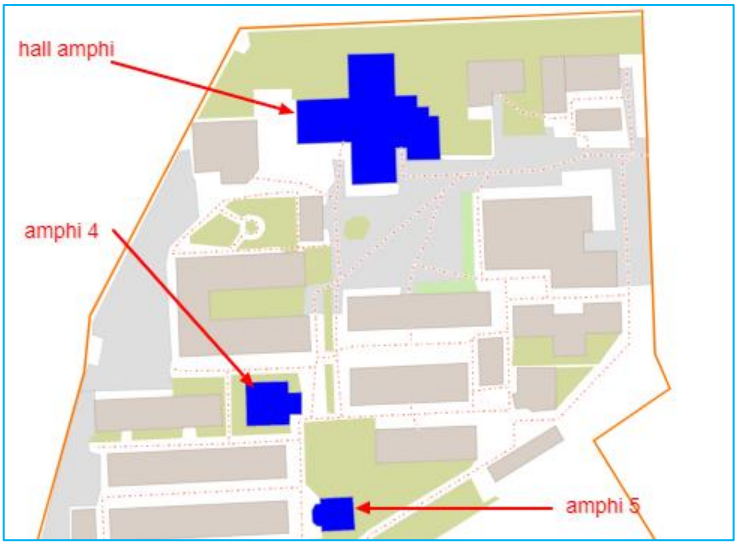


Figure 3. 30 : Amphithéâtres représentés sur la carte du site

Hall Amphithéatre ← Nom du bloc

#	Nom	Type de salle	Capacité	Status
1	Azzeddine	cours	100	Occupée
2	Rebi	cours	150	Occupée
3	---	cours	200	Libre
4	Reddoune	cours	300	Réservée
5	---	cours	400	Libre

Figure 3. 31 : Information des salles du bloc hall amphithéâtre

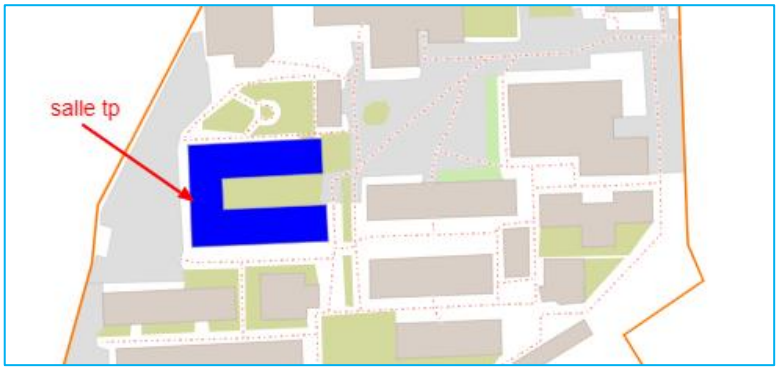


Figure 3. 32 : Salles de TP représentées sur la carte du site

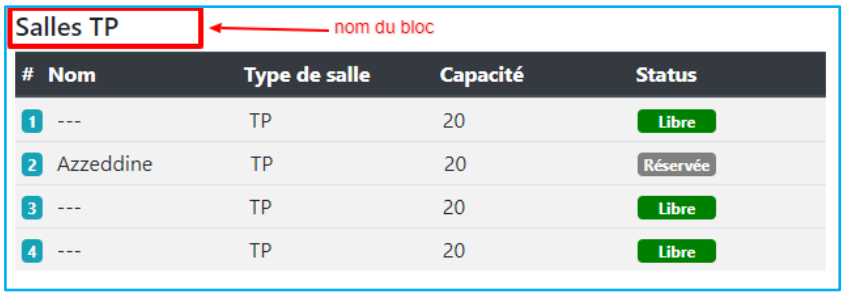


Figure 3. 33 : Information des salles du bloc salles TP

Figure 3. 34 : Bloc B représenté sur la carte du site

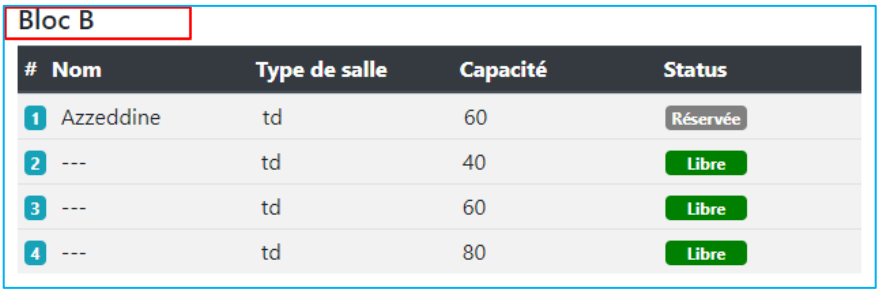


Figure 3. 35 : Informations des salles du bloc B

III.3.4.3.3 La section information

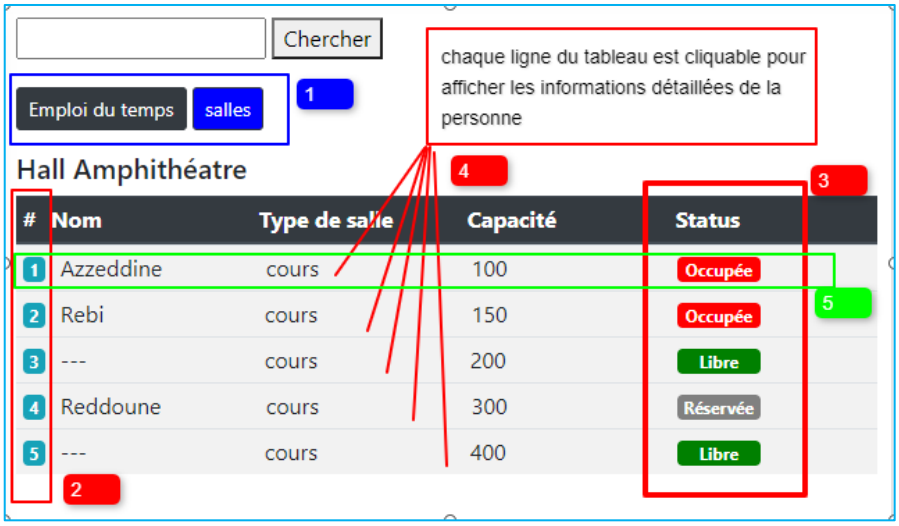


Figure 3. 36 : Section information de la page d'accueil

Cette section comporte un système d'onglet permettant de faire deux affichages différents. Pour basculer d'un onglet à un autre, il suffit de cliquer sur l'un des boutons Salles ou Emploi du temps. Le bouton actif est en bleu et celui non actif en noir. Ces boutons sont matérialisés par le rectangle bleu portant le numéro 1 sur la figure ci-dessus.

Le bouton **Salles** permet l'affichage des informations détaillées de chaque salle du bloc sur lequel le clic a eu lieu. Ces informations sont les suivantes :

- **ID** : numéro de la salle ;
- **Nom** : nom de la personne qui occupe la salle ;
- **Type de Salle** : renseigne sur le type de la salle (cours, TD, TP) ;
- **Capacité** : renseigne le nombre de places que peut prendre la salle ;
- **Statut** : renseigne sur l'état de la salle (occupée, libre ou en attente).

Le rectangle vert numéroté 5 représente une ligne du tableau. Nous avons au total 5 lignes (rectangle numéroté 2) qui représentent les 5 salles du bloc Hall Amphithéâtre. Chaque ligne est cliquable. Le clic sur la ligne 1 comme exemple permet d'afficher en-dessous de celle-ci les informations détaillées de la personne qui occupe la salle 1. Ces informations sont les suivantes :

- Nom de l'occupant ;
- Le module qu'il enseigne ;

- Le département auquel il est rattaché ;
- La spécialité qu'il enseigne ;
- Le niveau universitaire enseigné.

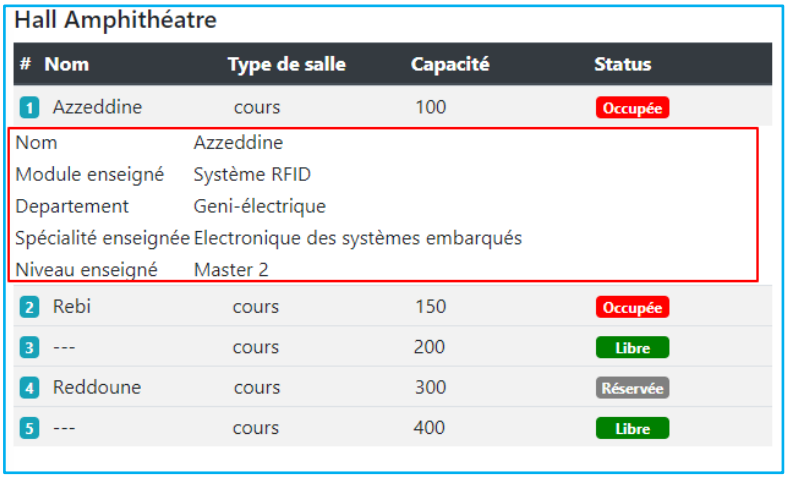


Figure 3. 37 : Information détaillée de la personne occupant la salle

Le bouton **Emploi du temps** permet l'affichage de l'emploi du temps de chaque salle du bloc sur lequel le clic a eu lieu.

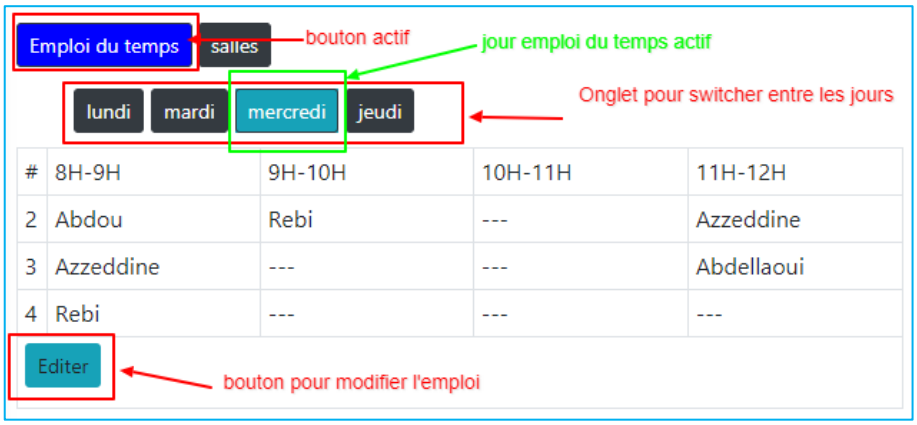


Figure 3. 38 : Section emploi du temps de la page d'accueil

Le deuxième rectangle rouge comportant des jours est un système d'onglet permettant d'afficher en particulier l'emploi du temps du jour que l'on souhaite visualiser ou modifier.

Le troisième rectangle rouge « Editer » en bas est un bouton permettant la modification de l'emploi du temps. Un clic sur ce bouton renvoie sur une nouvelle page figure ci-dessous pour apporter des modifications.

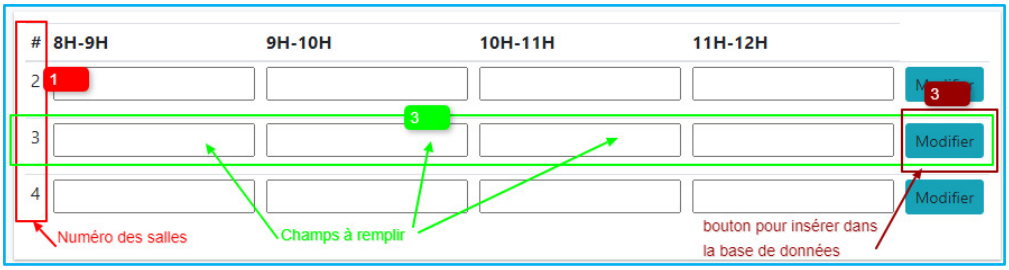


Figure 3. 39 : Page de modification de l'emploi du temps

- Le rectangle 1 correspond au numéro des salles du bloc ;
- Le rectangle 2 en vert est une ligne correspond à une salle, ici la salle 3. Cette ligne comporte des champs à remplir pour les différents horaires ;
- Le rectangle 3 est un bouton permettant d'envoyer les informations saisies à un script PHP afin d'insérer dans la base de données ces informations.

Afin de s'assurer que les informations envoyées ont bien été mise à jour dans la base de données, le script PHP qui s'occupe de ce traitement renvoie un message de réussite figure ci-dessous que nous pouvons afficher.

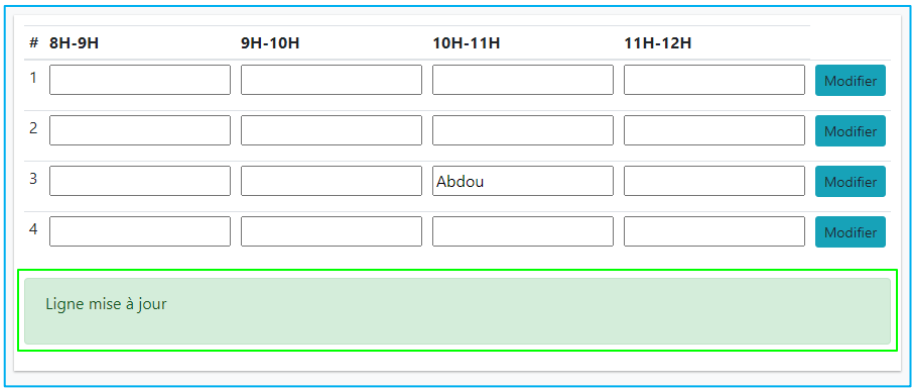


Figure 3. 40 : Notification de mise à jour de l'emploi du temps

III.3.4.3.4 Page de réservation de salle :

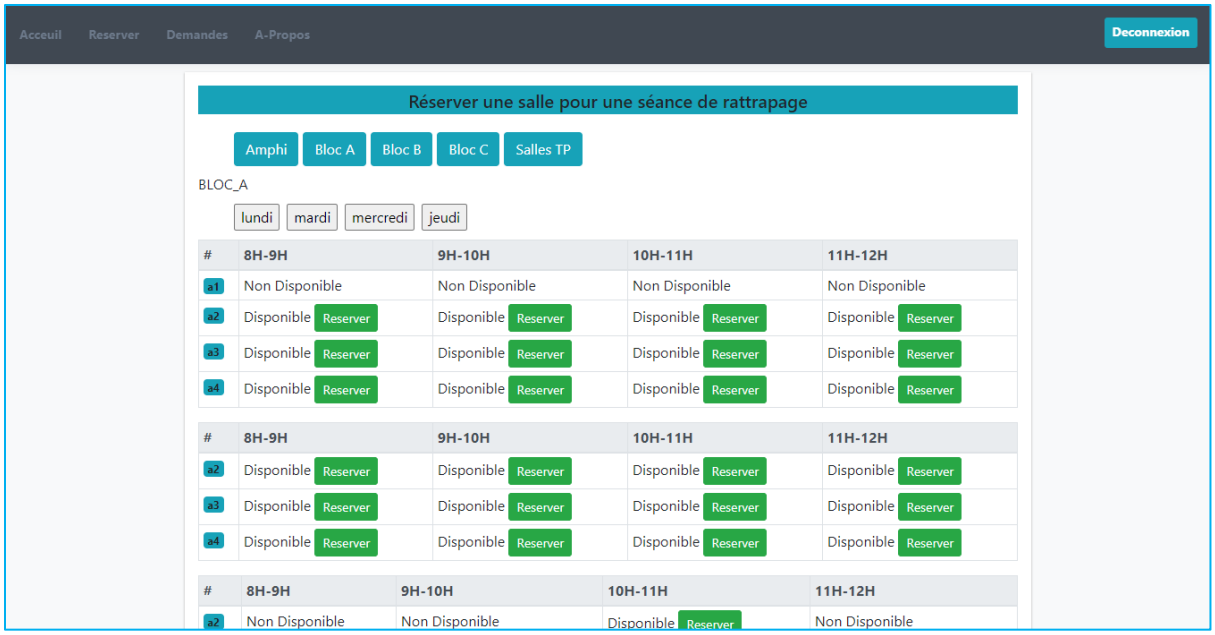


Figure 3. 41 : Page de réservation de salle

Cette page affiche des informations sur la disponibilité des salles de chaque bloc pour les jours ouvrables de la semaine et les différents horaires de l'emploi du temps. Ces informations permettront à une personne désirante de faire des séances de rattrapage de réserver une salle pour une date ultérieure.

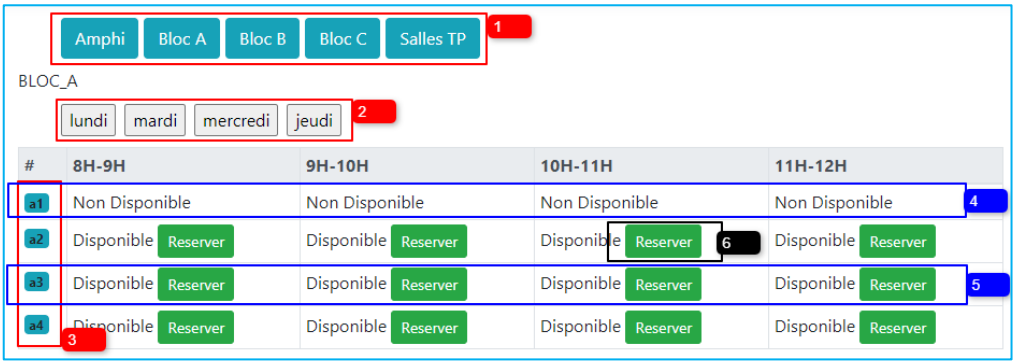


Figure 3. 42 : Détails explicatifs de la page de réservation de salles

- Le rectangle rouge 1 permet de sauter directement et d'aller sur la ligne où se trouve les informations du bloc en question ;
- Le rectangle rouge 2 permet d'afficher les informations de disponibilité des salles du bloc en question ici le bloc A par rapport au jour de la semaine ;
- Le rectangle rouge 3 correspond au numéro des salles ;

- Le rectangle bleu 4 est une ligne correspondant à une salle ici la salle a1, c'est dans ce champs que nous pouvons voir les informations de disponibilité par rapport aux différents horaires. Pour cette salle aucun horaire n'est disponible pour une quelconque réservation ;
- Pour le rectangle bleu 5, nous pouvons voir que des salles sont disponibles ;
- Aussitôt qu'une salle est disponible un bouton « **Réserver** » s'affiche (rectangle noir 6). Un clic sur ce bouton renvoie sur une nouvelle page. Opération à travers laquelle sont transitées les informations relatives au bloc, au numéro de salle, au jour et à l'horaire de l'emploi du temps, au nom de la personne connecté.

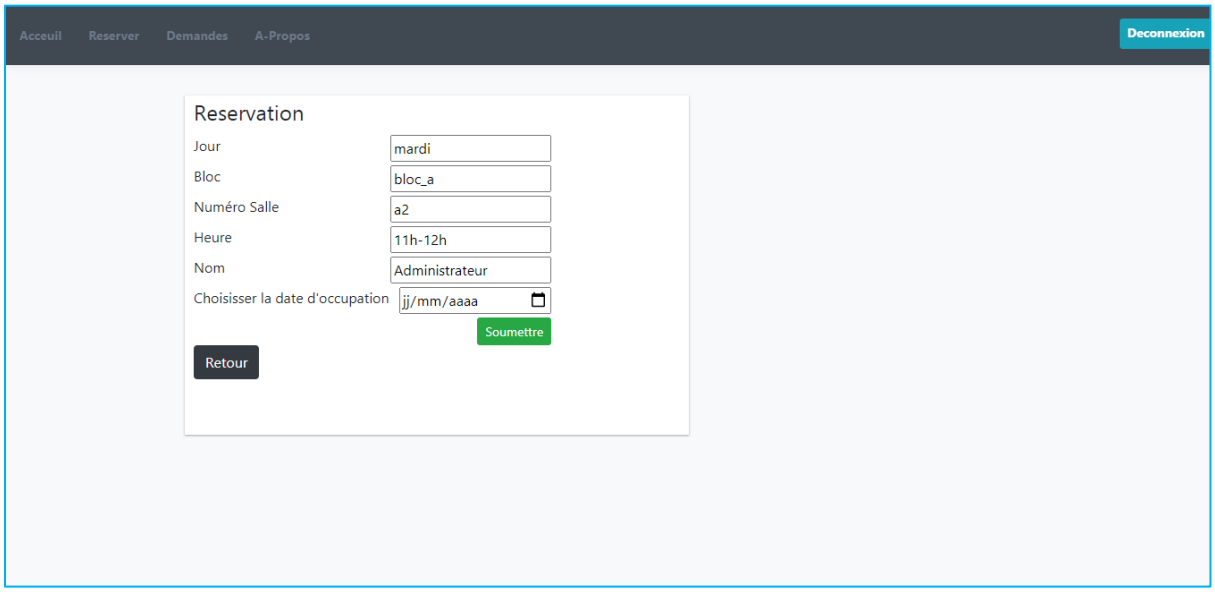


Figure 3. 43 : Page de finalisation de la réservation

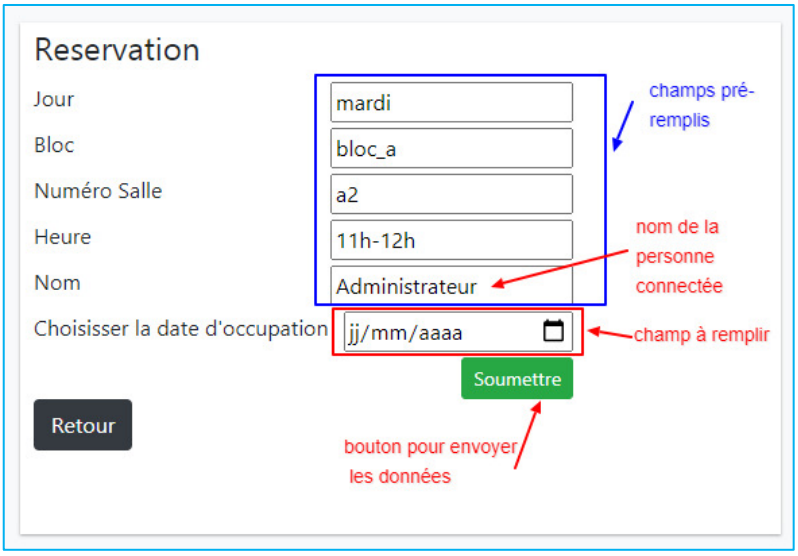


Figure 3. 44 : Détails explicatifs de la page de finalisation de la réservation

La personne remplie juste le champ relatif à la date et clic sur le bouton « Soumettre » pour envoyer les informations saisies à un script PHP afin d'insérer ces informations dans la base de données. Ces informations seront insérées dans la table « demande » de notre base de données.

a. Organigramme du script PHP de traitement de la réservation :

Variables	**Description**
$_POST	Tableau associatif contenant toutes les informations relatives à la réservation envoyées par l'utilisateur via le formulaire
bloc	Contient l'information du bloc
id	Contient le numéro de la salle choisie pour la réservation
date	Contient l'information sur la date de réservation

jour	Contient l'information sur le jour de l'emploi du temps
nom	Contient le nom de la personne qui souhaite faire la réservation
heure	Contient l'heure à laquelle la personne souhaite occuper la salle réservée
result	Résultat de la requête fait à la base de données pour vérifier si la date choisie n'existe pas déjà pour les autres informations

Tableau 3. 2 : table des variables du script de réservation

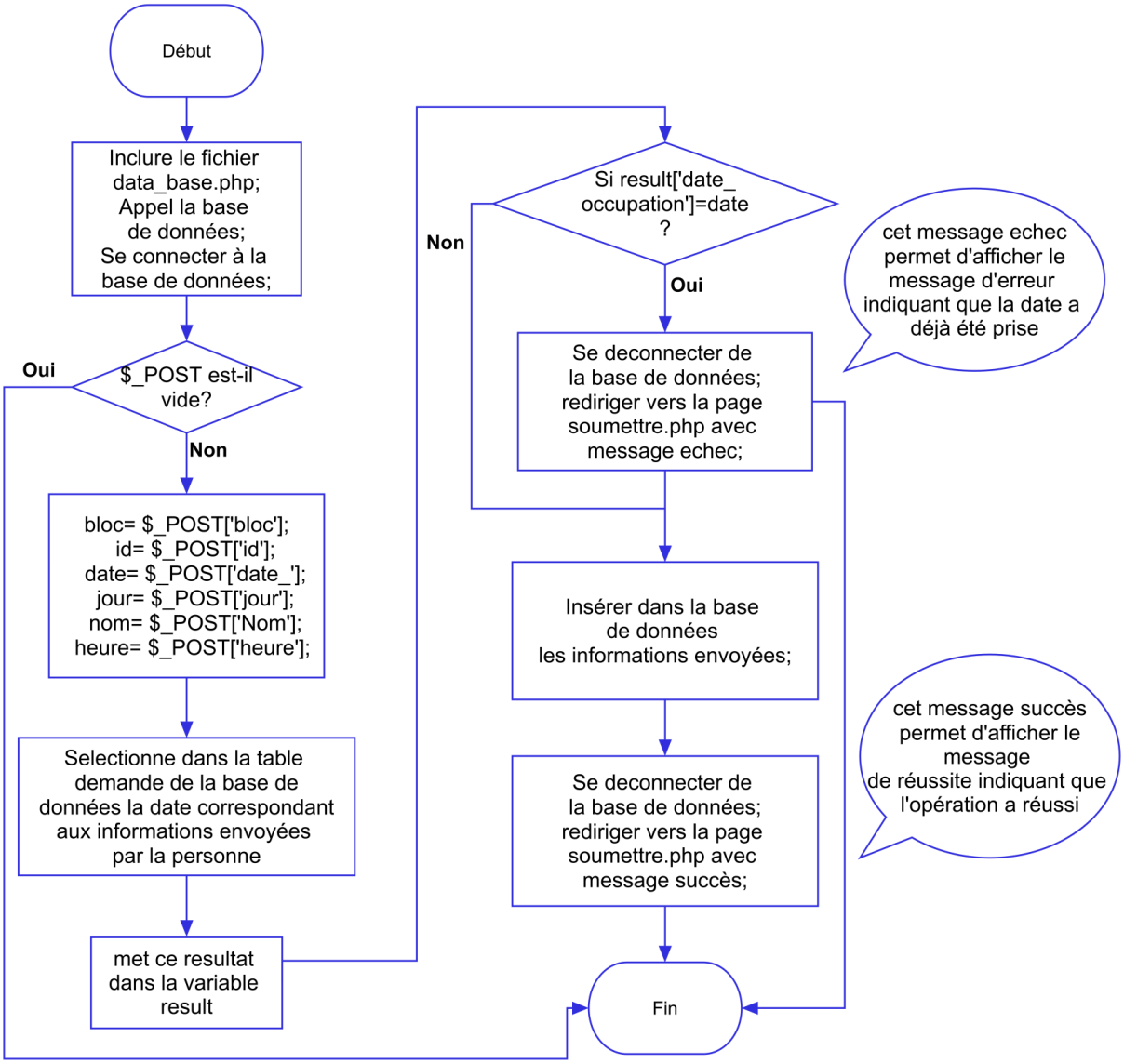


Figure 3. 45 : Organigramme du script php de réservation

b. Exemple de réservation :

- Cas 1 : utilisateur connecté Rebhi

Dans cet exemple la date choisie est le 11/09/2020. En cliquant sur « Soumettre », ces informations seront insérées dans la base de données.

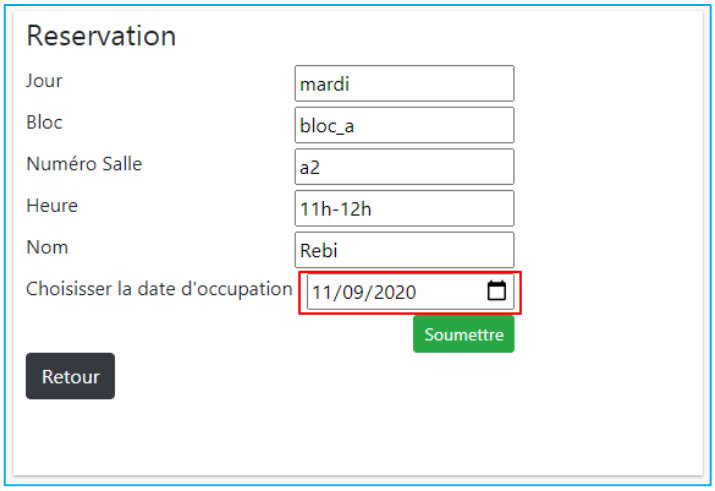


Figure 3. 46 : Réservation faite par l'utilisateur Rebhi

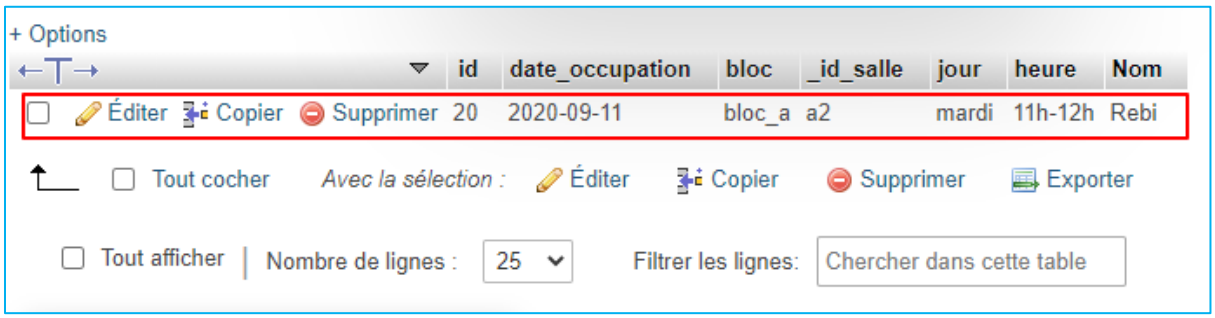


Figure 3. 47 : Réservation insérée dans la base de données

Si l'opération se passe correctement, alors un message de réussite est renvoyé par le script PHP qui effectue le traitement qui s'affichera en bas, les champs remplis sont vidés sauf le nom de la personne

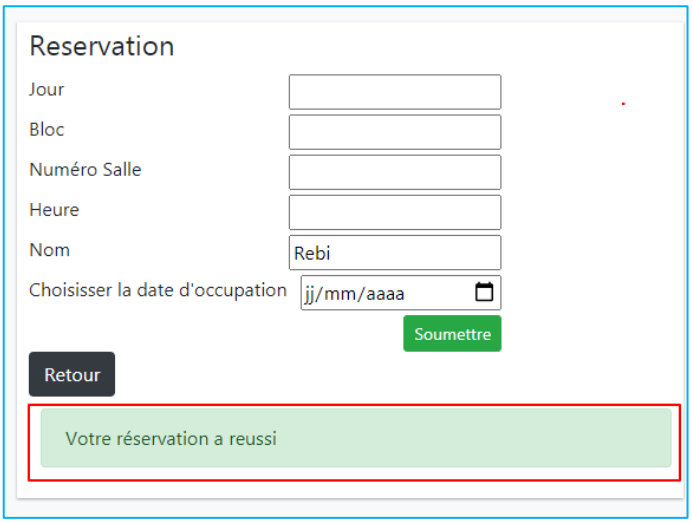


Figure 3. 48 : Notification de réussite de la réservation

- Cas 2 : utilisateur connecté Reddouane

Ici la date choisie est le 19/09/2020

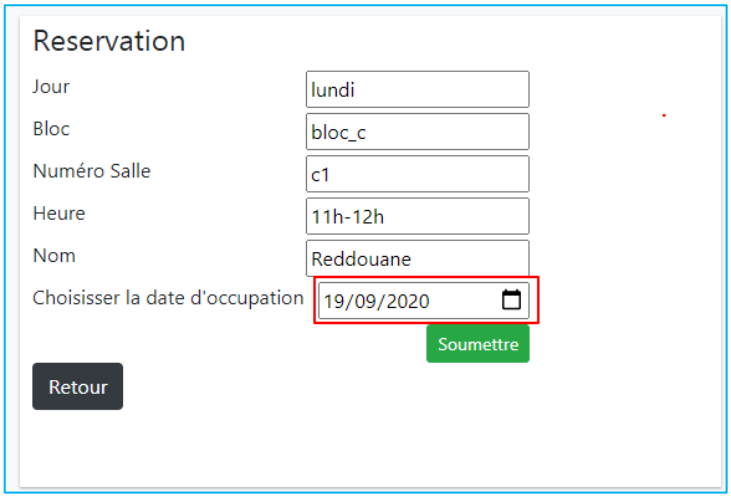


Figure 3. 49 : Réservation faite par l'utilisateur Reddouane

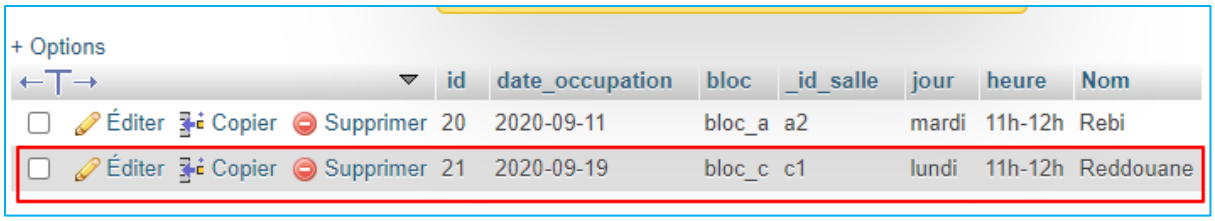


Figure 3. 50 : Réservation (Reddouane) insérée dans la base de données

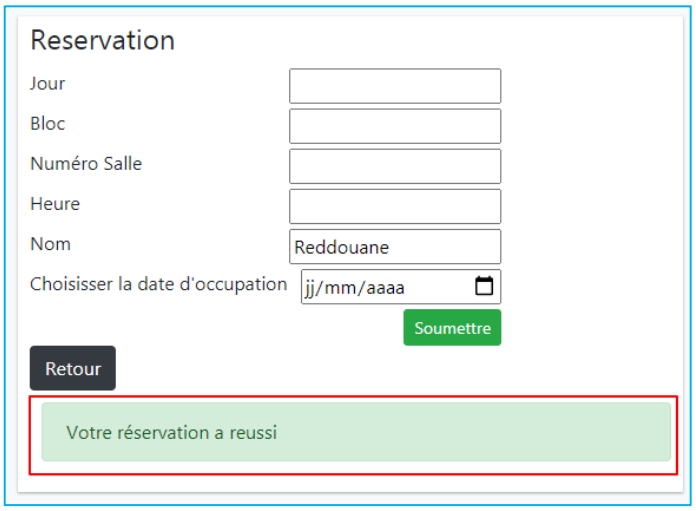


Figure 3. 51 : Notification de réussite de la réservation de Reddouane

Nous avons ajouté ce deuxième exemple pour illustrer ce qui peut se passer lorsqu'une personne essaye de réserver une salle pour une date qui se trouve déjà prise par une

autre personne pour la même salle, le même jour et le même horaire. Dans ce cas un message d'erreur s'affiche en bas pour indiquer à la personne que la date choisie a été déjà prise pour la salle concernée.

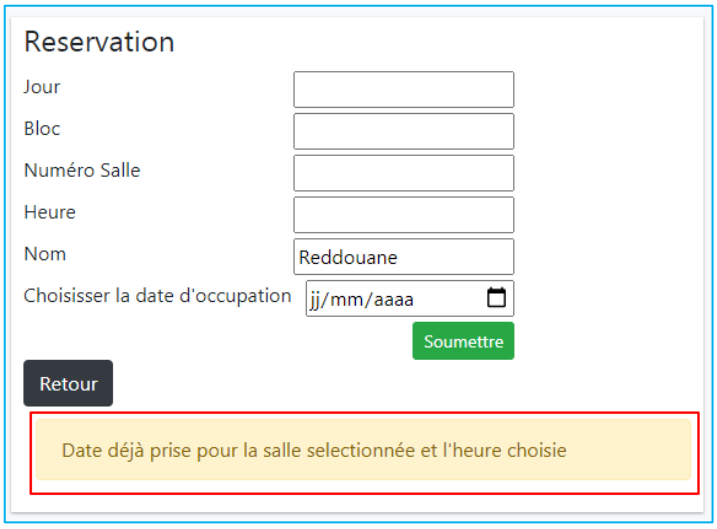


Figure 3. 52 : Notification d'échec de la réservation

III.3.4.3.5 Page de visualisation des réservations

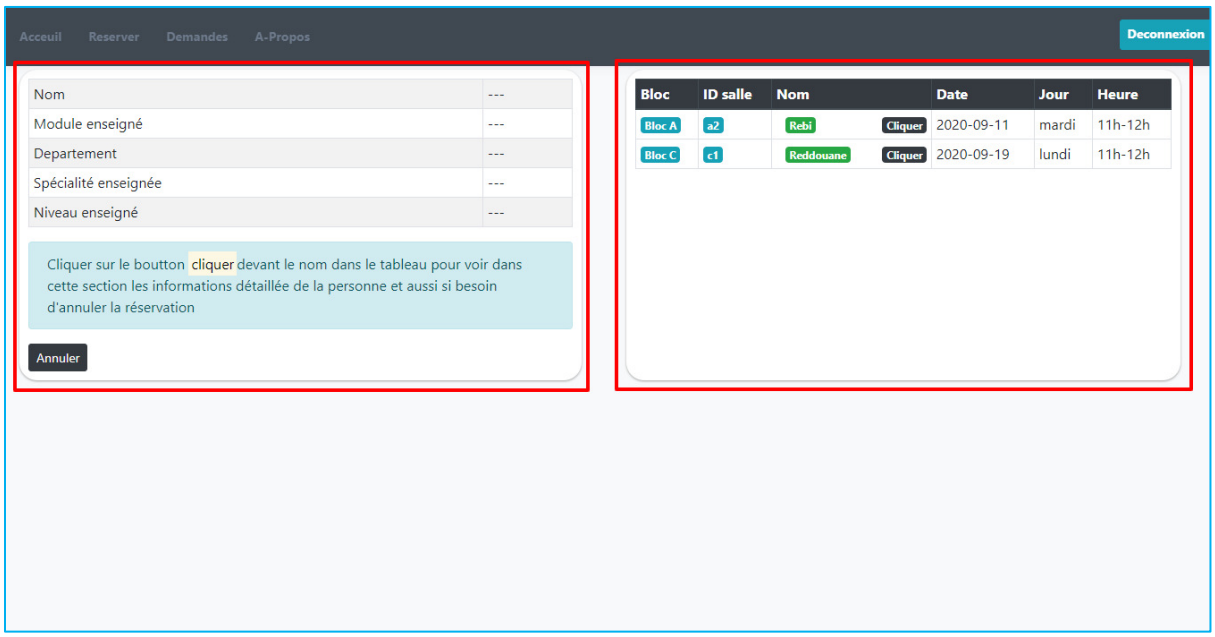


Figure 3. 53 : Page d'affichage des demandes de réservation

Cette page permet à l'administrateur du site de visualiser ou de supprimer les demandes de réservation. Ces informations sont récupérées de la table « demande » de la base de données et affichées sur la page. Elle comporte deux sections :

- La section droite permet d'afficher toutes les demandes de réservation qui ont été fait.

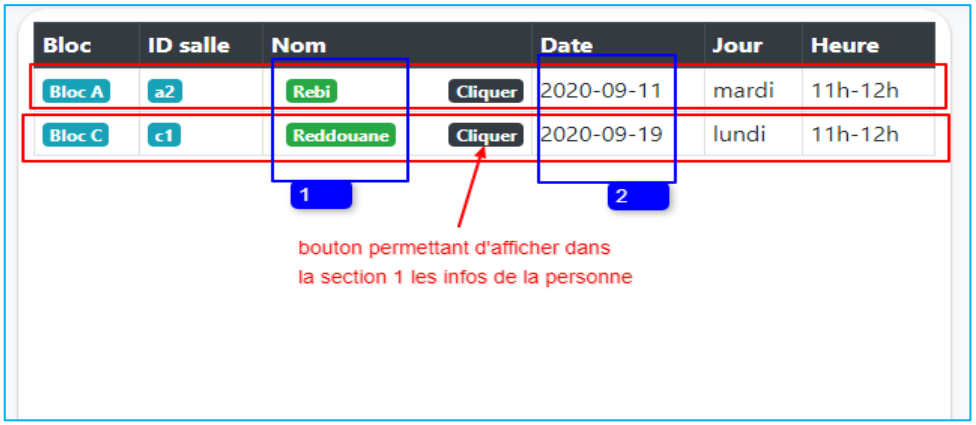


Figure 3. 54 : Affichage des réservations de salles

Nous pouvons remarquer ici que le contenu de cette section correspond aux deux entrées de réservation effectuées dans la partie qui traite de la page de réservation à savoir celle de :

1. Rebhi pour la date du 11/09/2020 ;
2. Reddouane pour la date du 19/09/2020.

- La section gauche permet d'afficher les informations relatives à la personne qui a fait la réservation et ce en les récupérant de la table « utilisateurs » de notre base de données.

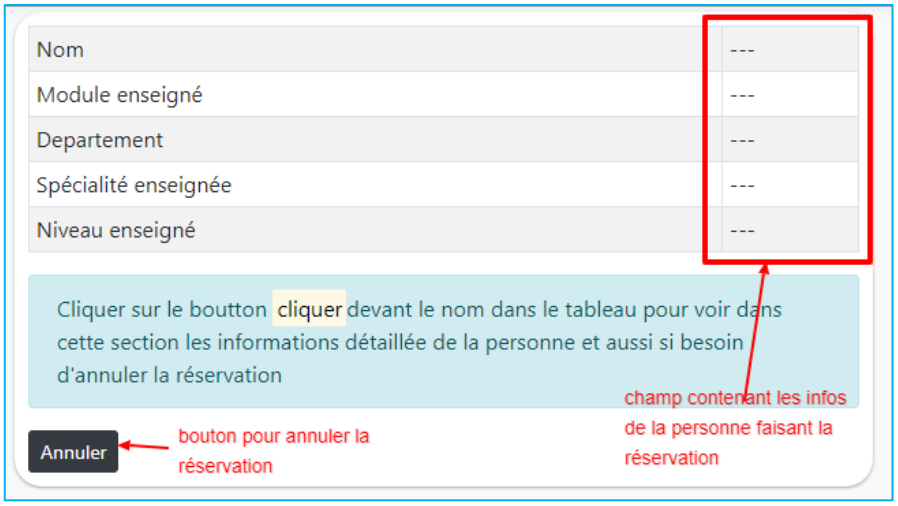


Figure 3. 55 : Section des détails de la personne ayant fait la réservation

Nom	role	departement	prof	specialite	niveau
Administrateur	1				
Azzeddine	0	Geni-électrique	Système RFID	Electronique des systèmes embarqués	Master 2
Abdellaoui	0	Geni-électrique	Système Embarqué	Electronique des systèmes embarqués	Master 2
Rebi	0	Geni-électrique	Microprocesseur	Télécom	Master 1
Reddouane	0	Geni-mécanique	Mécanique des Fluides	Conversion énergenitique	Licence 3
Abdou	0	Geni-civil	Matériaux de construction	Construction	Licence 1

Figure 3. 56 : Information des utilisateurs dans la base de données

Nom	Rebi
Module enseigné	Microprocesseur
Departement	Geni-électrique
Spécialité enseignée	Télécom
Niveau enseigné	Master 1

Figure 3. 57 : Info de la personne ayant fait la réservation 1 (Rebhi)

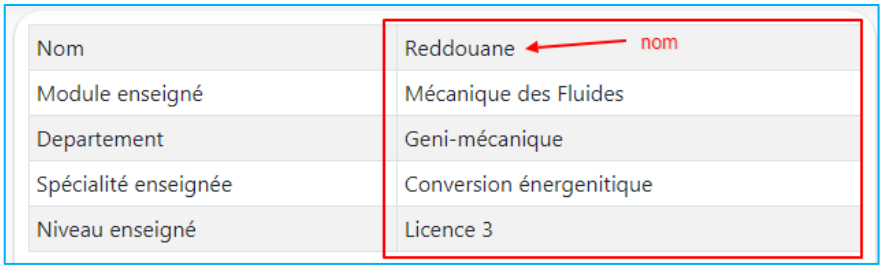


Figure 3. 58 : Info de la personne ayant fait la réservation 2 (Reddouane)

En cliquant sur le bouton « cliquer » devant le nom de la personne illustré dans la figure. Cela rend actif le bouton « annuler » de la figure et permet de supprimer cette réservation de la base de données.

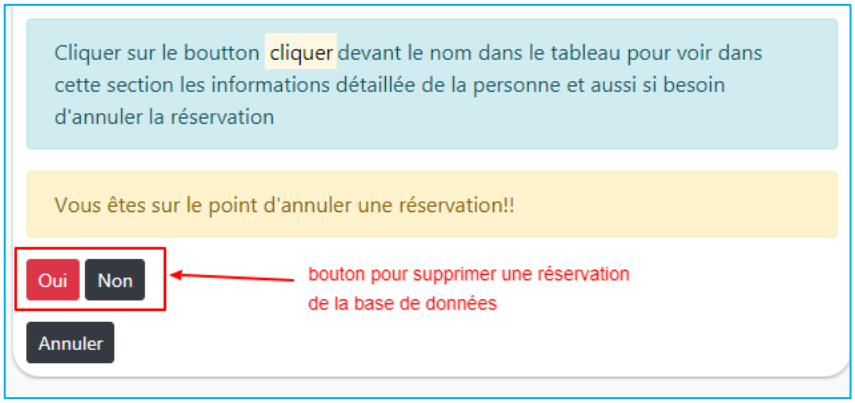


Figure 3. 59 : Bouton pour supprimer une réservation de la base de données

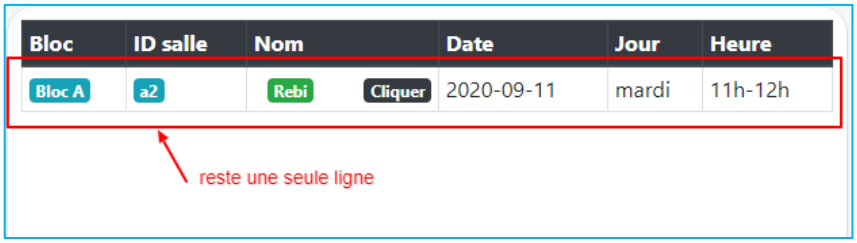


Figure 3. 60 : Affichage après suppression d'une réservation

III.4 Conclusion :

Ce chapitre étant le plus important du mémoire, il aura été riche en information et d'explication. Nous avons détaillé tout au long, le processus de réalisation de la carte d'accès à savoir : comment les composants sont reliés entre eux, le rôle de chacun d'eux, la logique du fonctionnement du système. Et aussi le processus de réalisation de l'application web à savoir : les différents outils de conception de web, le rôle de chaque page de l'application, le traitement et l'affichage des données. Dans le chapitre qui suit, nous ferons des tests de fonctionnement sur maquette.

Chapitre IV : Test de fonctionnement et implémentation sur la maquette

IV.1 Introduction

Après avoir détaillé le processus de réalisation de la carte d'accès et de l'application web dans le chapitre précédant.

Dans ce chapitre, nous ferons des tests pour s'assurer du bon fonctionnement de l'ensemble du système (carte d'accès et application web). Il fera l'objet de deux opérations principales à savoir : l'implémentation de la carte d'accès sur maquette et des tests de fonctionnement.

IV.2 Implémentation sur maquette

IV.2.1 Système sur plaque d'essai

Tout système nécessite une phase d'essai avant d'assembler les différents composants.

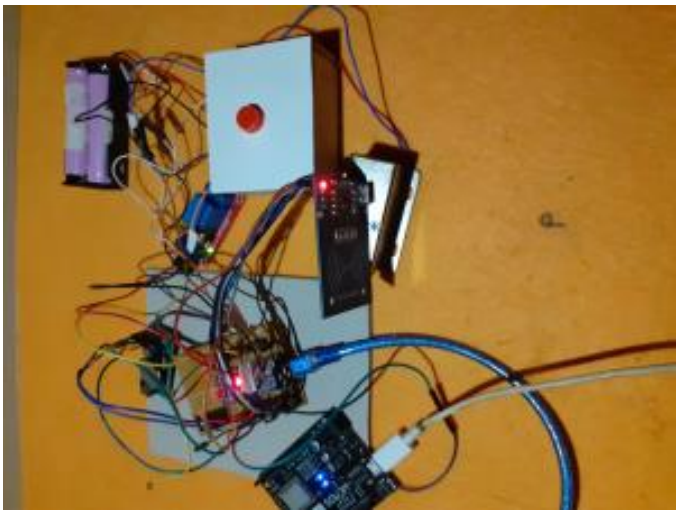


Figure 4. 1 : Système sur plaque d'essai

IV.2.2 Système sur maquette

Après avoir testé les différents composants sur une plaque d'essai afin de s'assurer de leur état de fonctionnement, nous sommes passé à l'implémentation sur la maquette finale.

Figure 4. 2 : système sur maquette

IV.3 Tests de fonctionnement

Cette phase consiste à faire des tests sur une journée ici le matin (de 8h00 à 8h40). L'unité horaire est de « **10 minutes ».** Donc nous aurons quatre séances (**8H00-8H10, 8H10-8H20, 8H20-8H30 et 8H30-8H40**).

IV.3.1 Test de lecture des tags RFID

Dans un premier temps on s'assure de la bonne lecture des Tags à savoir leur UID. L'UID (identifiant unique) correspond à une suite de 8 caractères hexadécimales. On obtient sur le moniteur série de l'IDE Arduino (branché sur le port COM3), le résultat ci-dessous :

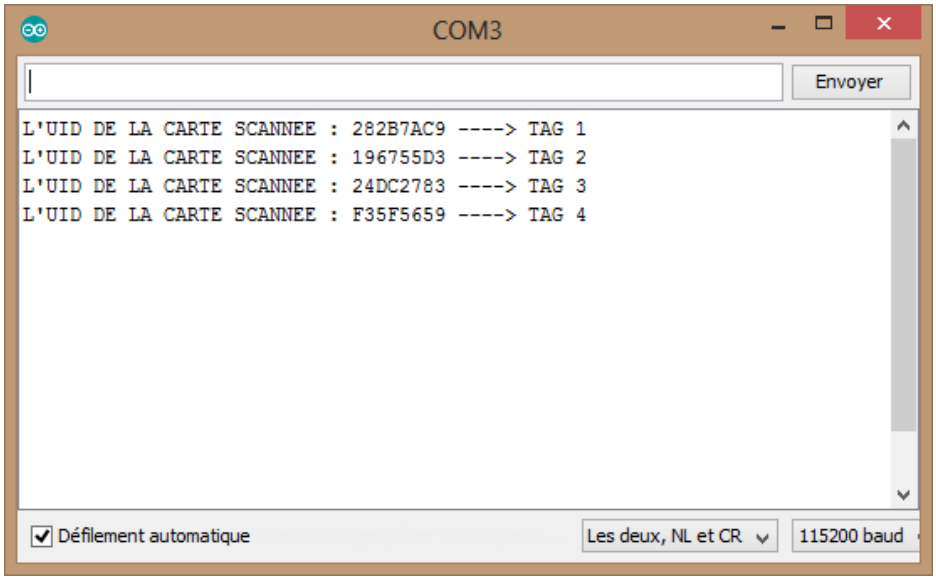


Figure 4. 3 : Communication entre Arduino et l'ordinateur

Chaque Tag (UID) sera associé à un professeur, un horaire et une salle. Ainsi nous définissons un emploi du temps pour les séances énumérées ci haut. Celui-ci sera utilisé par le programme de la carte d'accès et les scripts de l'applications web. Cela permettra de vérifier si les accès sont vérifiés correctement.

Nom	Horaire	Numéro Tag	UID	Salle
Reddouane	8H00-8H10	Tag 1	282B7AC9	Amphi 1
Rebhi	8H10-8H20	Tag 2	196755D3	Amphi 2
Azzeddine	8H20-8H30	Tag 3	24DC2783	Amphi 3
Abdellaoui	8H30-8H40	Tag 4	F35F5659	Amphi 4

Tableau 4. 1 : Emploi du temps

Chaque UID est également associé aux informations d'un professeur (comme indiquer dans le tableau ci-dessus) dans la base de données de l'application web. Cette donnée sera traitée par les scripts de l'application web lors de la réception de celle-ci depuis la carte d'accès après la validation de l'accès. Ce traitement s'effectue par comparaison aux UID qui sont dans la table « **utilisateurs** » de la base de données

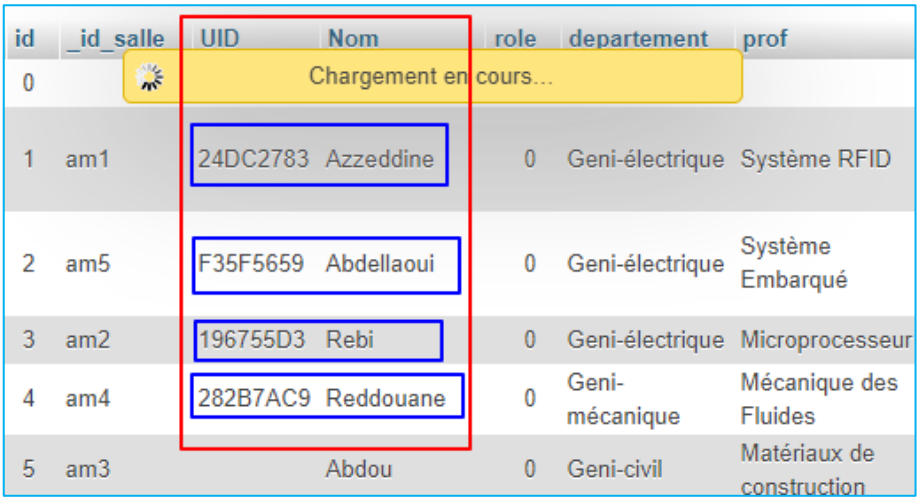


Figure 4. 4 : Association UID à utilisateur dans la base de données

IV.3.2 Test de réception du module wifi

Une fois l'information de la carte lue et celle-ci identifiée, son UID est envoyé au module wifi par voix série qui à son tour l'envoie au serveur de l'application web par requête HTTP pour les différents affichages. Notre module Wemos est branché sur le

port COM10. Le module renvoie un code, ce code fait partie du protocole HTTP, il vaut 200 si la requête a été validée. On obtient dans le moniteur série le résultat suivant :

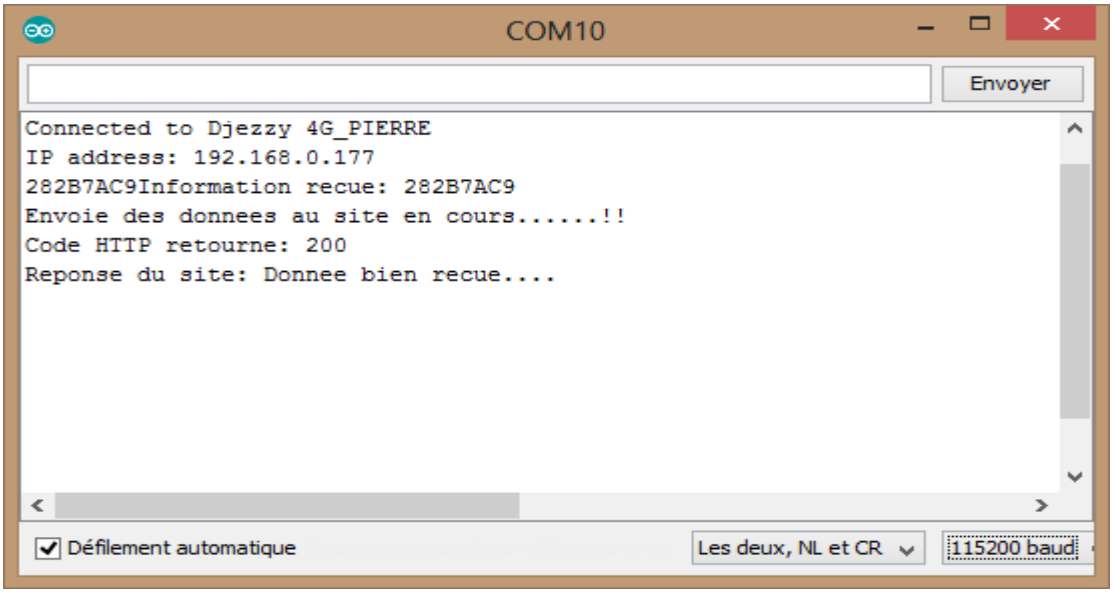


Figure 4. 5 : Réponse du module wifi suite à la requête au site web

IV.3.3 Test de réception par l'application web

Lorsque l'accès est validé par la carte d'accès. L'information de la carte est envoyée à l'application web que nous pouvons afficher sur une page web dans le navigateur.

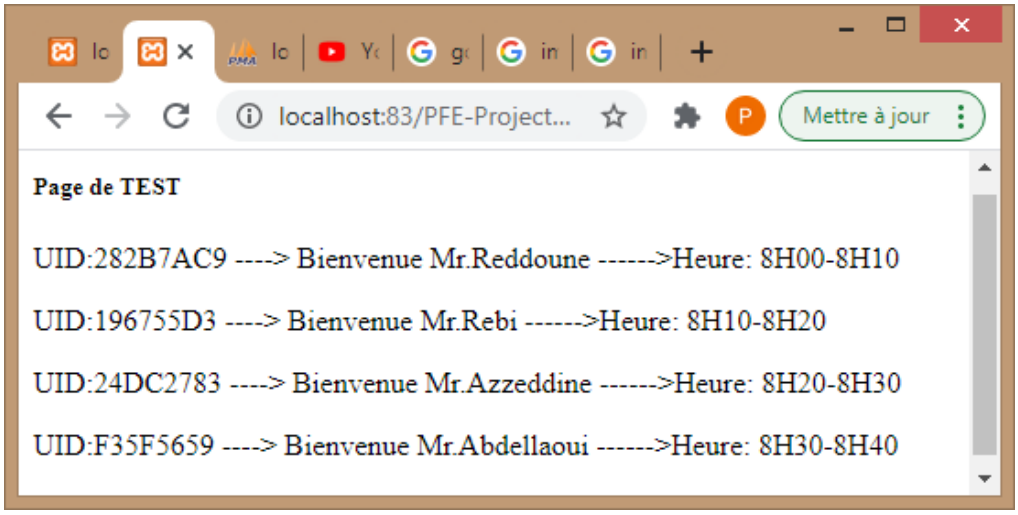


Figure 4. 6 : Page de test de réception dans le navigateur

IV.3.4 Test de séance: 8H00 - 8H10

Le test consiste en 2 points :

- L'enseignant se présente avant sa séance ici 8H ;

- Un autre enseignant essaye d'accéder à la salle ;
- L'enseignant se présente dans sa plage horaire qui est ici de 10 minutes (8H00 – 8H10) ;

1. Ce test concerne la première séance 8h00 – 8h10, plus précisément celle de Reddouane ayant le tag 1 portant comme UID : **282B7AC9.** S'il se présente avant 8h00, l'accès lui sera refusé

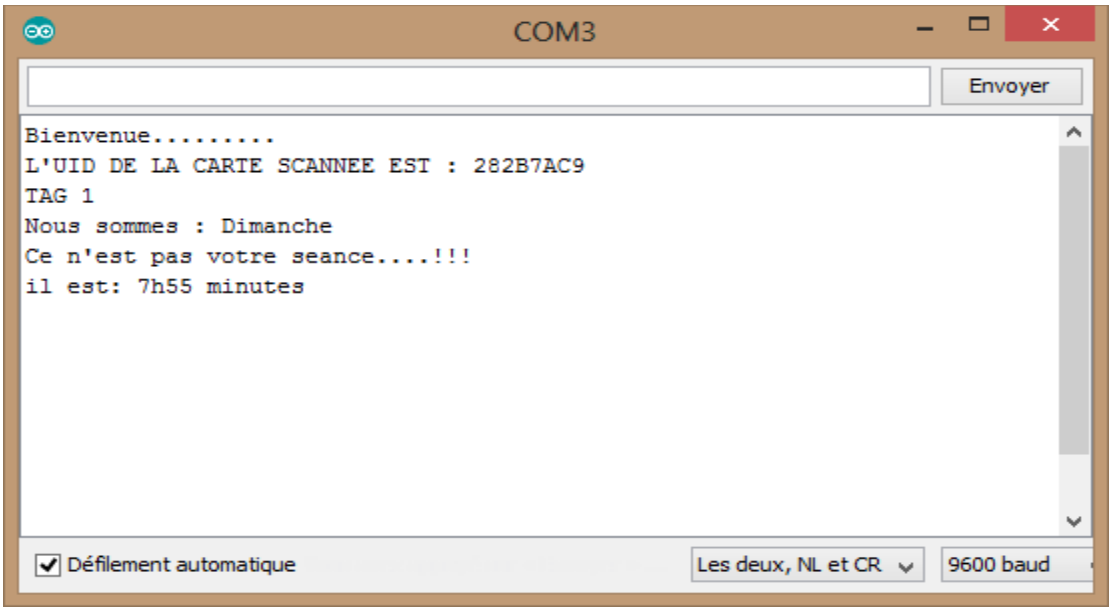


Figure 4. 7 : Résultat dans le moniteur du test avant 8h00

2. Si d'autres enseignants essayent d'accéder à cette salle durant cette séance de 8h00 – 8h10, l'accès leur sera également refusé. Pour cela nous utiliserons les tags 2 (UID=196755D3) et 3 (UID=24DC2783).

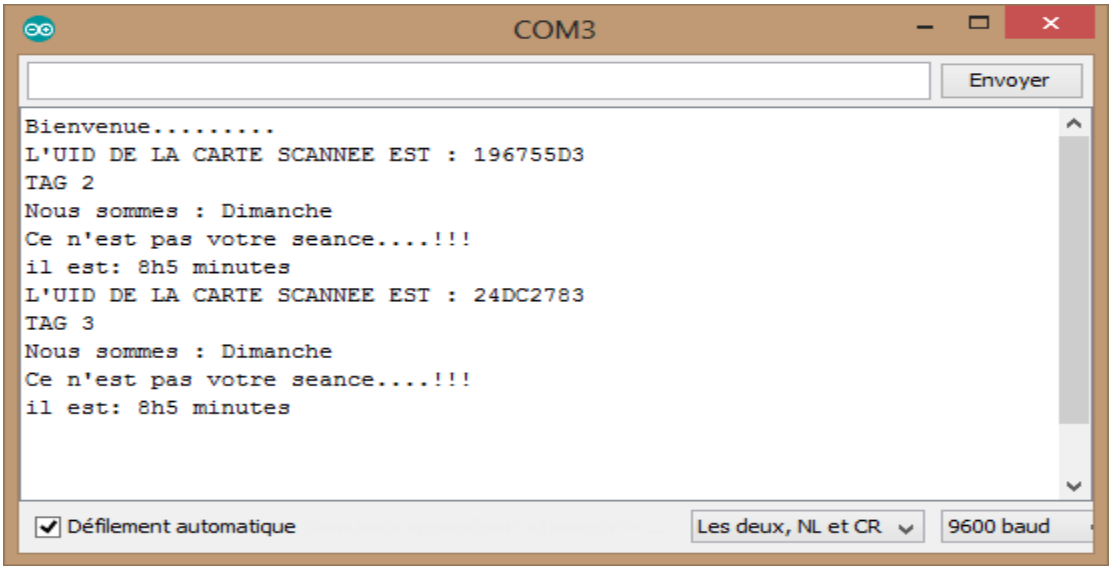


Figure 4. 8 : Résultat des tags non autorisés

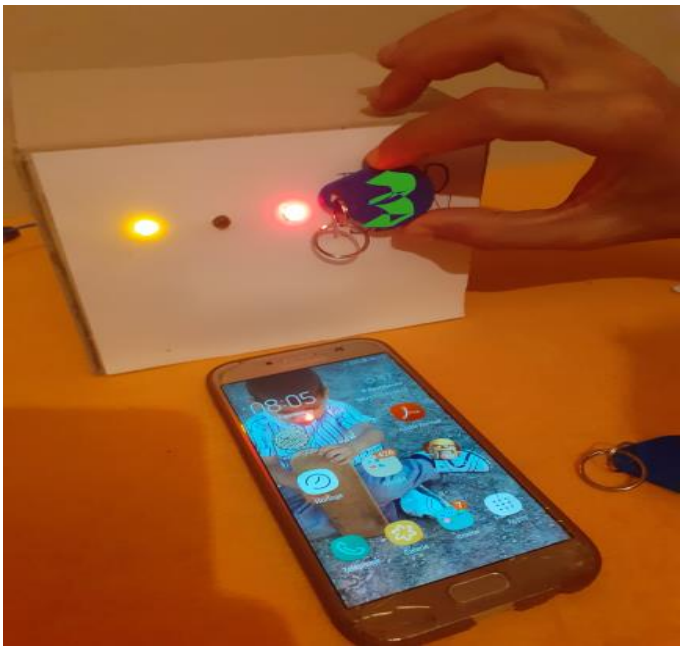


Figure 4. 9 : Visualisation sur la maquette

3. Et maintenant Mr. Reddouane se présente entre 8h00 et 8h10.

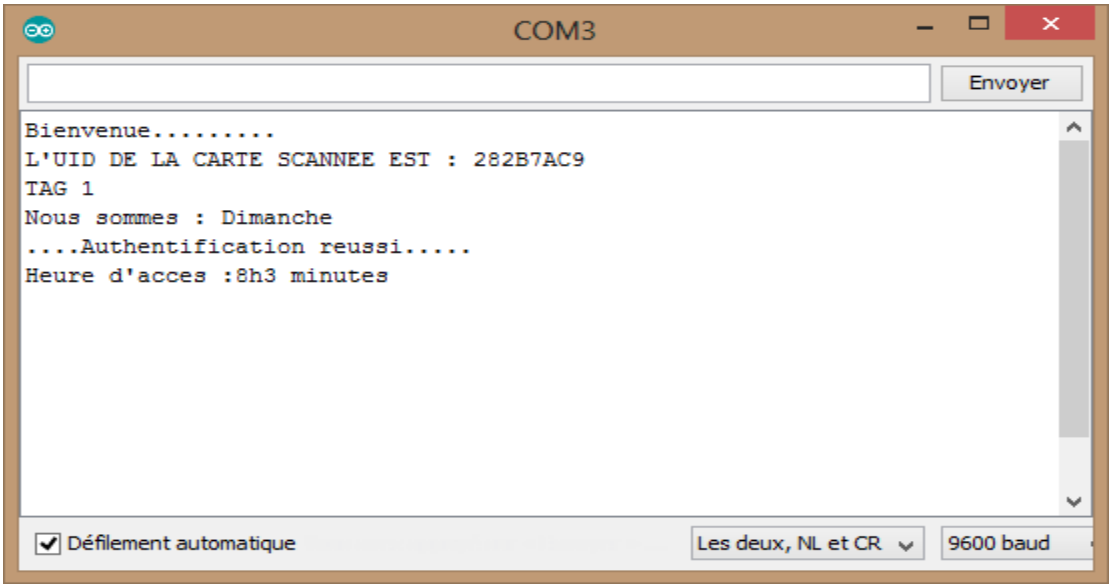


Figure 4. 10 : Résultat lors de la présentation à 8h00 dans le moniteur

Figure 4. 11 : led verte allumée sur la maquette pour signaler l'accès

Après la validation de l'accès, l'UID est transmis au module wifi qui à son tour l'envoie à notre application web. Notre site web renvoie un message « Donnée bien reçue » au module wifi que nous pouvons afficher dans le moniteur série.

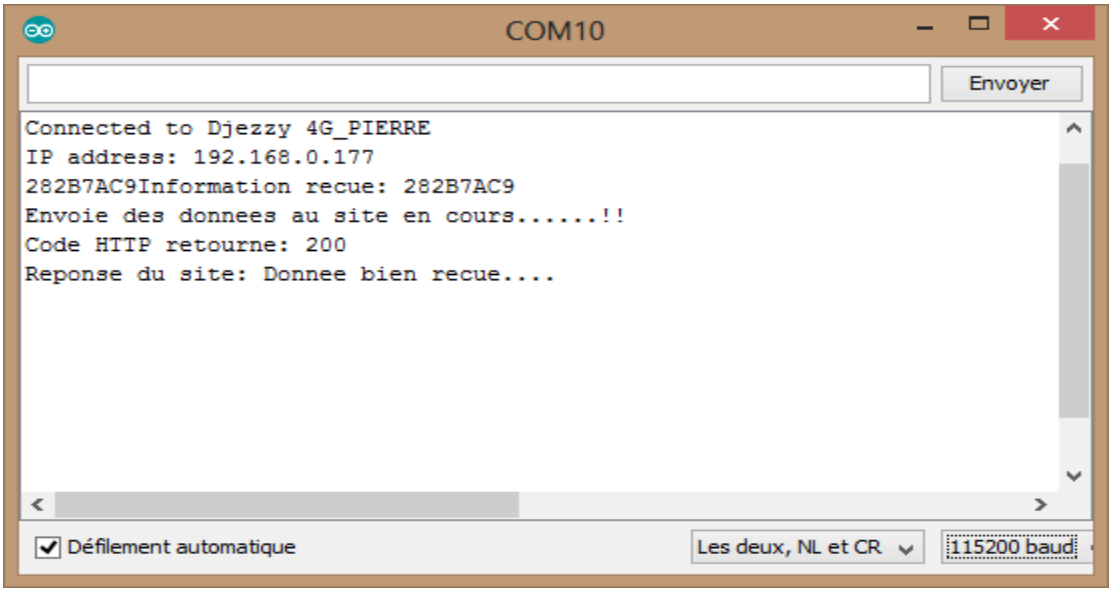


Figure 4. 12 : Réponse du module wifi

Lorsque les données sont reçues par l'application web, celle-ci change son affichage et nous pouvons voir que la colonne statut de la ligne 1 du tableau d'affichage correspondant à la salle 1 du hall amphithéâtre (amphi1) passe à « **occupée** » avec les autres salles à « **libre** » :

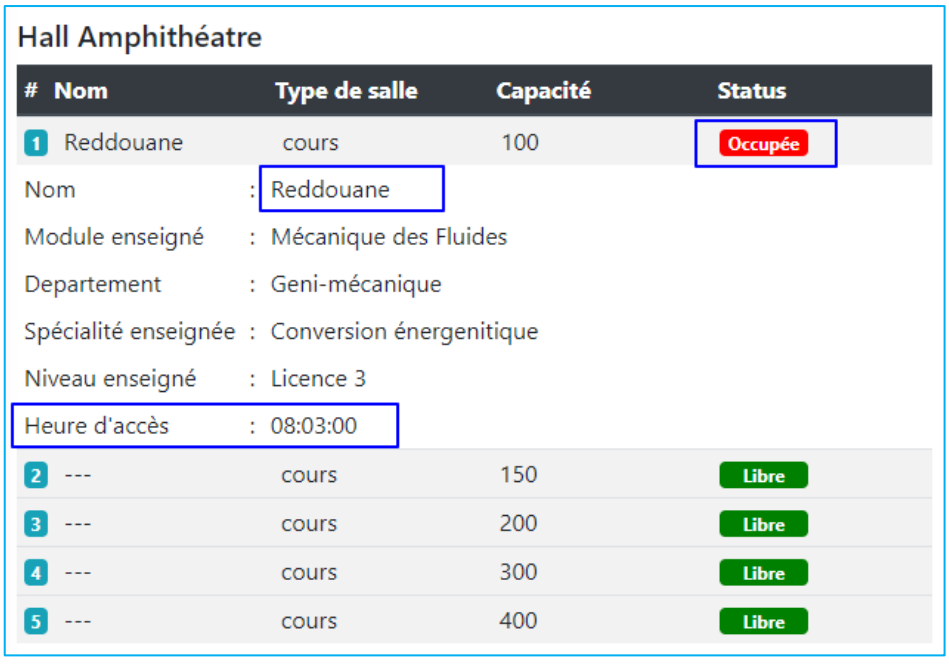


Figure 4. 13 : affichage dans l'application web

IV.4 Conclusion

Pour mettre en application notre système, des tests ont été réalisés. Ces tests portaient essentiellement sur la lecture (identification) des tags, l'authentification du tag par le système, le déverrouillage des portes, la transmission de l'information (UID) du tag au module wifi et à l'application web ainsi que l'affichage du suivi dans l'application web. Ainsi nous avons pu tester le fonctionnement de l'ensemble du système depuis le scanne du tag jusqu'à l'affichage dans l'application web. Ces tests nous ont permis de mettre en œuvres les trois principales fonctions d'un système de contrôle d'accès physique à savoir : l'identification et l'authentification, le traitement et le déverrouillage.

Conclusion Générale

Le contrôle d'accès physique est indispensable pour toute structure peu importe sa taille lorsqu'il s'agit de protéger des ressources, des biens ou seulement de contrôler l'accès.

Dans ce projet de fin d'étude, nos objectifs étaient de réaliser un système de contrôle d'accès physique basé sur la technologie des cartes sans contact avec une terminale (application web) de suivi des accès. Restreindre l'accès aux salles de cours suivant un emploi du temps pour contrôler les accès. Nous avons opté pour ce système de contrôle d'accès, de par son coût de réalisation bas par rapports aux autres systèmes de contrôle d'accès physique et d'autres part parce que c'est le système le plus vulgarisé et utilisé par les structures ou organismes pour leur contrôle d'accès, ce qui rend sa documentation plus accessible. Ainsi avec ce système, nous pouvons définir qui a accès, à quelle heure l'accès est autorisé et dans quelle condition ce qui est impossible avec les systèmes classiques (serrure et clé). Ainsi l'intégrité de l'emploi du temps est garantie tant pour les salles que pour les horaires. Aucun enseignant ne pourra accéder à une salle à laquelle il n'est pas rattaché dans l'emploi du temps et à un horaire qui n'est pas le sien. Notre système permet un audit plus facile des accès, chaque accès est enregistré dans la base de données de l'application web. Ainsi nous pouvons savoir qui a accédé à quelle salle et à quelle heure.

La réalisation de ce projet a été très instructif et informatif pour nous tant sur le plan électronique qu'informatique. Il nous a permis d'améliorer et d'approfondir nos connaissances sur les systèmes de contrôle d'accès et plus particulièrement sur les cartes sans contact (RFID), de découvrir les technologies de conception (HTML, CSS, PHP, JAVASCRIPT) d'un site internet. Mais également d'être confrontés aux problèmes que posent la conception et l'intégration d'un tel projet.

Comme difficulté rencontrée lors de la réalisation de ce projet, la réalisation de l'application web de gestion et de suivi car nous n'avions jamais travaillé auparavant avec les technologies (langages de conception) du web. Il nous a fallu du temps pour apprendre ces différents langages.

Comme perspectives à ce travail, nous proposons :

- ✓ De l'étendre aux étudiants afin de comptabiliser les présences ;
- ✓ D'inclure un protocole de cryptage des données lors d'échange d'information entre la carte d'accès et l'application web ou la terminale de gestion centrale, afin d'éviter qu'un individu mal intentionné ne dérobe les informations pour accéder frauduleusement à une salle.

Références Bibliographiques

[1] https://fr.wikipedia.org/wiki/Contrôle_d'accès_physique

[2] https://fr.wikipedia.org/wiki/Contrôle_d'accès

[3] http://www.nedap.info/post/qu-est-ce-que-le-contrôle-d-accès-est-pourquoi-est-ce-vital

[4] https://whatis.techtarget.com/fr/definition/Controle-dacces

[5] Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques.pdf, page 6 et 7

[6] g08_FABRE_projet_RFID_LEBORGNE_NDIAYE.pdf, page 9 et 10

[7] https://fr.wikipedia.org/wiki/Serrure

[8] https://fr.wikipedia.org/wiki/Cadenas

[9] https://fr.wikipedia.org/wiki/Clavier_à_code

[10] https://www.companeo.com/securite-electronique/guide/ le-controle-d-acces-1er-levier-de-la-securite

[11] https://fr.wikipedia.org/wiki/Biométrie

[12] Controles-acces-biometrie3.pdf, page 8 à 18

[13] https://fr.wikipedia.org/wiki/Interphone

[14] https://fr.wikipedia.org/wiki/Visiophonie

[15] https://fr.wikipedia.org/wiki/Lecteur_de_proximité

[16] https://entreprise-securite.net/2020/04/06/choisir-un-bon-controle-d-acces-pour-votre-pme-une-necessite

[17] https://fr.wikipedia.org/wiki/Radio-identification

[18] https://fr.wikipedia.org/wiki/Hypertext_Markup_Language

[19] https://fr.wikipedia.org/wiki/Feuilles_de_style_en_cascade

[20] https://fr.wikipedia.org/wiki/PHP

[21] https://fr.wikipedia.org/wiki/Structured_Query_Language

[22] https://fr.wikipedia.org/wiki/Base_de_données

[23] https://fr.wikipedia.org/wiki/Base_de_données_relationnelle

[24] https://fr.wikipedia.org/wiki/Serveur_informatique

[25] https://fr.wikipedia.org/wiki/Client-serveur

[26] https://fr.wikipedia.org/wiki/Hypertext_Transfer_Protocol

[27] RFID_REE_JPH.pdf, page 6 et 7

Liste des abréviations

PIN : Personal Identification Number

UTL : Unité de Traitement Local

EPROM : Erasable programmable Read Only Memory

IFF: Identification Friend or Foe

RFID : Radio Frequency Identification

UID : Unique Identifiant

RTC : Real Time Clock

HTR : Horloge Temps Réel

EPC : Electrical Product Code

BAP : Batterie Assisted Passive Tag

DSRC : Dedicated Short Range Communications

SAW : Surface acoustic Wave

WORM : Write Once Read Multiple

ISM : Industriel-Scientifique-Medical

IDE : Integrated Development Environment

HTML : HyperText Markup Langage

XML : Extensible Markup Langage

CSS : Cascading Style Sheets

PHP : PHP Hypertext Preprocessor

SQL : Structured Query Langage

WWW : World Wide Web

HTTP : HyperText Transfert Protocol

HTTPS : HyperText Transfert Protocol Secured

OSI : Open Systems Interconnection

TLS : Transfert Layer Security

SVG : Scalable Vector Graphics

JPG : Joint Photographic Experts Group

PNG : Portable Network Graphics

Annexe

La carte Arduino Nano

La **carte Arduino Nano** est une petite carte électronique faisant partie de la famille des cartes Arduino équipée d'un microcontrôleur basé sur **ATMega328** couplé à un **quartz de 16 MHz**. Le microcontrôleur permet, à partir d'événements détectés par des capteurs, de programmer et commander des actionneurs ; c'est donc une interface programmable. Pour la programmation on utilise l'interface IDE d'Arduino.

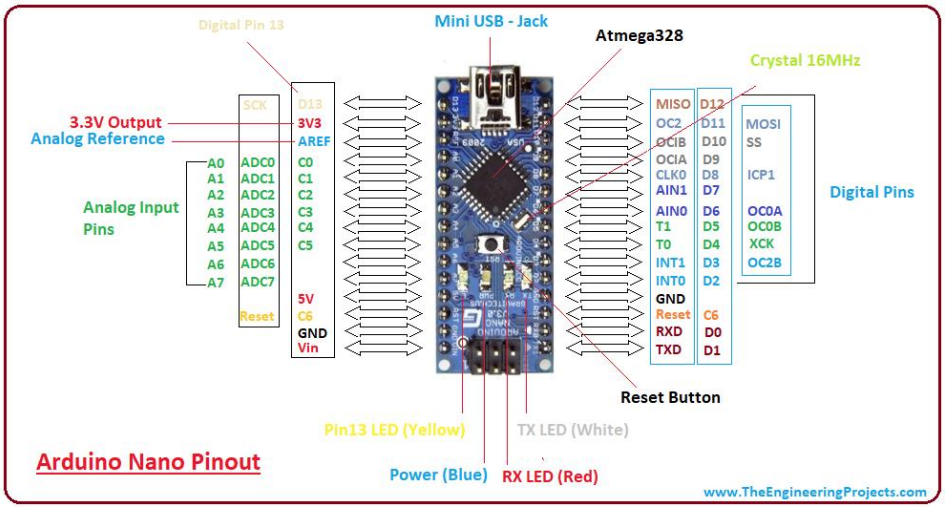


Figure a. 1 : carte Arduino nano

L'**ATmega328** est un microcontrôleur mono-puce créé par Atmel dans la famille mégaAVR. Il a un cœur de processeur RISC 8 bits à architecture Harvard modifiée. Le microcontrôleur Atmel 8 bits AVR RISC combine une mémoire flash ISP de 32 Ko avec des capacités de lecture en écriture, 1 Ko EEPROM , 2 Ko SRAM, 23 lignes d'E / S à usage général, 32 registres de travail à usage général , trois minuteries flexibles / compteurs avec modes de comparaison, interruptions internes et externes, USART programmable en série, interface série à 2 fils orientée octets, port série SPI, convertisseur A / N 6 canaux 10 bits (8 canaux dans les boîtiers TQFP et QFN / MLF) , la minuterie de surveillance est programmable avec l'oscillateur interne et cinq modes

d'économie d'énergie sélectionnables par logiciel. L'appareil fonctionne entre 1,8 et 5,5 volts. L'appareil atteint un débit approchant 1 MIPS par MHz [1].

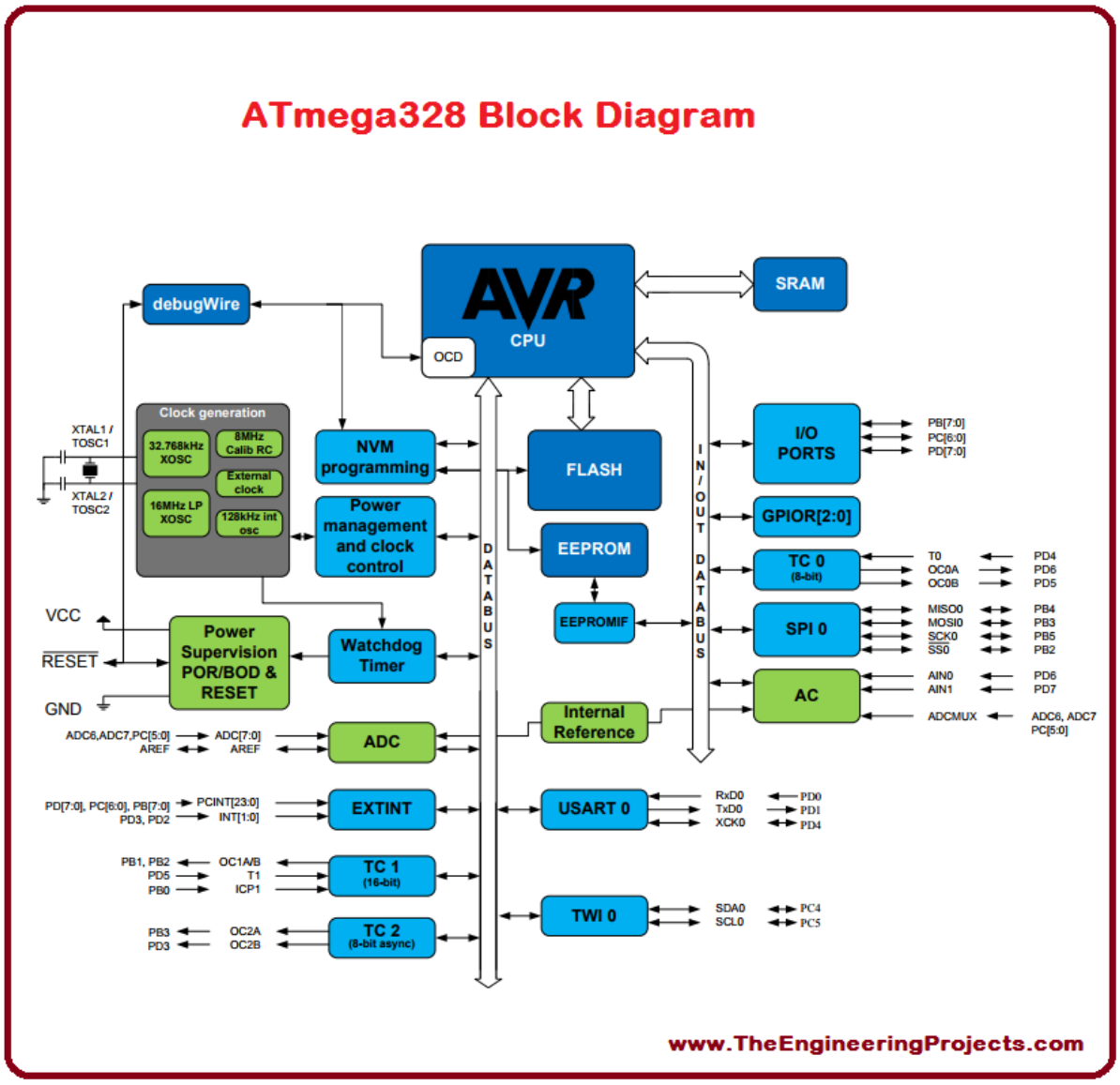


Figure a. 2 : diagramme de block de l'ATMEGA328

Caractéristiques [2] :

- Alimentation :
  - via port USB ou
  - 5 Vcc régulée sur broche 27 ou
  - 6 à 20 V non régulée sur broche 30 ;
- Microprocesseur : ATMega328 ;
- Mémoire flash : 32 kb ;

- Mémoire SRAM : 2 kb ;
- Mémoire EEPROM : 1 kb ;
- Interfaces :

  - 14 broches d'E/S dont 6 PWM ;
  - 8 entrées analogiques 10 bits ;
  - bus série, I2C et SPI ;
- Intensité par E/S : 40 mA ;
- Cadencement : 16 MHz ;
- Gestion des interruptions ;
- Fiche USB : mini-USB B ;
- Boîtier DIL30 ;
- Dimensions : 45 x 18 x 18 mm

[1] https://en.wikipedia.org/wiki/ATmega328

[2] https://www.gotronic.fr/art-carte-arduino-nano-12422.html

Le module Wemos (ESP8266)

Wemos est une carte de développement basée sur ESP8266. L'**ESP8266** est un circuit intégré à microcontrôleur avec connexion Wi-Fi développé par le fabricant chinois **Espressif**. Celui-ci, de taille réduite, permet de connecter un microcontrôleur à un réseau Wi-Fi et d'établir des connexions TCP/IP [3].

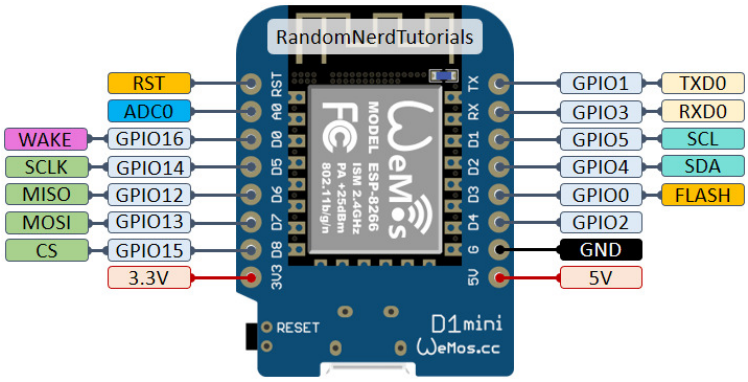


Figure a. 3 : module Wemos D1mini

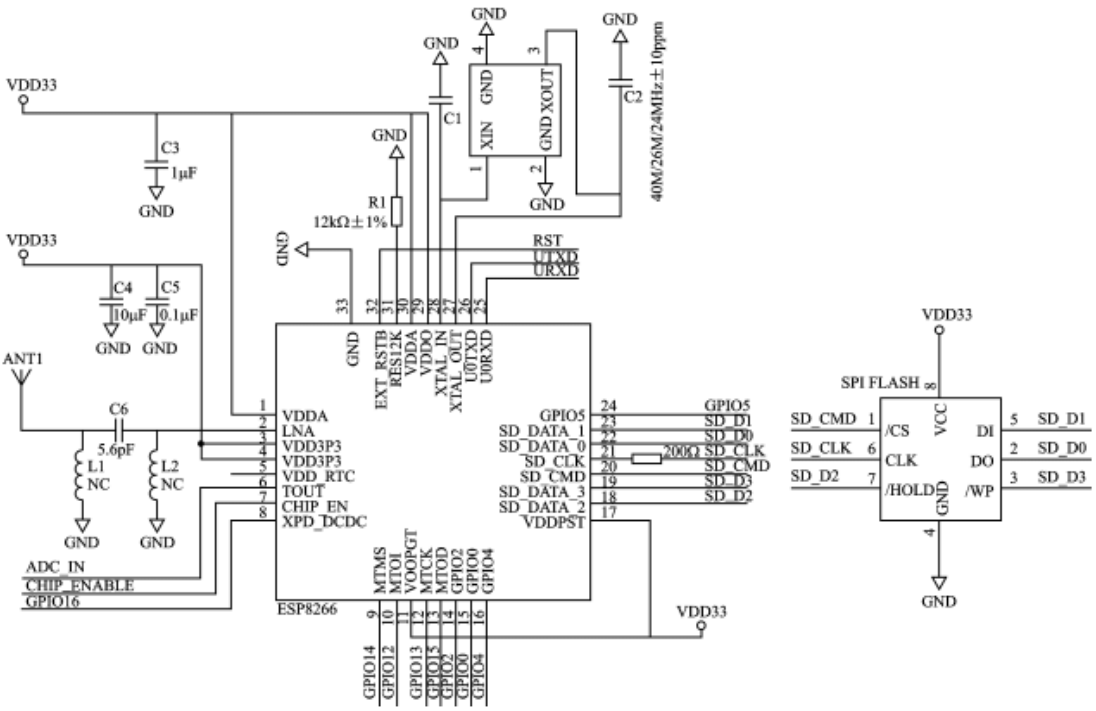


Figure a. 4 : Diagramme schématique de l'ESP8266

Caractéristiques [3] :

- 32-bit RISC CPU : Tensilica Xtensa LX106, 80 MHz ;
- 64 Ko de RAM instruction, 96 Ko de RAM data ;
- QSPI flash externe - 512 Ko à 4 Mo (supporte jusqu'à 16 Mo) ;
- IEEE 802.11 b/g/n Wi-Fi;
    - TR switch intégré, balun, LNA, amplificateur de puissance et matching network ;
    - Authentification par WEP ou WPA/WPA2 ou bien réseau ouvert
    - Certaines variantes supportent une antenne externe
- 16 broches GPIO
- Interfaces SPI, I²C ;
- Interface I²S avec DMA (partageant les broches avec les GPIO) ;
- UART sur des broches dédiées, plus un UART dédié aux transmissions pouvant être géré par GPIO2 ;
- 1-10 bits ADC

[3] https://fr.wikipedia.org/wiki/ESP8266

La Carte RFID MF-RC522 :

Le MF-RC522 est une puce de carte de lecture et d'écriture hautement intégrée appliquée à la communication sans contact avec comme fréquence 13,56 MHz. Lancé par la société NXP, il s'agit d'une puce de carte sans contact basse tension, peu coûteuse et de petite taille, un meilleur.

Le MF-RC522 utilise un concept de modulation et de démodulation avancé (modulation de charge) qui est entièrement présenté dans tous les types de méthodes et protocoles de communication passive sans contact 13,56 MHz. En outre, il prend en charge l'algorithme de cryptage CRYPTO1 rapide pour vérifier les produits MIFARE. Le MF-RC522 prend également en charge la série MIFARE de communication sans contact à haut débit, avec un débit de transmission de données bidirectionnel allant jusqu'à 424 kb / s. En tant que nouveau membre de la série de cartes de lecture hautement intégrées à 13,56 MHz, la MF-RC522 est très similaire aux MF RC500 et MF RC530 existantes lorsqu'il existe également de grandes différences. Il communique avec la machine hôte via la manière série qui nécessite moins de câblage. Vous pouvez choisir entre le mode SPI, I2C et UART série (similaire à RS232), ce qui permet de réduire la connexion, d'économiser de l'espace sur la carte PCB (taille plus petite) et de réduire les coûts [4].

Figure a. 5 : Carte RFID MRF-RC522

Diagramme de bloc :

Il possède un circuit analogique, un UART sans contact, un buffer type FIFO et un contrôle de travaux (job control) comme une interface hôte pour connecter les

composants au microprocesseur. Les drivers des Buffers de sortie du RC-522 activent la connexion directe de l'émission et réception de l'antenne sans amplification. Un nombre très large de registres sont utilisés pour la connexion du microprocesseur pour la lecture et écriture dans la programmation du RC-522.

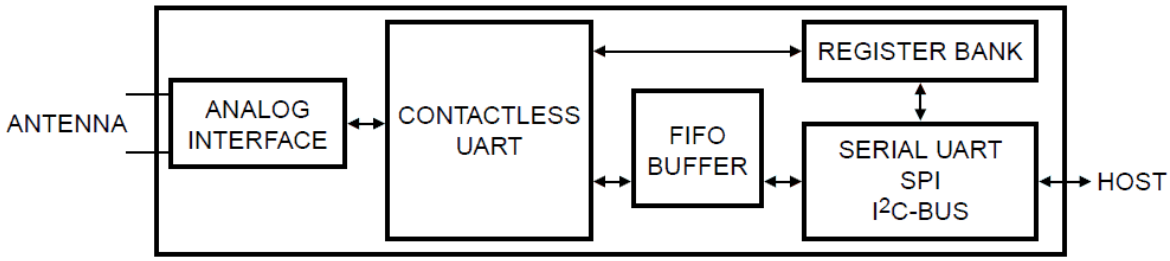


Figure a. 6 : Diagramme de bloc

Caractéristiques physiques [4] :

- Courant de fonctionnement : 13-26mA / DC 3.3V ;
- Courant de repos : 10-13mA / DC 3.3V ;
- Courant de veille : <80uA ;
- Courant de crête : <30mA ;
- Fréquence de fonctionnement : 13.56MHz Cartes prises en charge : mifare1 S50, mifare1 S70, mifare UltraLight, mifare Pro, mifare Desfire ;
- Taille :40 mm × 60 mm ;
- Température ambiante de fonctionnement : - 20 à 80 degrés centigrades ;
- Température ambiante de stockage : - 40 à 85 degrés centigrades ;
- Humidité relative ambiante : 5% à 95%.

[4] http://wiki.sunfounder.cc/index.php?title=Mifare_RC522_Module_RFID_Reader

Le module RTC-DS1302

Une **horloge temps réel** ou **HTR** (en anglais, *real-time clock* ou *RTC*) est une horloge permettant un décompte très précis du temps (par exemple en nanosecondes) pour un système électronique, en vue de dater ou déclencher des

évènements selon l'heure. On le retrouve le plus souvent sous la forme d'un **circuit intégré** incluant un **quartz piézoélectrique** [5].

Le module **RTC** (**Real Time Clock**) à base de **DS1302** est équipé d'une pile (**CR2032**) lui permettant de compter le nombre de tic émis par le **quartz 32**, même lorsque celui-ci est débranché. C'est le même principe que celui équipant les cartes mères depuis l'aube de l'informatique, lui permettant de garder en mémoire l'heure et la date, même si celui-ci est éteint ou coupé de toutes sources de courant [6].

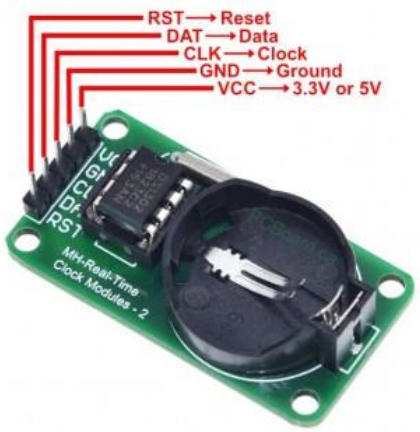


Figure a. 7 : module RTC DS1302

Le DS1302 est une puce d'horloge à charge lente, lancée par DALLAS aux Etats-Unis. Il intègre **8 RAM** statiques de **31 octets**. Il fournit des informations sur les secondes, les minutes, les heures, les jours, les semaines, les mois et les années. Il peut fournir la date au format 12h comme au format 24h. Il communique avec le MCU de manière série synchrone et n'a besoin que de trois câbles d'interface : câble de réinitialisation (**RST**), câble de données d'E / S (**SDA**) et câble d'horloge série (**SCL**) [7].

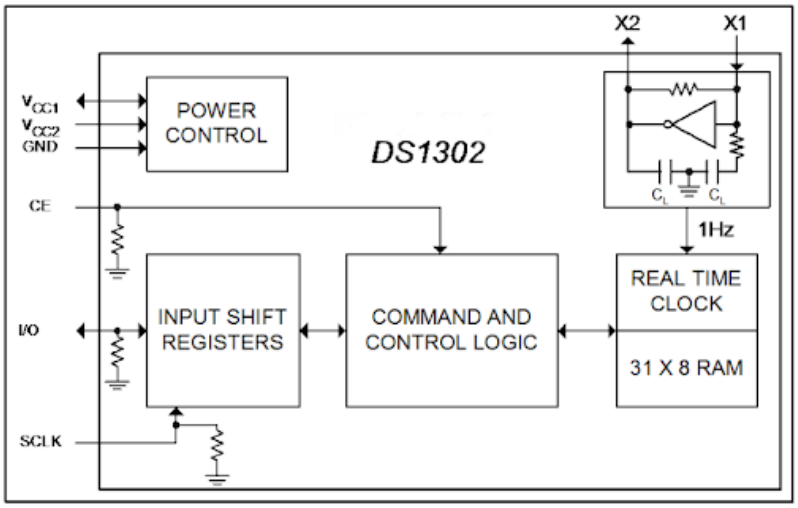


Figure a. 8 : Vue interne du circuit intégré DS1302

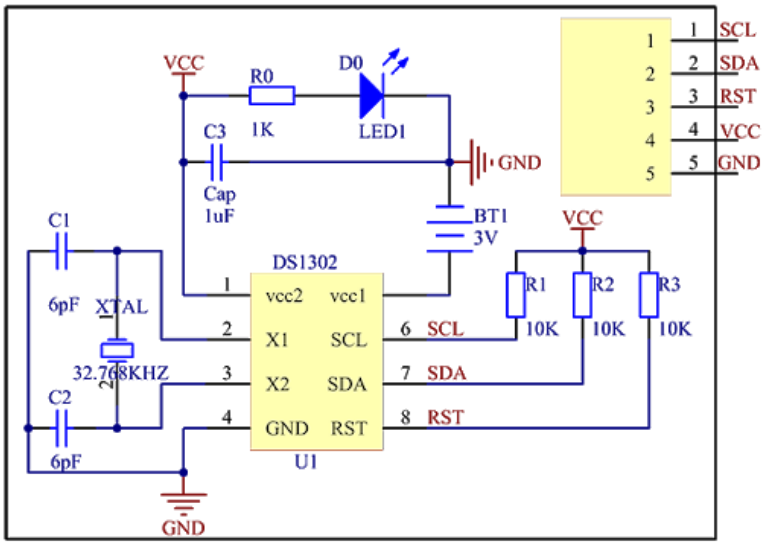


Figure a. 9 : Diagramme de block du module RCT-DS1302

PIN	NAME	FUNCTION
1	V_{CC2}	Primary Power-Supply Pin in Dual Supply Configuration. V_{CC1} is connected to a backup source to maintain the time and date in the absence of primary power. The DS1302 operates from the larger of V_{CC1} or V_{CC2}. When V_{CC2} is greater than V_{CC1} + 0.2V, V_{CC2} powers the DS1302. When V_{CC2} is less than V_{CC1}, V_{CC1} powers the DS1302.
2	X1	Connections for Standard 32.768kHz Quartz Crystal. The internal oscillator is designed for operation with a crystal having a specified load capacitance of 6pF. For more information on crystal selection and crystal layout considerations, refer to *Application Note 58: Crystal Considerations for Dallas Real-Time Clocks*. The DS1302 can also be driven by an external 32.768kHz oscillator. In this configuration, the X1 pin is connected to the external oscillator signal and the X2 pin is floated.
3	X2	
4	GND	Ground
5	CE	Input. CE signal must be asserted high during a read or a write. This pin has an internal 40kΩ (typ) pulldown resistor to ground. Note: Previous data sheet revisions referred to CE as $\overline{RST}$. The functionality of the pin has not changed.
6	I/O	Input/Push-Pull Output. The I/O pin is the bidirectional data pin for the 3-wire interface. This pin has an internal 40kΩ (typ) pulldown resistor to ground.
7	SCLK	Input. SCLK is used to synchronize data movement on the serial interface. This pin has an internal 40kΩ (typ) pulldown resistor to ground.
8	V_{CC1}	Low-Power Operation in Single Supply and Battery-Operated Systems and Low-Power Battery Backup. In systems using the trickle charger, the rechargeable energy source is connected to this pin. UL recognized to ensure against reverse charging current when used with a lithium battery.

Figure a. 10 : table de description de la fonction des pins

Caractéristiques [7] :

- Gère complètement toutes les fonctions de chronométrage
    - L'horloge en temps réel compte les secondes, les minutes, les heures, la date du mois, le mois, le jour de la semaine et l'année avec compensation des années bissextiles valable jusqu'à 2100
    - 31 x 8 RAM à usage général avec batterie
- Interfaces de port série simples avec la plupart des microcontrôleurs
    - Interface simple à 3 fils
    - Compatible TTL (VCC = 5 V)
    - Transfert de données sur un ou plusieurs octets (mode rafale) pour la lecture ou l'écriture de données d'horloge ou de RAM
- Le fonctionnement à faible consommation prolonge la durée de fonctionnement de la batterie de secours

- Fonctionnement complet de 2,0 V à 5,5 V
- Utilise moins de 300 nA à 2,0 V

- DIP 8 broches et SO 8 broches minimise l'espace requis
- Plage de température industrielle en option : -40°C à + 85°C Prend en charge le fonctionnement dans une large gamme d'applications.

[5] https://fr.wikipedia.org/wiki/Horloge_temps_réel

[6] http://wiki.funlab.fr/index.php/RTC-DS1302

[7] http://wiki.sunfounder.cc/index.php?title=RTC-DS1302_Module#Block_Diagram

La communication sans fil (Wi-Fi)

Un réseau sans fil (en anglais : Wireless network) est un réseau informatique numérique qui connecte différents postes ou systèmes entre eux par ondes radio. Il peut être associé à un réseau de télécommunications pour réaliser des interconnexions à distance entre nœuds [8].

Le Wi-Fi (Wireless Fidelity) est un ensemble de protocoles de communication sans fil régis par les normes du groupe **IEEE 802.11 (ISO/CEI 8802-11)**. Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, modem Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux [9].

Une radiocommunication est une télécommunication effectuée dans l'espace au moyen d'une transmission radio. L'information est transportée grâce à une modulation constante des propriétés de l'onde radio, soit son amplitude, sa fréquence, sa phase ou, entre autres, par la largeur d'une impulsion [10].

IEEE 802.11 est un ensemble de normes concernant les réseaux sans fil locaux (le Wi-Fi). Il a été mis au point par le groupe de travail 11 du comité de normalisation **LAN/MAN** de l'IEEE (IEEE 802). Le terme IEEE 802.11 est également utilisé pour désigner la norme d'origine **802.11** [11].

Taille	Normes définies par	
du réseau	l'IEEE	d'autres organismes
RAN	IEEE 802.22	
WAN	3GPP2 (1X-eVDO CDMA), IEEE 802.20 et IEEE 802.16e	3GPP (GPRS/UMTS/LTE), GSMA, OMA
MAN	IEEE 802.16d WiMax	ETSI HiperMAN & HiperACCESS
PAN	IEEE UWB, Bluetooth, Wi-Media, BTSIG, MBOA	ETSI HiperPAN
LAN	IEEE 802.11 Wi-Fi Alliance	ETSI-BRAN HiperLAN2

Figure a. 11 : Normes IEEE 802 selon la taille du réseau

Norme	Description	Remarque
IEEE 802.11a	Spectre de radiofréquences 5 GHz	Incompatible avec le spectre 2,4 GHz
IEEE 802.11b	Spectre de radiofréquences 2,4 GHz	Débit maximum de 11 Mbit/s
IEEE 802.11g	Spectre de radiofréquences 2,4 GHz	Débit maximum de 56 Mbit/s
IEEE 802.11n	Spectre de radiofréquences 2,4 GHz et 5 GHz	Débit maximum de 540 Mbit/s
IEEE 802.11ac	Spectre de radiofréquences 5 GHz	Débit maximum (théorique) de 1,3 Gbit/s

Figure a. 12 : Amendements principaux à la norme Wi-Fi IEEE 802.11

	IEEE 802.11b	IEEE 802.11a/11ac	IEEE 802.11g /11n	HiperLAN 1	HiperLAN 2	Bluetooth	ZigBee
Fréquence	Bande 2,4 GHz ISM	Bande 5 GHz ISM	Bande 2,4 GHz ISM	Bande 2,4 GHz ISM	Bande 5 GHz ISM	Bande 2,4 GHz ISM	Bande 2,4 GHz ISM + Bande 868+902-928 MHz
Technologies	DSSS	OFDM	OFDM	Narrowband	OFDM	FHSS	DSSS
Débit maximal	11 Mbit/s	54 Mbit/s / 1,3 Gbit/s	54 Mbit/s / 540 Mbit/s	23,5 Mbit/s	54 Mbit/s	1 à 3 Mbit/s	20 kbit/s à 250 kbit/s
Débit effectif	Environ 6 Mbit/s	Environ 30 Mbit/s / environ 400 Mbit/s	Environ 16 Mbit/s / environ 150 Mbit/s	Environ 20 Mbit/s	Environ 35 Mbit/s	0,7 à 2 Mbit/s	250 kbit/s
Portée	Maximum 50 m au débit maximal 500 m débit réduit	Maximum 30 m au débit maximal 500 m débit réduit	Maximum 30 m au débit maximal 500 m débit réduit	Maximum 150 m	Maximum 150 m	10 à 100 m	Maximum 10 m
Disponibilité	Mondiale	Mondiale	Mondiale	Européenne	Non déployé	Mondiale	Mondiale

Figure a. 13 : Caractéristiques des principales normes de réseaux locaux sans fil

Le modèle OSI (de l'anglais Open Systems Interconnection) est une norme de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions [12].

	PDU	Couche		Fonction
Couches hautes	Donnée	7	Application	Point d'accès aux services réseau
		6	Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
		5	Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment (en) / Datagramme	4	Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
Couches matérielles	Paquet	3	Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
	Trame	2	Liaison	Adressage physique (adresse MAC)
	Bit	1	Physique	Transmission des signaux sous forme numérique ou analogique

Figure a. 14 : Architecture en couches du modèle OSI

- La couche « **physique** » est chargée de la transmission effective des signaux entre les interlocuteurs. Son service est limité à l'émission et la réception d'un bit ou d'un train de bits continu (notamment pour les supports synchrones (concentrateur)).
- La couche « **liaison de données** » gère les communications entre deux machines directement connectées entre elles, ou connectées à un équipement qui émule une connexion directe (commutateur).
- La couche « **réseau** » gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets (cf. note ci-dessous).
- La couche « **transport** » gère les communications de bout en bout entre processus (programmes en cours d'exécution).
- La couche « **session** » gère la synchronisation des échanges et les « transactions », permet l'ouverture et la fermeture de session.
- La couche « **présentation** » est chargée du codage des données applicatives, précisément de la conversion entre données manipulées au niveau applicatif et chaînes d'octets effectivement transmises.
- La couche « **application** » est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme [12].

La norme **802.11** s'attache à définir les couches basses du **modèle OSI** pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire [9] :

- La couche physique (notée parfois *couche PHY*), proposant trois types de codages de l'information.
- La couche liaison de données, constitué de deux sous-couches : le contrôle de la liaison logique (**Logical Link Control**, ou **LLC**) et le contrôle d'accès au support (**Media Access Control**, ou **MAC**)

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche *liaison de données* définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations. Les normes 802.11 proposent donc en réalité trois couches (une couche physique appelée PHY et deux sous-couches relatives à la couche liaison de données du modèle OSI), définissant des modes de transmission alternatifs que l'on peut représenter de la manière suivante [9] :

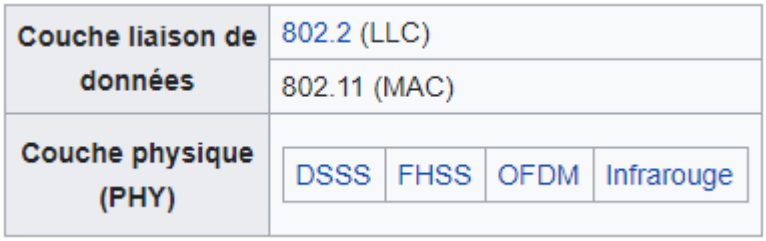


Figure a. 15 : couches physiques du protocole OSI

[8] https://fr.wikipedia.org/wiki/Réseau_sans_fil

[9] https://fr.wikipedia.org/wiki/Wi-Fi

[10] https://fr.wikipedia.org/wiki/Radiocommunication

[11] https://fr.wikipedia.org/wiki/IEEE_802.11

[12] https://fr.wikipedia.org/wiki/Modèle_OSI