REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE LARBI BEN M'HIDI -OUM EL BOUAGHI-
FACULTE DES SCIENCES EXACTES ET S.N.V
DEPARTEMENT MATHEMATIQUE ET DE L'INFORMATIQUE

MEMOIRE DE FIN D'ETUDE EN VUE DE L'OBTENTION DU

DIPLOME MASTER EN INFORMATIQUE

OPTION : VISION ARTIFICIELLE

Thème

Approche pour l'amélioration de la sécurité des systèmes informatiques

Elaborée par
M^lle^. AKOUD Fatima
M^me^. KABOUCHE Amel

Sous la supervision de
M^me^. BENGHIDA Amira

Devant le jury de soutenance suivants :

- Président : **HAMZA Lamia**
- Encadreur **: BENGHIDA Amira**
- Examinateur : **ZAITER Meriem**

Année Universitaire : 2022/2023

Remerciements

*Avant tout nous tenons à remercier **ALLAH** de nous avoir accordé la puissance, le courage, la patience, la volonté, la chance de l'étude et les moyens afin de pouvoir accomplir ce travail.*

*Nous remercions notre encadreur **BENGHIDA AMIRA** D'avoir accepté d'encadrer notre travail de fin d'études ainsi que pour son soutien, ses remarques pertinentes et son encouragement.*

*Nous remercions, tous **les professionnels** qui ont participé à la réalisation de ce mémoire de fin d'études et plus particulièrement les professionnels que nous avons interrogés.*

*Un grand merci à **nos parents, nos familles***

pour leurs encouragements, leurs soutiens inconditionnels

dont ils ont fait preuve.

Merci pour le soutien financier, moral, psychologique et matériel.

*Nos vifs remerciements vont également aux **membres du jury** pour l'intérêt qu'ils portent à notre travail en acceptant de l'examiner et de l'enrichir par leurs propositions.*

*Enfin, nous remercions l'ensemble **des collègues** de notre promotion pour cette année passée ensemble, dans les meilleurs moments comme dans les pires.*

RESUME

La sécurité des systèmes informatiques est une problématique d'une importance majeure aussi bien pour les individus que pour les entreprises. Elle repose sur la mise en place d'une politique de sécurité autour de ces systèmes.

Aujourd'hui, le système d'accès intelligent est devenu le moyen idéal pour gérer l'accès de tous les utilisateurs via des technologies avancées telles que la technologie de carte RFID et Arduino qu'on a adopté dans notre projet ainsi que l'attribution d'un mot de passe à chaque utilisateur pour améliorer davantage la précision et la sécurité du processus de vérification de la validité d'accès.

Mots Clés :

La sécurité des systèmes, contrôle d'accès, Tag, Mot de passe, Carte Arduino, Lecteur RFID, LED, Afficheur LCD, Diagrammes, UML, Application Arduino, C++.

ملخـــص:

يعد أمن أنظمة الكمبيوتر مشكلة ذات أهمية كبيرة للأفراد والشركات على حد سواء. وهو يقوم على تنفيذ سياسة أمنية حول هذه الأنظمة.

هذا اليوم، أصبح نظام الوصول الذكي الطريقة المثالية لإدارة الوصول لجميع المستخدمين، فهو يستخدم تقنيات متقدمة مثل RFID وتقنية بطاقة Arduino المعتمدة في مشروعنا بالإضافة إلى تخصيص كلمة مرور لكل مستخدم لزيادة تحسين الدقة وأمن عملية التحقق من الوصول الصالحة.

الكلمات المفتاحية:

أمان النظام، التحكم في الوصول، العلامة، كلمة المرور، بطاقة Arduino، قارئ RFID، LED، شاشة LCD، الرسوم البيانية، UML، تطبيق Arduino، C ++.

Abstract

The security of computer systems is an issue of great importance, important for both individuals and businesses. It is based on the implementation of a security policy around these systems.

Today, smart access system has become the ideal way to manage access for all users, it uses advanced technologies such as RFID and Arduino card technology adopted in our project as well as allocating a password for each user to further improve the accuracy and security of the valid access verification process.

Key Words :

System security, access control, Tag, Password, Arduino Card, RFID Reader, LED, LCD Display, Diagrams, UML, Arduino Application, C++.

TABLE DES MATIERES

CHAPITRE II :LE CONTROLE D'ACCES REALISES A BASE DE LA TECHNOLOGIE RFID

CHAPITRE III :IMPLEMENTATION

LISTE DES FIGURES

INTRODUCTION GENERAL

1. contexte

La Sécurité des systèmes informatique est un domaine extrêmement vaste puisqu'elle fait appel à de nombreux concepts juridiques, sociaux, et économiques, à la gestion de personnel, et à des connaissances techniques extrêmement pointues.

L'une des méthodes les plus importantes utilisées dans la Sécurité des systèmes informatique est le contrôle d'accès qui signifie les différentes solutions techniques qui permettent de sécuriser et gérer les accès physiques à une entreprise ou un site, ou les accès logiques à un système d'information. Les systèmes de contrôle d'accès sont des systèmes couramment utilisés pour marquer la présence dans les parkings, bureaux et les lieux de travail. Ces systèmes se sont considérablement améliorés, allant du marquage manuel des présences dans les registres de présence à l'utilisation d'applications de haute technologie. Lorsque nous parlons d'un système de contrôle d'accès physique, nous faisons généralement référence à un système de sécurité électronique. Ce dernier utilise généralement un identifiant, qui peut se présenter sous forme de badge d'accès, pour autoriser les personnes à pénétrer dans certaines zones. Et, comme le système est capable d'enregistrer qui est entré où et quand, il peut par la suite fournir des données précieuses pour nous aider à suivre l'utilisation de nos locaux et sites.

Dans ce projet, nous avons réalisé un système de contrôle d'accès on utilisant le module RFID (Radio Frequency Identification) via la carte Arduino pour contrôler l'accès en deux étapes :

L'une en vérifiant le badge RFID et le second par l'introduction d'un code personnel à travers un clavier matriciel, à la fin, notre système permet d'enregistrer la liste de présence.

2. Problématique

La sécurité est l'un des aspects les plus importants pour les entreprises. Le système de contrôle d'accès est l'une des approches importantes de la sécurité des systèmes informatiques qui régit l'accès aux zones nécessitant une protection selon les principes « qui, quand, où ? » et, éventuellement, « avec qui ». Un système de contrôle d'accès est un outil électronique responsable de contrôler les accès et vérifiant automatiquement si une personne a les autorisations pour accéder à une entreprise, les banques, les laboratoires de recherches …etc. La durée de ces autorisations est également définie. Celle-ci peuvent être unique, limitée dans le temps ou illimitée.

Donc quelle est la solution technique qui permet de sécuriser et gérer les accès physiques pour garantir une meilleure sécurité de notre système informatique ?

3. Objectifs

L'objectif principal de notre travail c'est faire la conception et le développement d'un système d'accès intelligent. Notre étude a ciblé la protection de l'information et les accès dans l'organisation.

En générale, et ses différentes structures en particulier, dont les permissions des utilisateurs sont déterminées par le système. Ainsi, notre système d'accès doit traiter d'une manière automatique et intelligente toutes les demandes d'accès aux ressources ou sites on utilisant. Pour développer notre système de contrôle et de surveillance d'accès, on a besoin d'étudier une nouvelle technique : la technologie RFID et la carte électronique ARDUINO.

4. Organisation du mémoire

Nous avons choisi notre sujet pour le contrôle d'accès à base de la technologie RFID et le présent mémoire est divisé en trois chapitres :

- Le premier chapitre présentera les différents systèmes de sécurité informatiques et on se basant sur l'approche du contrôle d'accès au différent système, leur principe de fonctionnement et les fréquences de communication utilisées.
- Le deuxième chapitre sera dédié à l'étude des différents éléments de notre système de sécurité sous forme d'une carte électronique y compris essentiellement la carte ARDUINO et le module RFID et la présentation du modèle de contrôle d'accès par le langage UML.
- Le dernier chapitre sera consacré à la présentation de notre système de sécurité et les différentes étapes de programmation (codes utilisés) et câblage.

CHAPITRE I

LA SECURITE INFORMATIQUE

I.1.Introduction :

L'information et la dépendance accrue à l'égard de l'information sont parmi les caractéristiques les plus importantes qui caractérisent l'ère moderne. Avec le développement rapide de la technologie, l'intérêt pour la sécurité de l'information augmente, les développeurs de systèmes et les utilisateurs doivent assurer la protection et la préservation des informations, la sécurité de l'information est la plus importante et l'un des problèmes les plus importants pour nous. Dans ce chapitre nous allons présenter la sécurité informatique ainsi que les techniques de Sécurité de l'information.

I.2. La sécurité informatique :

I.2.1. Définition de la sécurité informatique :

La sécurité informatique est l'ensemble des mesures techniques, organisationnelles, juridiques et humaines nécessaires pour maintenir, restaurer et assurer la sécurité des systèmes informatiques. Elle est étroitement liée à la sécurité de l'information et des systèmes d'information. Elle traite de la prévention des activités frauduleuses des utilisateurs de systèmes informatiques afin de garantir certaines conditions définies ci-après. **[1]**

I.2.2. Objectifs de la sécurité informatique :

- ✓ **La confidentialité**

Le but de la confidentialité est d'empêcher l'accès non autorisé à des informations confidentielles. Un tel accès peut être intentionnel, comme lorsqu'un intrus s'introduit dans un réseau et lit des informations, ou il peut être involontaire en raison de la négligence ou de l'incompétence de la personne qui traite les informations. Les deux moyens les plus importants pour garantir la confidentialité sont le cryptage et le contrôle d'accès. **[2]**

- ✓ **L'intégrité**

L'intégrité comprend trois objectifs qui contribuent à la sécurité des données :

- Empêcher les utilisateurs non autorisés de modifier les informations.
- Empêcher les modifications non autorisées ou accidentelles des informations par les utilisateurs autorisés.
- Maintenir la cohérence interne et externe :

Cohérence interne : Garantit que les données sont cohérentes en interne. Par exemple, dans une base de données d'organisation, le nombre total d'éléments détenus par l'organisation doit être égal au nombre total d'éléments répertoriés dans la base de données détenus par chaque élément de l'organisation.

Cohérence externe : Garantit que les données stockées dans la base de données sont cohérentes avec le monde réel. Par exemple, le nombre total d'articles sur l'étagère doit correspondre au nombre total d'articles dans la base de données. **[2]**

- ✓ **La disponibilité**

La disponibilité en informatique a pour but de garantir l'accès à une application, un système ou une donnée. L'impact d'une panne dépendra de la nature des activités de l'organisation affectées. **[3]**

- ✓ **La non-répudiation**

La non-répudiation est une méthode de protection de la transmission de messages entre les parties à l'aide de signatures numériques et/ou de cryptage. C'est l'un des cinq piliers de l'assurance de l'information (IA). Les quatre autres sont la disponibilité, l'intégrité, la confidentialité et l'authentification. **[4]**

- ✓ **L'authentification**

L'authentification est le processus permettant de déterminer si une personne ou une chose est vraiment ce qu'elle est censée être. **[5]**

I.2.3. Les différents types de sécurité informatique :

Il existe de nombreux types de sécurité informatique, car ils sont classés en fonction des fonctions et des tâches qu'ils exécutent. Les types de sécurité informatique appartiennent aux catégories suivantes :

- ✓ **Sécurité du réseau**

La sécurité réseau protège votre réseau et vos données contre les fuites, les intrusions et autres menaces. Il s'agit d'un terme large et général désignant les solutions et processus matériels et logiciels, ou les règles et configurations, liés à l'utilisation du réseau, à l'accessibilité et à la protection générale contre les menaces. **[6]**

- ✓ **Sécurité Internet**

La sécurité Internet est un terme collectif désignant un très large éventail de sujets qui affectent la sécurité des transactions sur Internet. En général, la sécurité Internet comprend la sécurité du navigateur, la sécurité des données saisies via les formulaires Web, ainsi que

l'authentification générale et la protection des données transmises via les protocoles Internet. **[7]**

- ✓ **Sécurité du nuage**

Dans la société d'aujourd'hui, nous sommes plus connectés que jamais. La sécurité du cloud est un large éventail de technologies, de politiques et d'applications utilisées pour protéger la propriété intellectuelle, les services, les applications et d'autres données en ligne sensibles contre les cybermenaces et les activités malveillantes.

- ✓ **Sécurité des applications**

La sécurité des applications est un terme utilisé pour décrire les mesures de sécurité au niveau de l'application qui protègent les données et le code contenus dans une application contre le vol ou l'utilisation abusive. Cela inclut non seulement les considérations de sécurité qui surviennent lors de la conception et du développement des applications, mais également les systèmes et les approches de sécurisation des applications après le déploiement.

I.2.4. Risques associés à la sécurité informatique :

Nous savons que la sécurité de l'information est la science de la protection de l'information contre les risques qui la menacent. Les risques liés à la sécurité informatique se répartissent en deux catégories : les perturbations du système et les attaques malveillantes ciblées. **[7]**

I.2.4.1. Les perturbations du système :

Les perturbations du système peuvent inclure des interruptions d'activité temporaires causées par des composants du système tels que des pannes de composants matériels, des pannes de réseau et des erreurs logicielles. Dans une telle situation, les entreprises risquent de perdre des ventes en raison d'un manque de capacité commerciale ou d'une atteinte à leur réputation.

I.2.4.2. Les attaques malveillantes ciblées :

- ✓ **Menaces persistantes avancées (APT)**

Les menaces persistantes avancées (APT) sont des cyberattaques durables et sophistiquées dans lesquelles un intrus établit une présence indétectable sur un réseau et vole des données sensibles sur une longue période de temps. Il s'agit d'une forme d'attaque soigneusement conçue et planifiée visant à infiltrer une orga nisation spécifique et à contourner les fonctions de sécurité existantes pour éviter d'être détectée. **[8]**.

- ✓ **Logiciels malveillants**

Un logiciel malveillant, ou malware, est un programme ou un code conçu pour endommager un ordinateur, un réseau ou un serveur. Les types de logiciels malveillants les plus courants sont les virus, les rançongiciels, les enregistreurs de frappe, les chevaux de Troie, les vers et les logiciels espions. **[8]**

- ✓ **Phishing**

Le phishing se produit lorsque les victimes sont amenées à partager des informations personnelles telles que des mots de passe et des numéros de compte bancaire, ou à télécharger des fichiers malveillants qui installent des virus sur leurs ordinateurs ou leurs téléphones via e-mail, SMS, téléphone, etc. Il s'agit d'un type de cyberattaque qui Réseaux sociaux. **[8]**

- ✓ **Attaques DoS ou DDoS**

Une attaque par déni de service (**DoS**) est une attaque ciblée qui inonde délibérément un réseau de fausses requêtes dans le but de perturber les activités de l'entreprise. Lors d'une attaque **DoS**, les utilisateurs sont incapables d'effectuer des tâches courantes et nécessaires, comme accéder à la messagerie électronique, à des sites web, à des comptes en ligne ou à d'autres ressources gérées par un ordinateur ou un réseau compromis.

Une attaque par déni de service distribué (**DDoS**) consiste à inonder la ressource ciblée de demandes afin de rendre un service ou un système (par exemple : serveur, ressource réseau ou transaction spécifique) inaccessible. **[8]**

- ✓ **Réseaux de robots ou botnets**

Un botnet est un ensemble d'ordinateurs compromis surveillés via des canaux de commande et de contrôle. Ceux qui exécutent l'infrastructure de commande et de contrôle, utilisent ces ordinateurs ou bots compromis pour compromettre le réseau de la cible, injecter des logiciels malveillants, collecter des informations d'identification ou lancer des attaques visant à effectuer des tâches nécessitant des calculs lourds. **[8]**

- ✓ **Menaces internes**

Les menaces internes sont des cyberattaques qui proviennent de l'intérieur d'une organisation, généralement par des employés actuels ou anciens.

Nous savons que la sécurité de l'information est la science de la protection de l'information contre les risques qui la menacent. Les risques liés à la sécurité informatique se répartissent en deux catégories : les perturbations du système et les attaques malveillantes ciblées. **[8]**

I.2.5. La gestion des risques liés à la sécurité de l'information :

La gestion des risques de sécurité de l'information (**ISRM**) est le processus de gestion des risques associés à l'utilisation des technologies de l'information. Comme mentionné précédemment, les organisations identifient et évaluent les risques pour la confidentialité, l'intégrité et la disponibilité des actifs informationnels. Ce processus peut être décomposé en deux composantes principales :

- ✓ **Évaluation des risques**

Processus consistant à combiner les informations recueillies sur les actifs et les contrôles pour définir le risque.

- ✓ **Traitement des risques**

Actions prises pour éliminer, atténuer, éviter, accepter, transférer ou contrôler les risques. Divers cadres peuvent soutenir la formulation de la stratégie **ISRM** d'une organisation. L'un des plus courants est le NIST Cybersecurity Framework, qui comprend les activités suivantes :

- ✓ **Identifier**

Les activités du groupe visent à développer les connaissances sur les risques de cybersécurité pour les systèmes, les personnes, les actifs, les données et les capacités. Connaître le contexte de votre entreprise, les besoins de votre entreprise et les risques associés vous aide à identifier les menaces et à hiérarchiser vos efforts de sécurité. Les activités à ce stade comprennent la gestion des actifs, la gouvernance et l'évaluation des risques.

- ✓ **Protéger**

Les organisations mettent en œuvre des sauvegardes et des contrôles de sécurité appropriés pour protéger leurs actifs les plus critiques contre les cybermenaces. Ces activités comprennent, par exemple, la gestion des identités et le contrôle d'accès, la sensibilisation et la formation des employés.

- ✓ **Détecter**

Les organisations doivent identifier rapidement les événements susceptibles de présenter un risque pour la sécurité des données. Les organisations s'appuient généralement sur des techniques de surveillance continue de la sécurité et de détection des incidents.

- ✓ **Réagir**

L'organisation prend des mesures en cas d'incidents de cybersécurité détectés. Les organisations peuvent limiter l'impact des incidents à l'aide de techniques telles que la planification de la réponse, la communication, l'analyse, l'atténuation et la résolution.

- ✓ **Récupérer**

L'organisation conçoit et met en œuvre des activités pour restaurer les fonctionnalités et les services affectés par les incidents de sécurité. Les activités de ce groupe contribuent à un retour rapide aux opérations normales pour atténuer l'impact de l'incident. Cela comprend les plans d'itération, les améliorations (telles que l'introduction de nouvelles politiques ou la mise à jour des politiques existantes) et les plans de communication.

I.2.6. Les approches pour améliorer la sécurité informatique :

- ✓ **Rédiger une politique de cyber sécurité et une charte informatique**

En premier lieu, il est toujours important de déterminer le périmètre du système d'information. Quelles applications et données devez-vous protéger, quels sont vos points faibles ?

Cela vous donne une vue d'ensemble des faiblesses et des forces de votre SI, et peut vous aider à vous orienter dans la bonne direction pour améliorer la sécurité informatique de votre entreprise. Le rôle de la charte informatique est de sensibiliser tous les utilisateurs aux bonnes pratiques et de rendre compte de leur rôle dans la protection des données. **[9]**

- ✓ **Sensibiliser ses collaborateurs**

Oui, car sensibiliser les collaborateurs aux bonnes pratiques de cybersécurité est essentiel. Il est important de les sensibiliser aux différents enjeux et de leur expliquer les risques et pourquoi l'amélioration de la sécurité de l'information est si importante. Cela vous permet de réagir intelligemment au chaos, aux e-mails suspects ou aux menaces sur votre poste de travail. Chaque utilisateur peut également identifier les comportements à risque et apporter les modifications nécessaires (utiliser des mots de passe forts, interdire des postes de travail, contrôler la diffusion des fichiers au sein de l'entreprise, etc.). **[9]**

- ✓ **Protéger physiquement son infrastructure**

La cybersécurité ne concerne pas seulement les réseaux informatiques ! La sécurité physique des équipements informatiques doit également être prise en compte. Améliorer la sécurité informatique d'une entreprise signifie également protéger les équipements de protection coûteux contre les dommages ou les dysfonctionnements. Cela vous permet de mieux protéger le contenu de votre ordinateur, serveur et logiciel de stockage. N'hésitez pas à combiner le tout avec un dispositif de détection de fuite d'eau ou d'incendie et amenez vos équipements sensibles dans un local sécurisé, verrouillé et dédié avec contrôle d'accès. **[9]**

- ✓ **Sécuriser l'accès à Internet**

L'accès Wi-Fi peut également être une source de cyberattaques. Pour améliorer la sécurité informatique de votre entreprise, vous devez protéger vos systèmes du monde extérieur et sécuriser votre connexion Internet. Ceci est particulièrement important lorsque les réseaux Wi-Fi sont largement répandus pour faciliter la connectivité. Gardez à l'esprit qu'Internet est la passerelle la plus populaire pour les pirates. Par conséquent, utilisez des protocoles de sécurité fiables tels que les clés WPA ou WPA2. Aussi, si vos employés connectent leurs téléphones en utilisant la connexion Wi-Fi de l'entreprise, vérifiez si l'appareil en question a un niveau de sécurité adéquat. **[10]**

- ✓ **Mettre à jour son réseau informatique**

Certaines menaces peuvent être évitées simplement en mettant à jour votre système ou votre logiciel. En fait, tous les virus, logiciels malveillants, pirates, etc. aiment exploiter les failles des applications obsolètes pour compromettre l'intégrité du réseau. Pour contourner ce problème, installez un pare-feu sur tous les postes de travail, y compris Nomades. Ajoutez un programme antivirus puissant et installez régulièrement les mises à jour nécessaires pour garantir l'efficacité de vos outils et logiciels. **[9]**

- ✓ **Effectuer des sauvegardes de données**

Vous souhaitez peut-être renforcer la sécurité informatique de votre entreprise pour éviter la perte de données. Il n'y a rien de mieux qu'une sauvegarde pour cela. En cas de sinistre ou d'attaque, vous devez récupérer vos données. Vous pouvez configurer des processus de sauvegarde automatisés et des systèmes de récupération pour atténuer les effets du vol ou de la perte de données. Fournissez des disques durs externes pour les fichiers importants de vos employés et configurez un serveur de sauvegarde pour prendre le relais en cas de panne. Si vous utilisez le cloud computing en interne, assurez-vous que votre fournisseur de services protège adéquatement vos données. **[10]**

- ✓ **Crypter ses informations et ses données**

Une autre façon d'améliorer la sécurité de votre ordinateur consiste à crypter vos données. La technologie de cryptage asymétrique rend illisibles les données que vous transmettez à des tiers. Le déchiffrement est ensuite effectué à l'aide de clés dont seuls les utilisateurs ayant accès disposent. Par conséquent, si un pirate intercepte ces données, il sera impossible de les décrypter et de les utiliser. Combiné avec un mot de passe complexe, les informations peuvent être transmises en toute sécurité. **[11]**

- ✓ **Sécuriser les messageries professionnelles**

Connaissez-vous le phishing ? Il s'agit d'une technique de piratage qui "hameçonne" les utilisateurs par e-mail pour qu'ils cliquent sur des liens ou des pièces jointes contenant du contenu piraté. Pour éviter cela, nous vous recommandons d'utiliser d'abord un filtre anti-spam. Ces outils et la formation du personnel à la reconnaissance des e-mails malveillants et potentiellement dangereux peuvent grandement améliorer la sécurité informatique. **[11]**

- ✓ **Anticiper les incidents pour réduire leurs impacts**

La question aujourd'hui n'est plus de savoir si nous serons attaqués, mais quand : Améliorer la

Sécurité de l'information d'une entreprise ne consiste pas seulement à faire attention Il est également important d'anticiper les incidents potentiels et de se protéger des cyberattaques. Certes, le risque n'est pas nul, mais on s'attend à ce que de nombreuses atteintes à la sécurité humaine ou physique se produisent. La cybersécurité nécessite des mesures proactives, telles que la création d'un plan de reprise après sinistre (DRP) pour minimiser les dommages économiques ou opérationnels d'une attaque. **[9]**

- ✓ **Améliorer le contrôle d'accès d'un système**

Améliorer le contrôle d'accès au système d'information est l'un des bons moyens d'améliorer la sécurité de l'information. L'accès au système d'information nécessite une identification et Pré-authentification. L'utilisation de comptes joints ou anonymes est interdite. Affilier Des mécanismes pour limiter les services, les données et les privilèges auxquels vous accédez L'utilisateur doit être mis en œuvre conformément à son rôle dans l'organisation.

I.3. Contrôle d’accès :

I.3.1. Définition de contrôle d’accès :

Le contrôle d'accès est une mesure de sécurité qui empêche les individus au sein d'une organisation d'accéder aux données et aux ressources. C'est un aspect essentiel de tout plan de sécurité. Le contrôle d'accès authentifie et autorise des employés spécifiques à sécuriser le système. **[12]**

I.3.2. Les systèmes de contrôle d'accès :

Un système de contrôle d'accès est un dispositif qui permet l'authentification et l'enregistrement des personnes et des véhicules entrant dans une installation. Grâce aux progrès

de la technologie, nous disposons maintenant de plusieurs types de contrôles d'accès et de présence qui contribuent à améliorer la sécurité informatique. **[13]**

I.3.3. Type de contrôle d'accès :

- ✓ **Contrôle d'accès physique**

Le contrôle d'accès physique est la restriction de l'accès aux espaces physiques au sein d'une entreprise ou d'une organisation. Ce type de contrôle d'accès restreint l'accès aux salles, aux bâtiments et aux ressources informatiques physiques. De plus, des contrôles d'accès physiques surveillent qui entre et sort des zones réglementées. Cela protège vos actifs.

Des exemples d'accès physiquement contrôlés sont les portes protégées par un mot de passe et les portes contrôlées par des télécommandes ou des cartes électroniques (exemples étudiés dans notre projet).

- ✓ **Contrôle d'accès logique**

Le contrôle d'accès logique comprend l'authentification et l'autorisation des utilisateurs. Ceci est différent du contrôle d'accès physique. Les clés et les badges sont utilisés pour le contrôle d'accès physique. Le contrôle d'accès logique utilise des programmes de mots de passe avancés et des fonctions de sécurité biométrique avancées. **[11]**

I.3.4. Les modèles de contrôle d'accès :

I.3.4.1. DAC (Discretionary Access Control) :

Le contrôle d'accès discrétionnaire (**DAC**) est un type de contrôle d'accès de sécurité qui accorde ou restreint l'accès aux objets via des politiques d'accès définies par les propriétaires d'objets et les groupes de sujets. Le contrôle du mécanisme **DAC** est défini en identifiant l'utilisateur à l'aide des informations d'identification fournies lors de l'authentification, telles que le nom d'utilisateur et le mot de passe. La **DAC** est facultative dans la mesure où un sujet (propriétaire) peut déléguer l'accès à des objets ou des informations authentifiés à d'autres utilisateurs. Autrement dit, les droits d'accès aux objets sont déterminés par le propriétaire. C'est le modèle que nous utilisons dans notre travail.

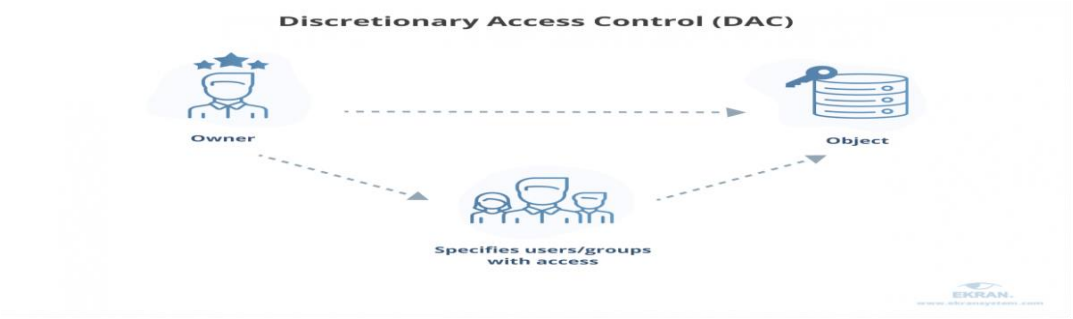


Figure. I. 1:Schéma montrant un modèle DAC (Discretionary Access control).[14]

I.3.4.2. MAC (Mandatory Access Control):

Le contrôle d'accès obligatoire (**MAC**) est un modèle de contrôle d'accès dans lequel le système d'exploitation accorde l'accès aux utilisateurs en fonction de la confidentialité et du niveau de privilège de l'utilisateur. Dans ce modèle, l'accès est accordé sur la base du besoin d'en connaître. Les utilisateurs doivent prouver qu'ils veulent les informations avant que l'accès ne soit accordé.

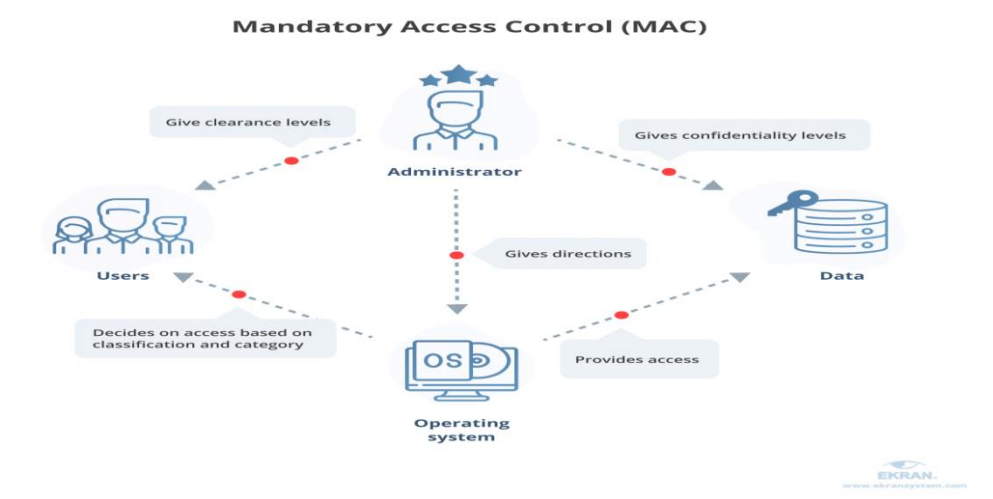


Figure. I. 2: Schéma montrant un modèle MAC (Mandatory access control).[15]

I.3.4.3. RBAC (Role-Based Access Control):

Le contrôle d'accès basé sur les rôles (**RBAC**) est un mécanisme de contrôle d'accès qui définit les rôles et les privilèges de chaque utilisateur. Les rôles sont définis en fonction de caractéristiques telles que l'emplacement, le service, l'ancienneté et les responsabilités de l'utilisateur. Les autorisations sont attribuées en fonction de l'accès (ce que l'utilisateur peut voir), de l'action (ce que l'utilisateur peut faire) et de la session (combien de temps l'utilisateur peut faire).

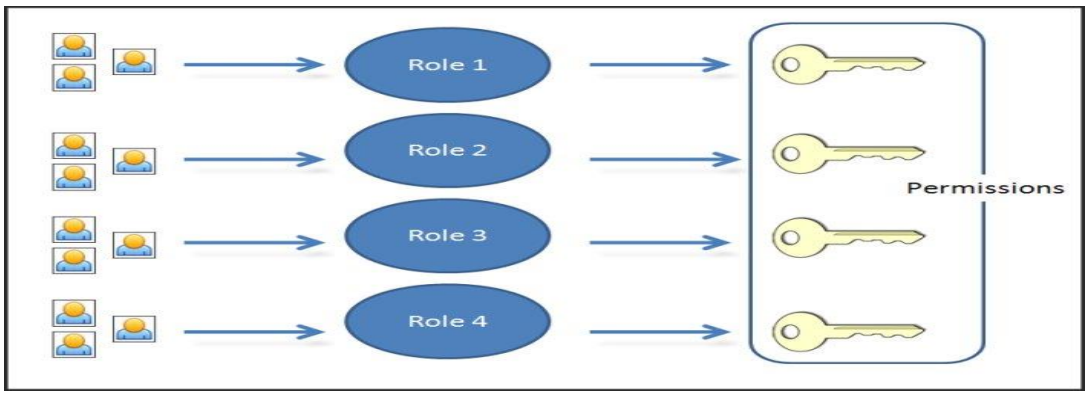


Figure. I. 3: Schéma montrant un modèle RBAC (Role-Based Access Control).[16]

I.3.4.4. Modèle de contrôle d'accès à basé d'équipe (TMAC) :

Le système de contrôle d'accès **TMAC** est basé sur les relations entre plusieurs employés travaillant sur la même tâche. La réussite des missions dépend donc d'une bonne gestion des droits d'accès.

I.3.4.5. ORBAC (Organization Based Access Control):

Le modèle **ORBAC** considère les organisations comme l'entité principale du modèle, car il permet des politiques entièrement configurables et la possibilité de gérer simultanément plusieurs politiques de sécurité associées à différentes organisations. Les politiques de sécurité ne s'appliquent pas directement aux sujets, actions ou objets. **[17]**

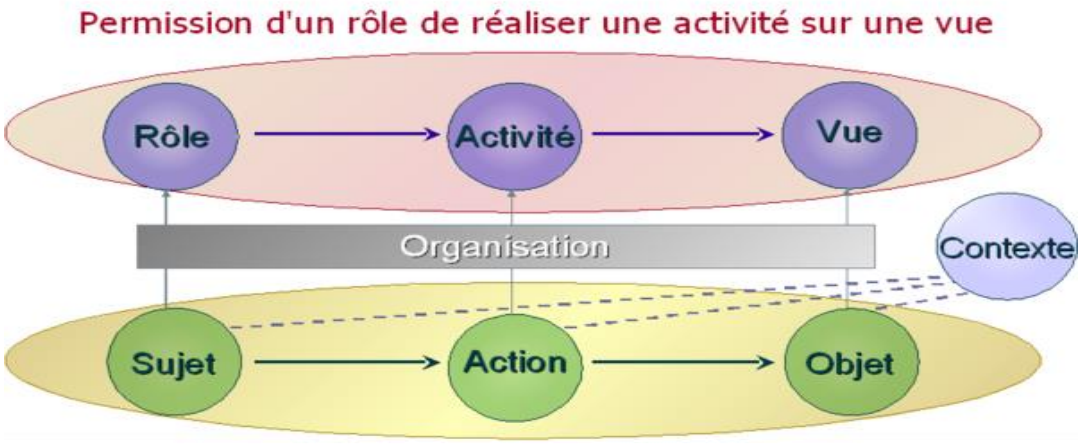


Figure. I. 4: Schéma montrant un modèle ORBAC (Organization Based Access Control).[18]

I.4. Conclusion :

La protection des données personnelles et de la vie privée est un enjeu important pour les entreprises et les agences gouvernementales qui collectent et stockent aujourd'hui des données personnelles. La mise en place d'une politique de sécurité est obligatoire. Plusieurs modèles de contrôle d'accès ont été proposés dans la littérature pour permettre aux utilisateurs d'appliquer des politiques de sécurité. Le système de contrôle d'accès installé est souvent un véritable obstacle et rend le travail des utilisateurs inefficace. Avant d'implémenter des modèles de contrôle d'accès, vous devez en savoir plus sur les modèles de contrôle d'accès.

Dans ce chapitre, nous avons présenté des généralités sur la sécurité informatique, ses Objectifs, puis Les différents types de sécurité informatique, ainsi que quelques attaques et les étapes pour gérer ses attaques. Ensuite nous avons mentionné les différentes approches pour améliorer la sécurité, et puis nous avons parlé de contrôle d’accès, on a présenté quelques modèles de contrôle d’accès de base.

CHAPITRE II

LE CONTROLE D'ACCES REALISES A BASE DE LA TECHNOLOGIE RFID

II.1. Introduction :

Dans ce chapitre, nous traitons des différentes questions relatives au système de contrôle d'accès plus particulièrement la technologie **RFID** (Radio Frequency Identification), nous donnons aussi une succincte définition, son principe de fonctionnement, ainsi que l'analyse et la conception des besoins et des exigences des utilisateurs qui permet de traduire les besoins fonctionnels et de la spécification des exigences dans un langage plus professionnel et compréhensible (**UML**).

II.2. Définition de la technologie RFID :

RFID « Radio-Frequency Identification » est une technologie pour laquelle les données numériques codées dans des étiquettes RFID ou « tags ». Elles sont capturées par un lecteur via des ondes radio. La RFID est similaire aux codes-barres dans la mesure où les données d'une étiquette sont capturées par un appareil qui stocke les données dans une base de données.

II.3. Composants des systèmes RFID :

La **RFID** appartient à un groupe de technologies appelées Automatic Identification and Data Capture (**AIDC**). Les méthodes **AIDC** identifient automatiquement les objets, collectent des données les saisissent directement dans des systèmes informatiques avec une intervention humaine minime. Les méthodes **RFID** utilisent des ondes radio pour y parvenir. À un niveau simple, les systèmes **RFID** se composent de trois composants :

1. **Une étiquette RFID « RFID tag »** : C'est un dispositif récepteur, que l'on place sur des éléments (objet, animal…). Ils sont munis d'une puce contenant les informations et d'une antenne pour permettre les échanges d'informations.

La figure ci-dessous, montre une étiquette à radiofréquence qui se compose d'une puce et d'une antenne. **[19]**

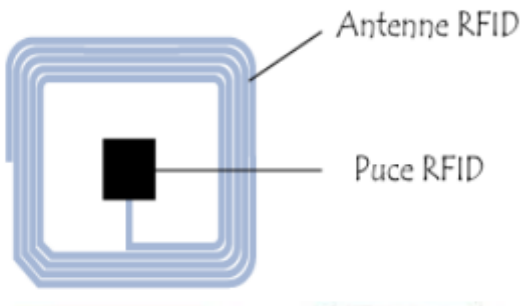


Figure. II. 1: Etiquettes (tag) à radiofréquence.[20]

Figure. II. 2: Etiquettes (tag) à radiofréquence.[21]

- **Modèles des étiquettes RFID :**

  Porte clé :

  Le porte-clés RFID est un produit simple et pratique qui s'adapte à toutes les situations. Cette clé RFID permet un contrôle d'accès fiable et sécuritaire à l'entrée des immeubles, des parkings ou de portes sécurisées grâce au tag RFID.

Figure. II. 3: Le porte-clés RFID (Key Tag).[22]

Badge RFID :

Le badge RFID devient incontournable pour faciliter et sécuriser l'accès aux bâtiments des entreprises. Ces badges RFID sont munis d'une antenne et d'une puce aussi, pour permettre la transmission de données avec un lecteur. Il est réalisé à partir d'un PVC ultra blanc offrant une résistance parfaite lors de manipulations répétées. Le badge RFID est au format : 84 x 56 x 0.76 mm.

Figure. II. 4: Badge RFID.[23]

Un lecteur RFID : Le lecteur/enregistreur est constitué d'un circuit qui émet une énergie électromagnétique à travers une antenne, et d'une électronique qui reçoit et décode les informations envoyées par l'étiquette et les envoie au dispositif de collecte des données. Le lecteur RFID est l'élément responsable de la lecture des étiquettes radiofréquence et de la transmission des informations qu'elles contiennent.

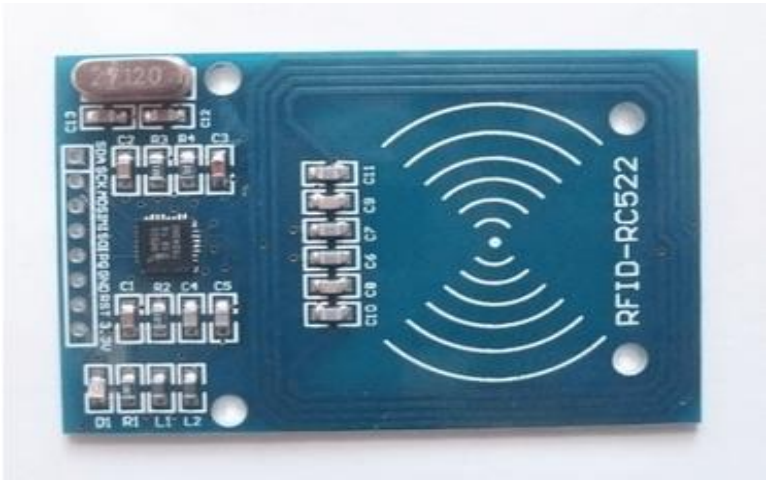


Figure. II. 5: Le lecteur RFID.[24]

II.4. Principe de fonctionnement d'un système RFID :

Les étiquettes RFID contiennent un circuit intégré et une antenne, qui permettent de transmettre des données au lecteur RFID. Le lecteur convertit ensuite les ondes radio en une forme de données plus utilisable. Les informations collectées à partir des étiquettes sont ensuite transférées via une interface de communication vers un système informatique hôte pour les traitements ultérieurs.

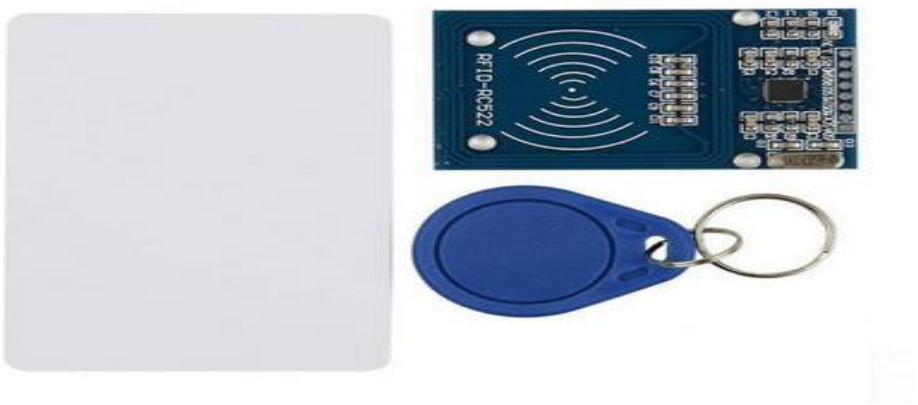


Figure. II. 6: Un module RFID est accompagné de deux badges de formes différentes l'un se forme d'une carte et l'autre d'une clé.[25]

II.5. Applications et domaines des badges RFID :

Les badges **RFID** servent dans de multiples domaines Les cartes à puce sont utilisées dans les systèmes de paiement comme les cartes bancaires, mais aussi sous forme de carte **SIM** en téléphonie. On dénombre beaucoup de possibilités d'utilisation des cartes à puce dans le contrôle d'accès afin d'identifier les individus que ce soit pour entrer dans un bâtiment, une pièce ou pour se connecter à un ordinateur via un contrôle d'accès logique.

Au quotidien nous utilisons énormément de cartes à puce sans y faire attention. Notre téléphone fonctionne avec une carte **SIM**, les puces sont partout et nous accompagnent au quotidien :

- Monétique / paiement
- Téléphonie
- Identification
- Santé
- Sécurité
- Transport
- Authentification
- Logistique
- Traçabilité

Ils peuvent notamment servir dans les payés développées en :

- Contrôle d'accès : porte-clés d'accès.
- Abonnement : carte de membre.
- Titre de transport : carte de bus et tramway.
- Fidélité : carte de fidélité.

- Restaurants administratifs : carte de self.
- Carte d'identité.
- Passeport.
- Suivi de stocks : tag **RFID.**
- Serrure électronique.
- Piscine / **SPA** : bracelets d'accès / bracelet de casier.
- Salle de sport : bracelet **RFID**.
- Club de forme.
- Bibliothèque : carte de bibliothèque, carte de médiathèque.

II.6. Présentation de la carte Arduino :

Est une petite carte électronique **(5,33 × 6,85 cm)** équipée d'un microcontrôleur, ce dernier permet, à partir des d'événements détectés par des capteurs, de programmer et de commander des actionneurs ; la carte Arduino est donc une interface programmable.

Elle est couplée avec le lecteur **RFID**. Elle permet de détecter la présence du badge, reconnaitre son identifiant (code du badge). Elle sert également à activer l'ouverture de la porte ou l'alarme. **[26]**

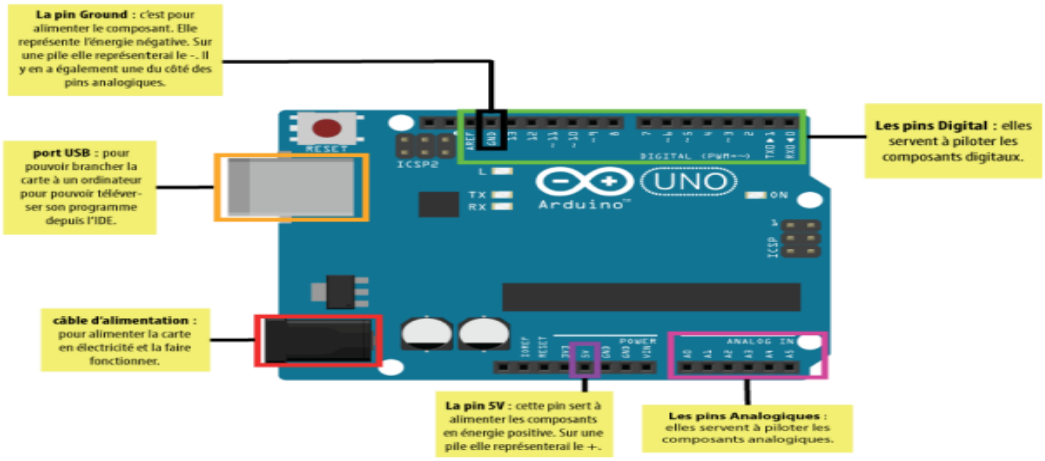


Figure. II. 7: Anatomie d'une carte Arduino UNO.[27]

II.7. Montage de la carte Arduino avec le lecteur RFID :

Nous allons donc raccorder comme ceci : **Arduino →RC-522**

- 3.3v sur 3.3v.
- GND sur gnd.
- SDA sur D10.
- SCK sur D13.

- MOSI sur D11.
- MISO sur D12.
- RST sur D9.

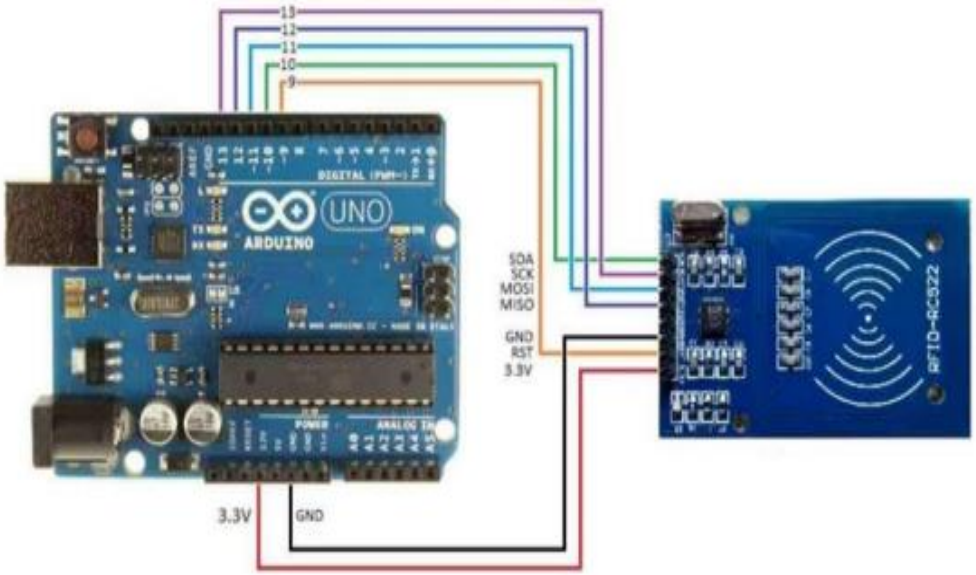


Figure. II. 8: Montage carte Arduino+Lecteur RFID.[28]

II.8. Câblage d'une LED verte et rouge avec la carte Arduino :

LED verte :

Voyant indiquant l'ouverture de la porte. La LED s'allume pendant une seconde lorsqu'un badge reconnu est détecté. Elle reste éteinte dans le cas contraire.

LED rouge :

Voyant indiquant la détection d'un faux badge (identifiant non reconnu du badge).

La LED rouge s'allume pendant une seconde puis s'éteint pour chaque fausse détection.

Lorsque le nombre de tentatives est atteint, la LED rouge clignote en boucle infinie en état d'alarme.

Aucune moyenne n'est possible pour réactiver le système à part la réinitialisation de la carte Arduino.

Le montage de base d'une LED est ressemblé à ça :

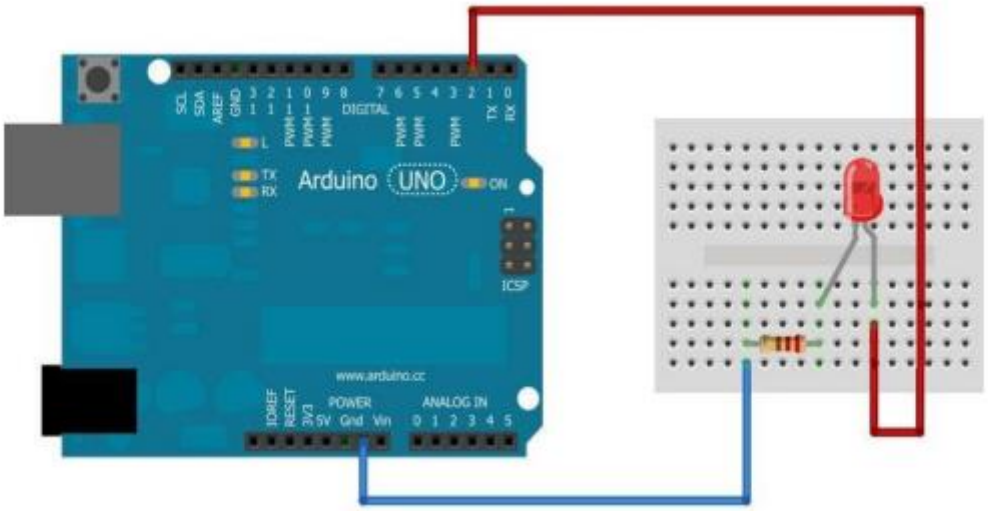


Figure. II. 9: Montage carte Arduino+LED.[29]

II.9. Unité de sortie et de communication (Afficheur LCD) :

Les afficheurs à cristaux liquides, autrement appelés afficheurs **LCD** (Liquid Crystal Display), sont des modules compacts intelligents et nécessitent peu de composants externes pour un bon fonctionnement. Ils consomment relativement peu **(de 1 à 5 mA),** ils sont relativement bons marchés et s'utilisent avec beaucoup de facilité. **[30]**

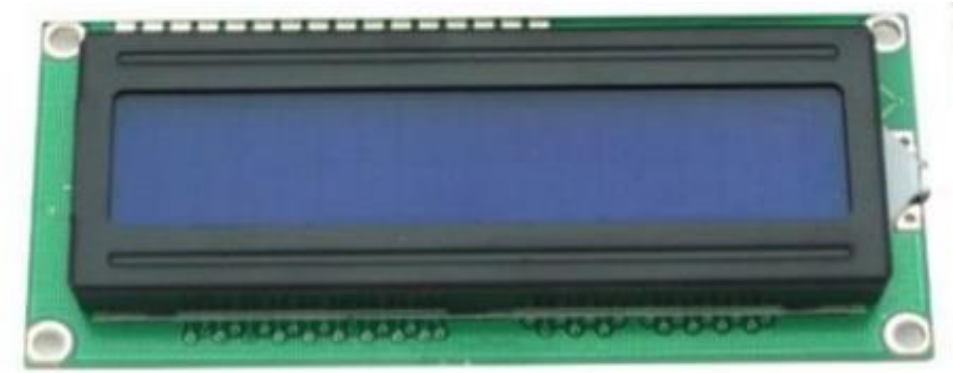


Figure. II. 10: Afficheur LCD.[31]

L'afficheur **LCD** utilisé est un écran permettant l'affichage de **16×2** caractères, c'est-à dire deux lignes de **16** caractères.

Le montage que nous allons réaliser va connecter l'afficheur **LCD** à l'Arduino, et ajouter un potentiomètre pour ajuster le contraste. Le transfert des données sous forme de bits est pris en compte par la bibliothèque 'LiquidCrystal'.

Arduino ⟶ **LCD**

- La broche VSS est reliée à la masse (GND).
- La broche VDD est reliée à l'alimentation 5 V.
- RS est reliée au port digital 12.
- RW est reliée à la masse, une façon de lui donner une valeur basse pour passer en mode écriture.
- E est relié au port digital 11.
- V0 est reliée à la broche de données du potentiomètre (au centre).
- La broche à gauche derrière la broche seule sur sa rangée (3) du potentiomètre est reliée à 5 V.
- La broche à droite à la masse.
- Les broches D4 à D7 du LCD sont reliées aux ports digitaux 4 à 7 de l'Arduino.

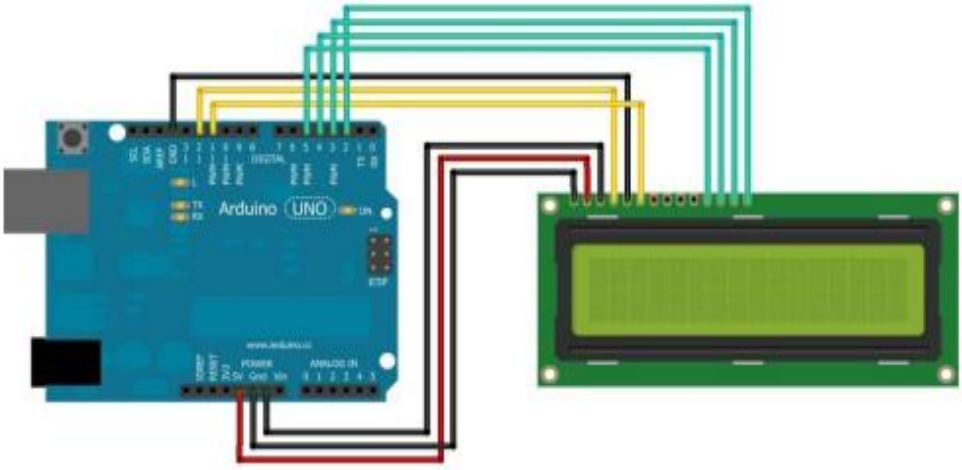


Figure. II. 11: Montage carte Arduino + afficheur LCD.[32]

II.10. L'organigramme de fonctionnement :

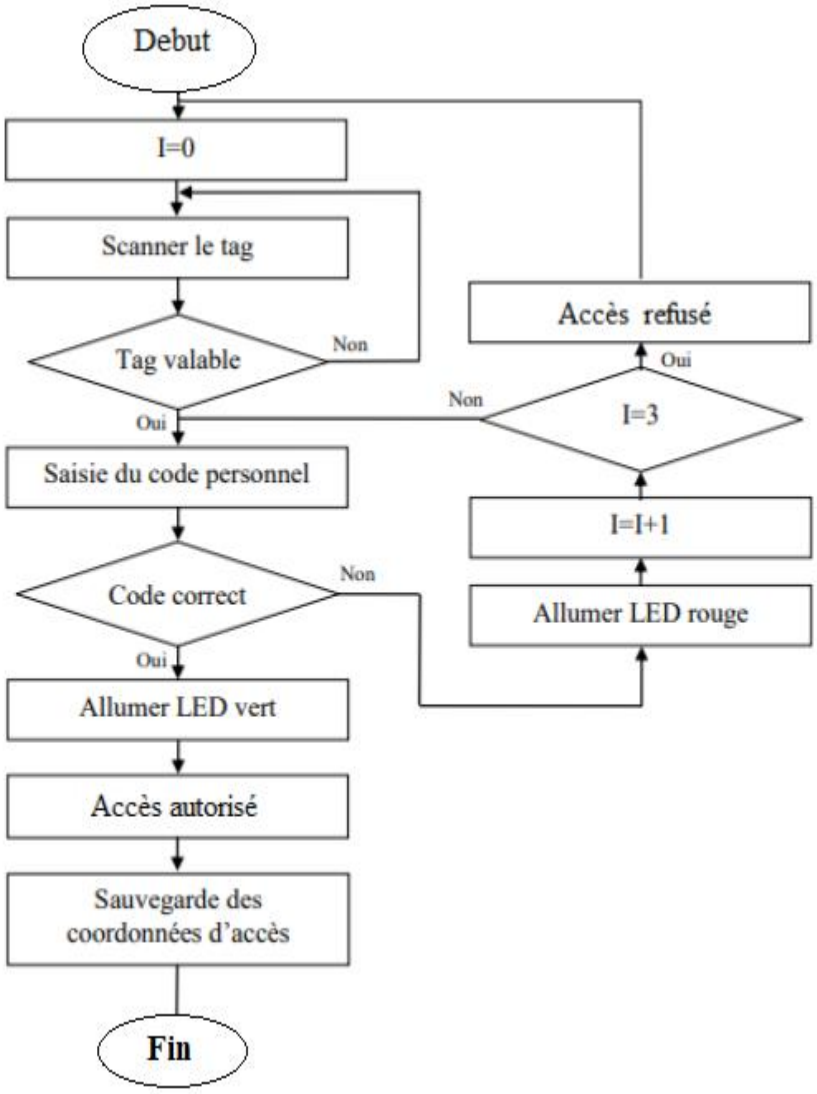


Figure. II. 12: L'organigramme de fonctionnement.

II.11. Analyse des besoins des utilisateurs :

Ce système consiste l'ouverture d'une porte d'une entreprise ou bien autres sites qui nécessitent un haut niveau de sécurité en utilisant un badge. Le lecteur RFID couplé à la carte Arduino permet de détecter un badge enregistré ou non. Lorsque l'utilisateur est reconnu, le système déclenche l'ouverture de la porte ou une alarme dans le cas échéant. L'utilisateur à droit de trois tentatives. Le nombre de tentatives est ajustable par le programme Arduino**.**

II.11.1. Modélisation en UML :

II.11.1.1. Diagramme de cas d'utilisation :

Un diagramme de cas d'utilisation capture le comportement d'un système, d'un sous-système, d'une classe ou d'un composant tel qu'un utilisateur extérieur le voit. Il scinde la fonctionnalité du système en unités cohérentes, les cas d'utilisation, ayant un sens pour les acteurs. Les cas d'utilisation permettent d'exprimer le besoin des utilisateurs d'un système, ils sont donc une vision orientée utilisateur de ce besoin au contraire d'une vision informatique**. [33]**

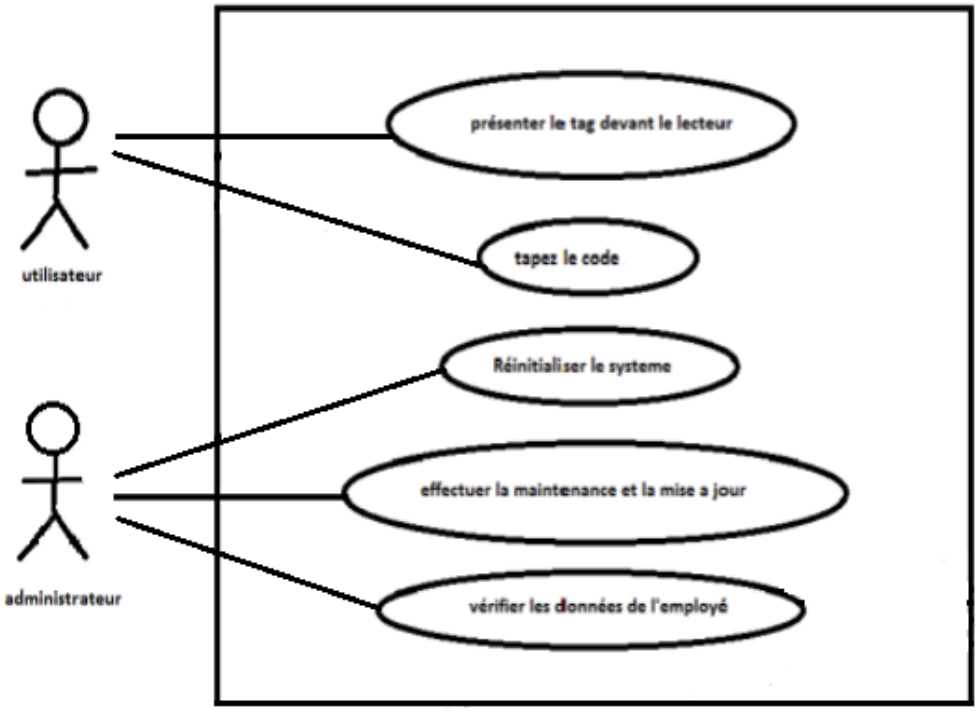


Figure. II. 13: Diagramme des cas d'utilisation du système contrôle d'accès.

Description textuelle

- **Le cas « présenter le badge devant le lecteur » :**

Nom : présenter le badge devant le lecteur.

Objectif : la reconnaissance du badge par le système et le déclenchement du cas d'utilisation « taper code PIN ».

Acteurs principaux : l'employé, administrateur.

Acteurs secondaires : le système.

Pré conditions :

- Le système doit être fonctionnel.
- Le message « scannez carte» affiché sur l'écran.
- L'employé possède un badge RFID.

Scénario nominal :

- Employé présente le tag devant le lecteur.
- Système affiche « accès permis ».

Scénario alternatif :

- Badge non valide.
- Système affiche «ID non accepté accès refusé ».

Post-conditions : le système demande de l'employé de valider son entrée par un Mot de passe.

- **Le cas « tapez le Mot de passe » :**

Nom : taper mot de passe.

Objectif : confirmer le badge scanné et le système déverrouille la porte.

Acteurs principaux : l'employé, le système.

Acteurs secondaires : administrateur.

Pré condition :

- Présentation d'un badge valide
- Le message « Mot de passe » affiché sur l'écran.
- Taper le mot de passe.

Scénario nominal :

- L'employé tape son mot de passe.
- Système affiche « BIENVENUS Université O.E.B » et déverrouille la porte.

Scénario alternatif :

- Code PIN erroné.
- Système fournie trois fois d'essais, si on dépasse trois essais le système réinitialise.

Post conditions : le système déverrouille la porte et l'employé pourrait entrer.

II.11.1.2. Diagramme d'activités :

Un diagramme d'activité permet de modéliser le comportement du système, dont la séquence des actions et leurs conditions d'exécution.

Les actions sont les unités de base du comportement du système. Un diagramme d'activités permet de grouper et de dissocier des actions. Si une action peut être divisée en plusieurs actions en séquence, vous pouvez créer une activité les représentant. **[34]**

- **Diagramme général du système :**

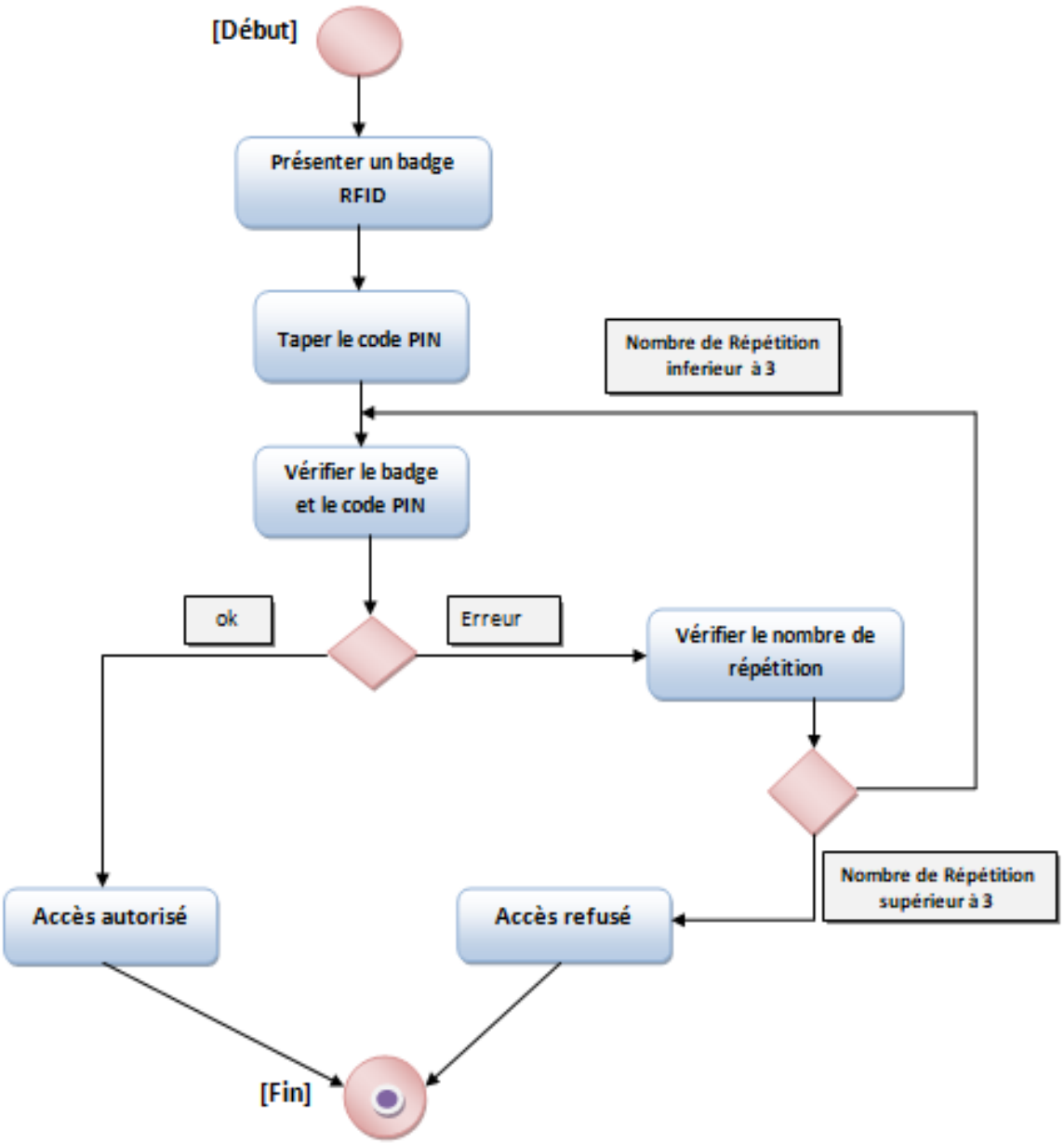


Figure. II. 14: Diagramme d'activité du système contrôle d'accès.

➢ **Diagramme d'authentification :**

L'utilisateur choisit une porte et passe son badge (Carte RFID). Une interrogation de la base de données s'effectue pour s'assurer que le badge existe dans le système.

Un code d'accès est demandé si l'accès à la porte le nécessite. Le code est vérifié, puis le badge est bloqué si le code d'accès est faux trois consécutives. La porte n'étant pas ouverte, la tentative d'accès est tout de même insérée dans l'historique.

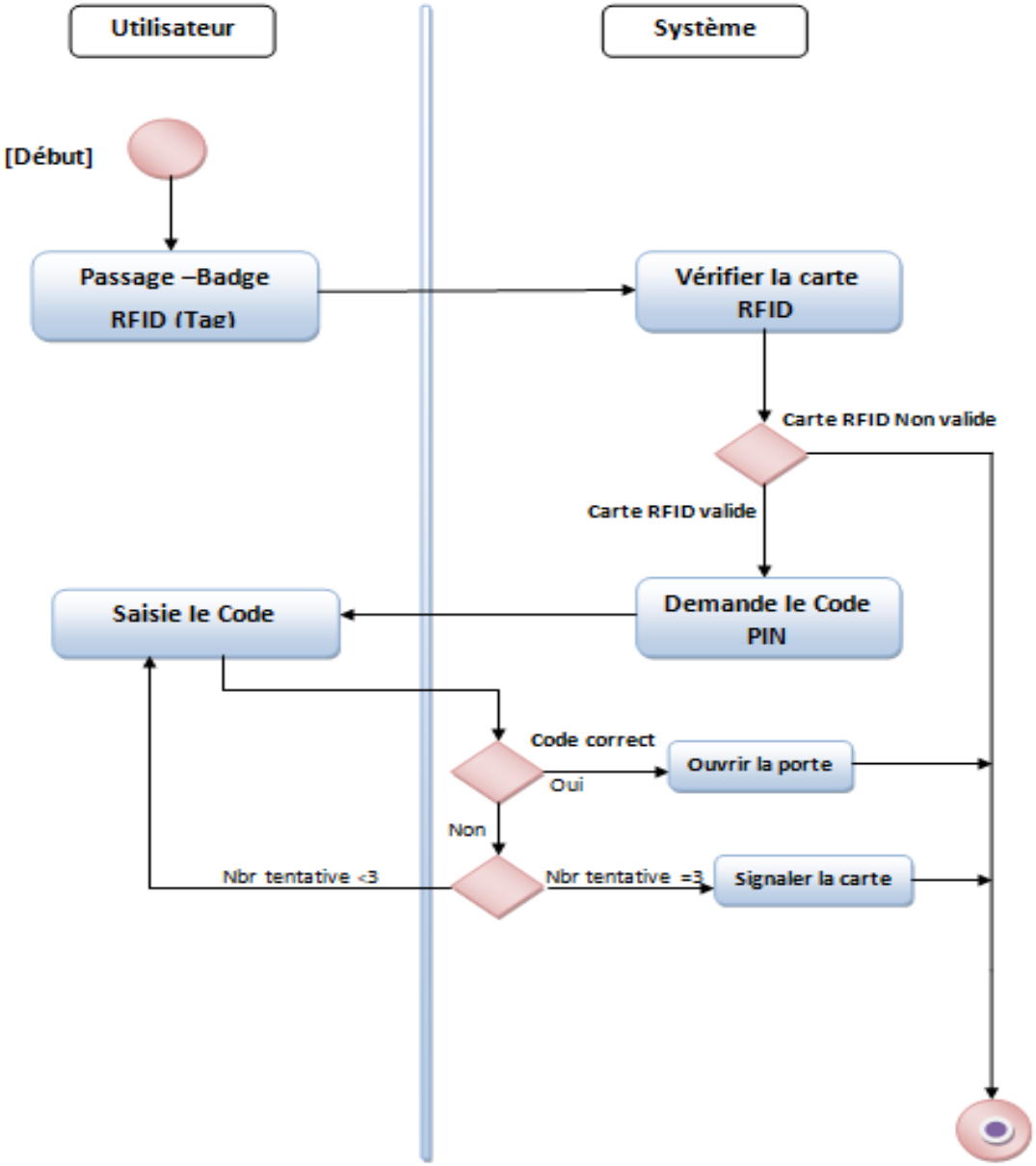


Figure. II. 15: Diagramme d'authentification.

➢ **Diagramme gestion des Cartes RFID (Badges) :**

Ce diagramme représente la gestion des cartes RFID (Badges) par l'administrateur du système et selon les besoins des acteurs :

- L'utilisateur demande à accepter l'ajout au système, et celui-ci est étudié par l'administrateur, soit par acceptation et on lui remet un badge d'entrée utilisable avec le mot de passe, soit par refus.
- L'utilisateur signale un badge manquant qui sera bloqué (supprimé) par l'administrateur et rendu inutilisable par des personnes non autorisées.

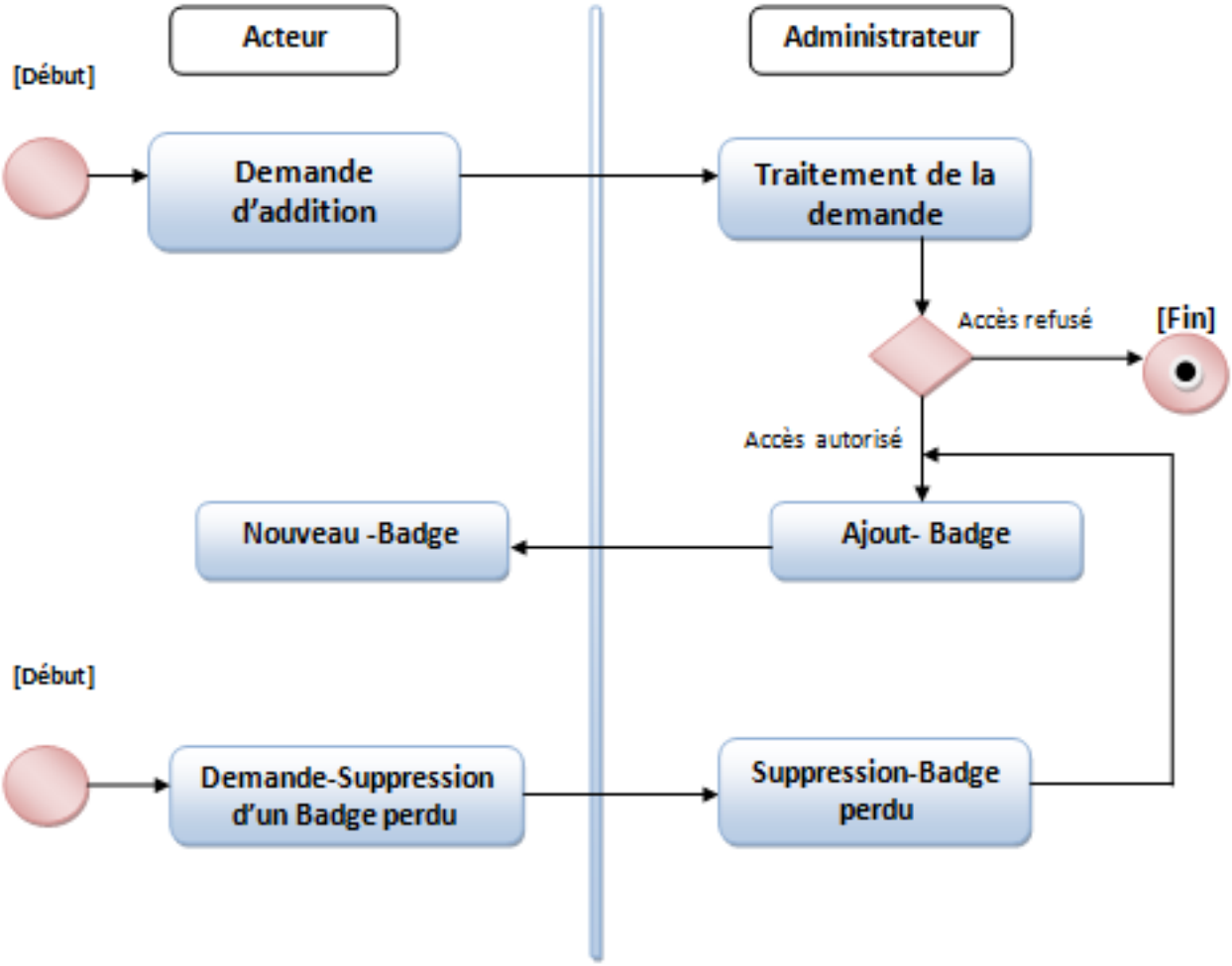


Figure. II. 16: Diagramme gestion des Cartes RFID (Badges).

II.11.1.3. Diagramme de séquence :

Le diagramme de séquence est la représentation graphique des interactions entre les acteurs et le système selon un ordre chronologique dans la formulation Unified Modeling Language.

Il représente la collaboration d'objets et est utilisé pour définir des séquences d'événements entre les objets pour un certain résultat. Donc c'est un composant essentiel utilisé dans les processus liés à l'analyse, la conception et la documentation. **[34]**

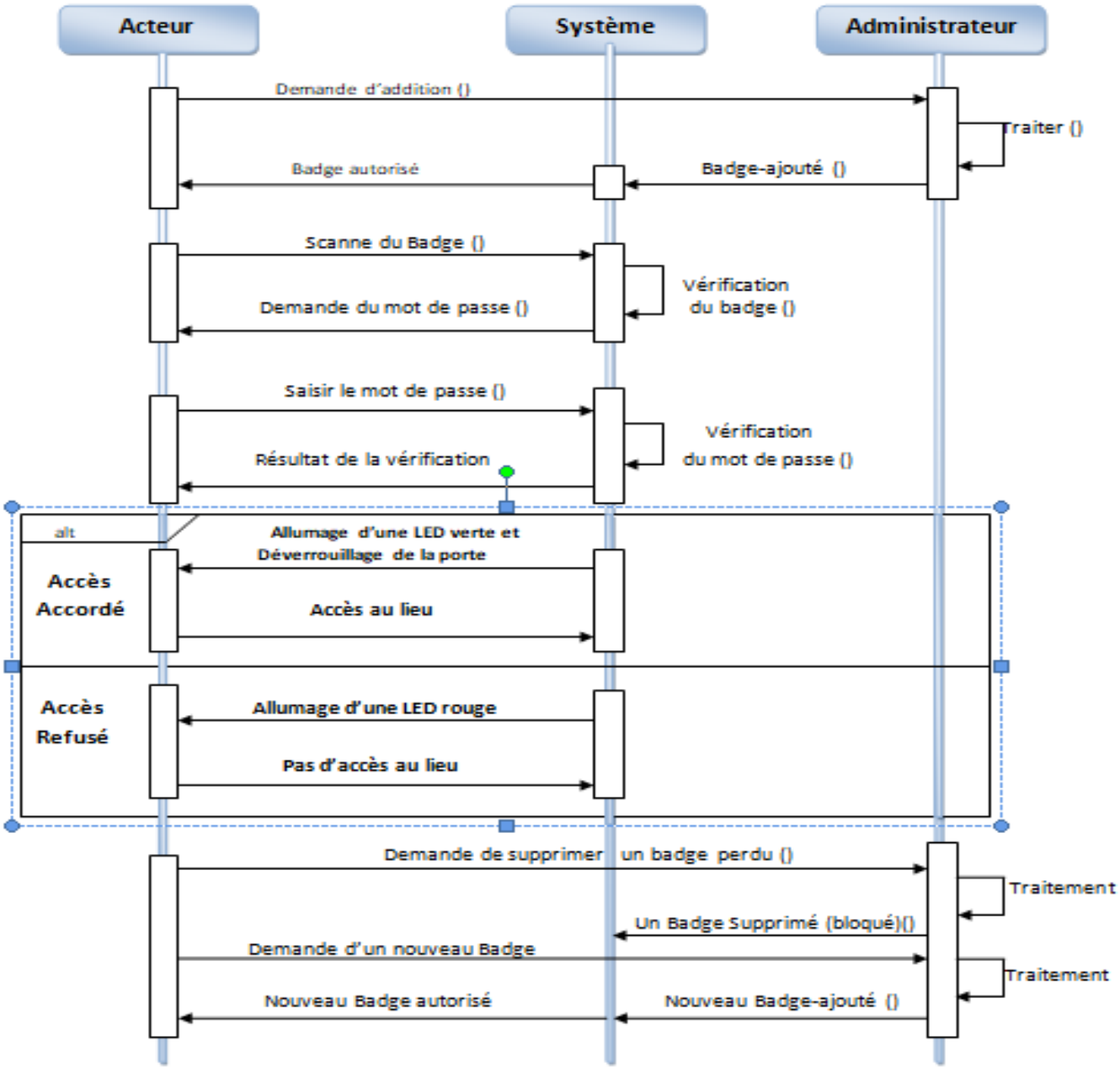


Figure. II. 17: Diagramme de séquence du système contrôle d'accès.

II.11.1.4. Diagramme de classe :

Il représente les classes intervenant dans le système. Le diagramme de classe est une représentation statique des éléments qui composent un système et de leurs relations. Chaque application qui va mettre en œuvre le système sera une instance des différentes classes qui le compose. A ce titre il faudra bien garder à l'esprit qu'une classe est un modèle et l'objet sa réalisation.

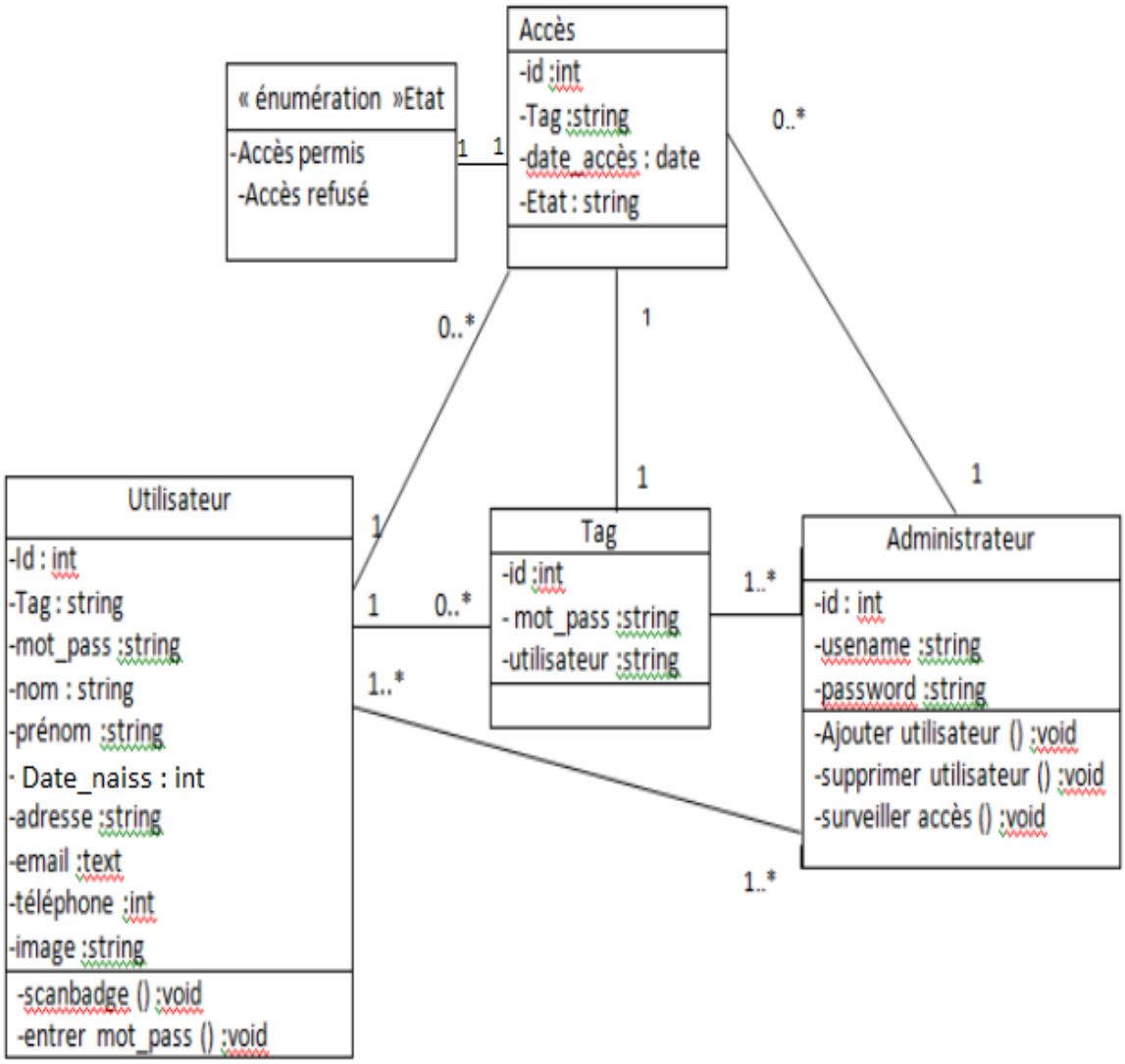


Figure. II. 18: Diagramme de classe du système contrôle d'accès.

II.12. Conclusion :

Dans le présent chapitre nous avons présenté la partie théorique des différents modules constituant notre carte électronique pour un système de contrôle d'accès. La première partie du présent chapitre a été consacré pour la présentation des caractéristiques techniques et le schéma simplifie de la carte RFID- Arduino. La deuxième partie de ce chapitre, présente la modélisation de cette technologie en UML pour mieux comprendre le principe de fonctionnement de cette technique dans le contexte d'améliorer la sécurité de ce système intelligent.

CHAPITRE III
IMPLEMENTATION

III.1. Introduction :

Dans le cycle de vie d'un logiciel, l'implémentation c'est la phase la plus importante après celle de la conception. Cette phase consiste à transformer le modèle conceptuelle vue précédemment en des composants logiciels formant notre système. Dans le présent chapitre nous présentons le système que nous avons conçu, ainsi que les outils et langages de programmation utilisés. Les principales interfaces du système sont montrées par des captures d'écran.

III.2. Outils de développement :

III.2.1. Outils matériels :

Dans cette partie, nous présentons l'ensemble des composants nécessaire pour notre projet :

- Unité de commande et de traitement : Arduino uno.
- Unité de sortie et de communication : Afficheur **LCD 16×2.**
- Unité d'entrée : un clavier électronique et le module **RFID**.

Le rôle de chacun de ces composants est :

- **Arduino :**

La carte Arduino se compose de plusieurs composants électroniques qui ont été mentionnés précédemment dans le deuxième chapitre, et le plus important de ces composants est un microcontrôleur pour stocker et exécuter le programme informatique, donc Le rôle de la carte Arduino est de stocker un programme et de le faire fonctionner.

Le modèle Arduino que nous avons choisi pour notre projet est **l'Arduino uno**, et cela en raison de ses caractéristiques techniques qui sont suffisantes pour bien commencer à programmer (**14 entrées/sorties numériques, 6 entrées analogiques, une mémoire flash de 32 KB, un de SRAM 2 KB, un EPPROM de 1 KB** …)

Il existe de nombreux modèles de cartes Arduino, mais le modèle **Arduino uno** est le plus répandu et nous permet faire un large éventail de possibilités.

- **Afficheur LCD 16×2 :** Son rôle est de transmettre les informations utiles d'un système à un utilisateur.

- **Clavier matriciel**

Nous savons que le problème de notre étude est de savoir comment améliorer la sécurité des informations du système **RFID**, en plus d'utiliser des cartes biométriques pour se connecter, nous définissons un mot de passe pour chaque utilisateur, ainsi qu'un mot de passe pour les administrateurs, et c'est en afin de rendre le système **RFID** plus sécurisé. Le mot de passe est saisi au niveau d'un clavier électronique appelé Clavier matriciel.

Le clavier numérique est plus aisé et plus pratique à utiliser, il présente la communication Homme-Machine

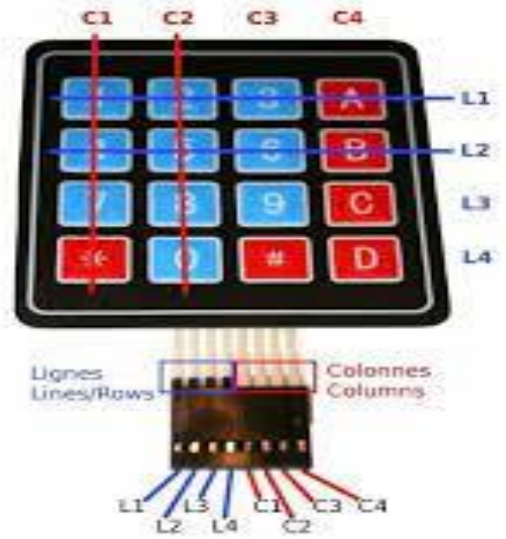


Figure. III. 1: Clavier matriciel.[35]

Ils existent plusieurs claviers selon le nombre de boutons qu'ils contiennent, ils peuvent se configurer en **3×3, 3×4, 4×4**…etc. Le clavier que nous avons utilisé est **4×4.**

Principe de fonctionnement :

Clavier numérique est un ensemble de 16 boutons qui montés sous forme de matrice, c'est à dire que tous les boutons d'une colonne sont reliés une entrée et tous les boutons d'une même ligne sont reliés à une autre. Lorsqu'on appuie sur un bouton l'entrée correspondant à la ligne est reliée à l'entrée correspondant à la colonne ce qui ferme le circuit. L'avantage de ce type de montage est que l'on peut gérer 16 boutons avec seulement 8 entrées du microcontrôleur. **[36]**

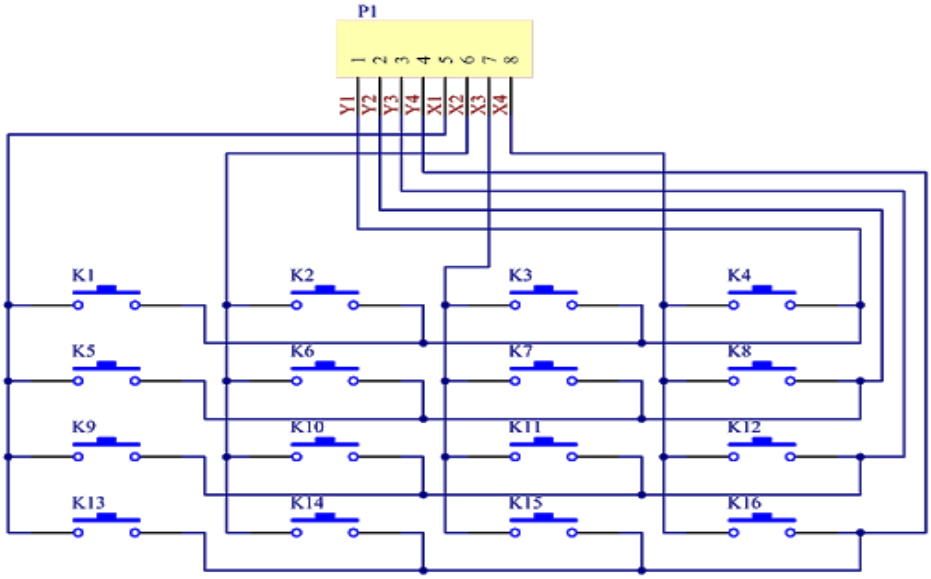


Figure. III. 2: keypad-4x4-principle.[37]

Schéma de branchement

Le clavier numérique utilise 8 broches de l'Arduino. Il est possible de les brancher sur n'importe quelle broche. Les broches 0 et 1, utilisées pour la connexion série via le port USB, sont à éviter**.[36]**

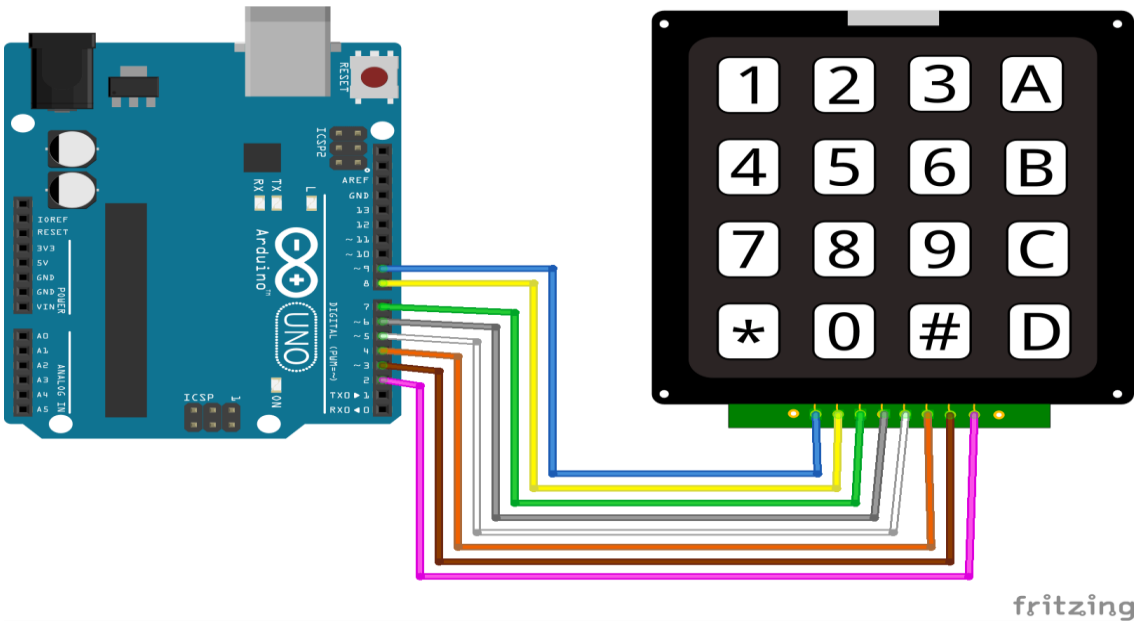


Figure. III. 3: keypad-4x4-arduino_bb.[38]

- **Le module RFID :**

- **Porte clé et Badge RFID :**

Ce type de matériel s'équipe généralement d'une antenne et d'une puce destinée à stocker des données.

- **Le module RC522**

  C'est une sorte de lecteur RFID.
  Est une interface qui permet l'identification sans contact à partir d'un badge ou une clé RFID.

III.2.2. Outils logiciels :

Le logiciel utilisé au cours de la réalisation de notre travail est présenté comme suit :

Le logiciel Arduino est un Environnement de Développement Intégré (IDE) open source et gratuit.

L'IDE Arduino est le logiciel qui permet de programmer les cartes Arduino.

L'IDE Arduino permet :

- D'éditer **un programme :** les programmes sont écrits en langage C.
- De **compiler ce programme** dans le langage « machine » de l'Arduino, la compilation est une traduction du langage C vers le langage du microcontrôleur.
- La **console** donne des informations sur le déroulement de la compilation et affiche les messages d'erreur.
- De **téléverser** le programme dans la mémoire de l'Arduino, le téléversement (upload) se passe via le port USB de l'ordinateur une fois dans la mémoire de l'Arduino, le logiciel s'appelle un microgiciel.
- La **console** donne des informations sur le déroulement du téléversement et affiche les messages d'erreur.

- De **communiquer avec la carte Arduino** grâce au terminal (ou moniteur série). Pendant le fonctionnement du programme en mémoire sur l'Arduino, il peut communiquer avec l'ordinateur tant que la connexion est active (câble USB, **…).[39]**

III.2.2.1. Présentation du logiciel Arduino :

Lorsque nous ouvrons l'application Arduino, cette interface apparaît.

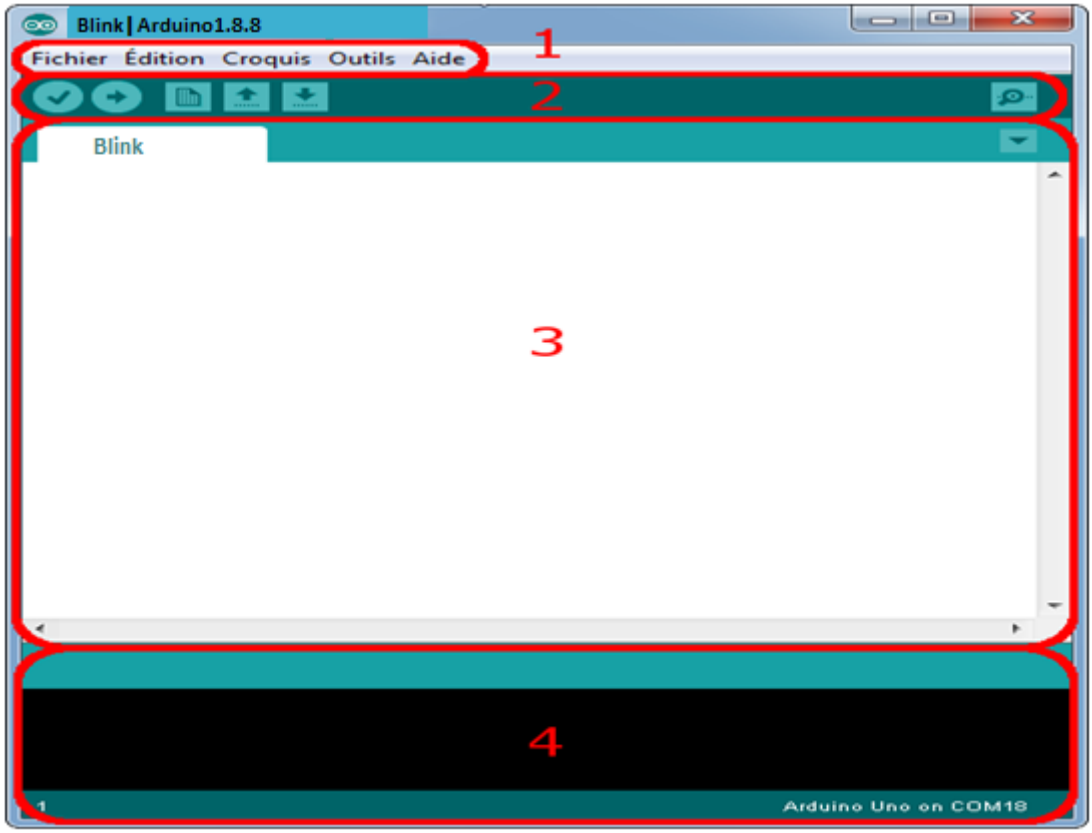


Figure. III. 4: Interface Arduino.

- **Le cadre numéro 1 :** Ce sont les options de configuration du logiciel.
- **Le cadre numéro 2 :** Il contient les boutons qui vont nous servir lorsque l'on va programmer nos cartes.
- **Le cadre numéro 3 :** Ce bloc va contenir le programme que nous allons créer.
- **Le cadre numéro 4 :** Celui-ci est important, car il va nous aider à corriger les fautes dans notre programme. C'est le débogueur.

III.2.2.2. Approche et utilisation du logiciel :

La barre des menus est entourée en rouge et numérotée par le chiffre 1.

✓ **Le menu file**

C'est principalement ce menu que l'on va utiliser le plus. Il dispose d'un certain nombre de choses qui vont nous être très utiles.

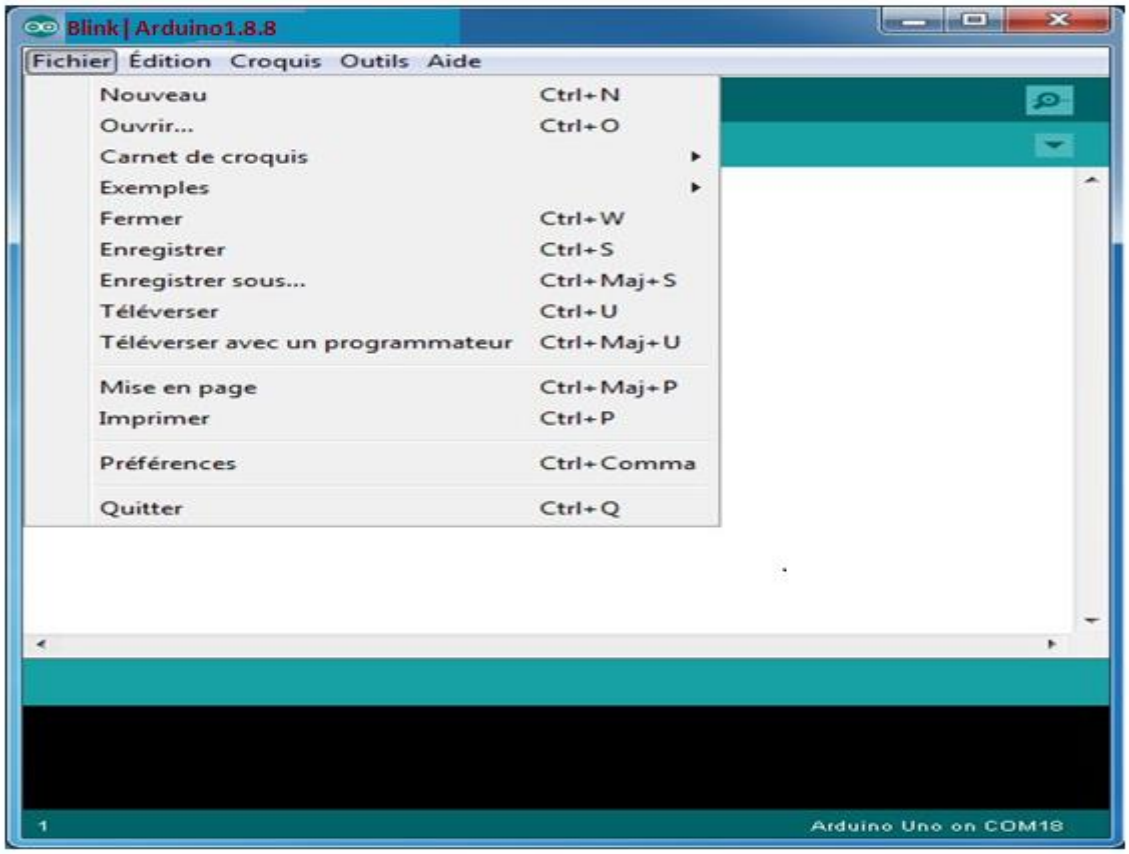


Figure. III. 5: Barre de menu.

- **Carnet de croquis :** Ce menu regroupe les fichiers que vous avez pu faire jusqu'à maintenant (et s'ils sont enregistrés dans le dossier par défaut du logiciel).
- **Exemples (exemples) :** Ceci est important, toute une liste se déroule pour afficher les noms d'exemples de programmes existants ; avec ça, vous pourrez vous aider/inspirer pour créer vos propres programmes ou tester de nouveaux composants.
- **Téléverser :** Permet d'envoyer le programme sur la carte Arduino.
- **Téléverser avec un programmateur :** Idem que ci-dessus, mais avec l'utilisation d'un programmateur.
- **Préférences :** Vous pourrez régler ici quelques paramètres du logiciel. Le reste des menus n'est pas intéressant pour l'instant.

✓ **Menu « Outils »**

Nous allons maintenant passer à la configuration de l'**IDE** Arduino pour notre carte Arduino. Pour ce faire, dans les options, nous devrons choisir le type de carte. Pour certaines cartes il faudra aussi choisir la fréquence, le type de compilateur, la vitesse de transfert et le port **COM** correspondant au canal de communication avec l'Arduino.

Pour **Arduino UNO**, nous choisissons ce qui suit :

- Carte Arduino / Genuino **UNO.**
- Le port **COM** correspondant à votre connexion.
- Programmeur : Arduino Gemma.

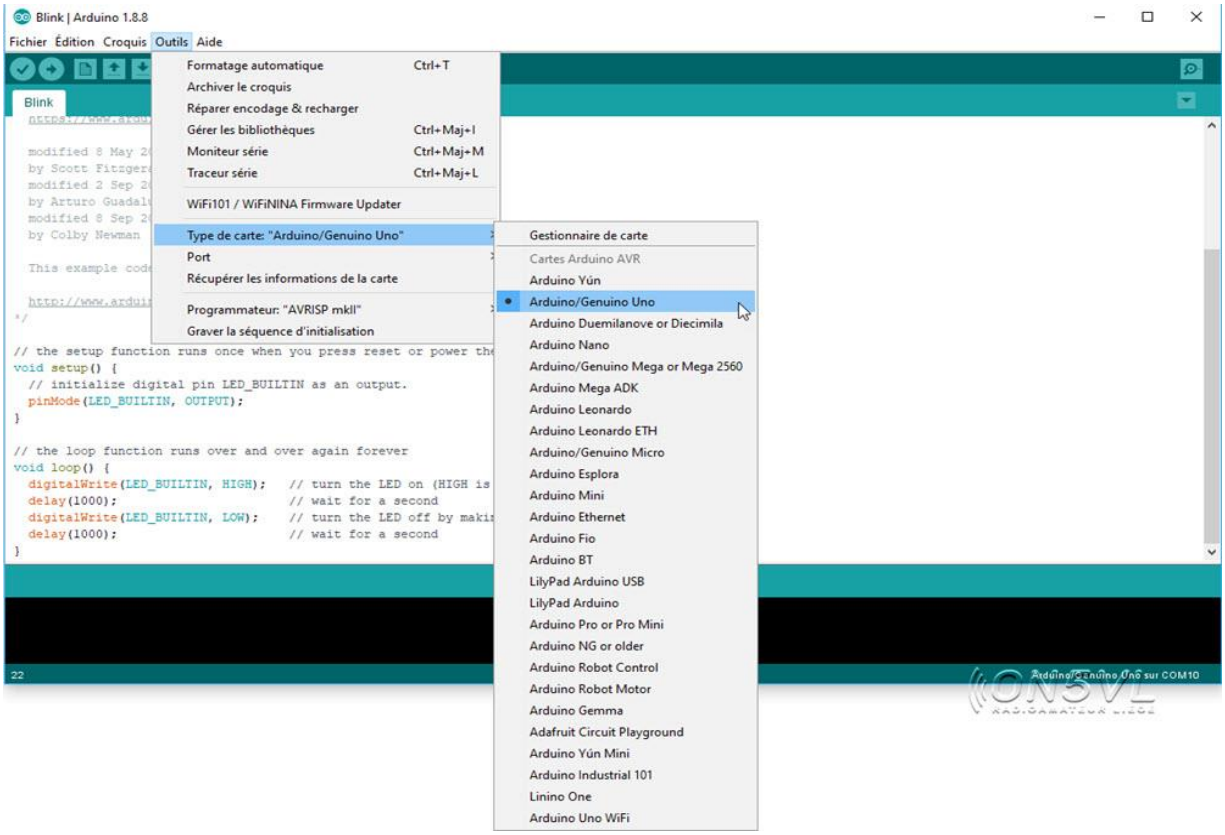


Figure. III. 6: Outils.

✓ **Les boutons**

Voyons à présent à quoi servent les boutons, encadrés en rouge et numérotés par le chiffre 2.

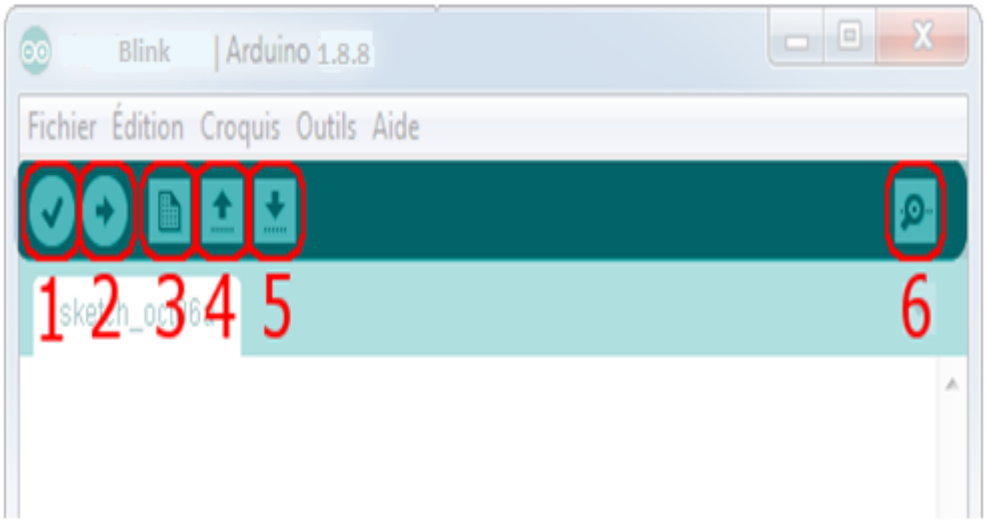


Figure. III. 7: Boutons.

- **Bouton 1 :** Ce bouton permet de vérifier le programme, il actionne un module qui cherche les erreurs dans votre programme.
- **Bouton 2 :** Charge (téléverse) le programme dans la carte Arduino.
- **Bouton 3 :** Crée un nouveau fichier.
- **Bouton 4 :** Ouvre un fichier.
- **Bouton 5 :** Enregistre le fichier.
- **Bouton 6 :** Ouvre le moniteur série.

III.2.2.3. Langages de programmation :

Dans cette partie, nous allons présenter le langage de programmation utilisé pour réaliser notre projet.

C++ est un langage de programmation compilé permettant la programmation sous de multiples paradigmes, dont la programmation procédurale, la programmation orientée objet et la programmation générique. Ses bonnes performances, et sa compatibilité avec le C en font un des langages de programmation les plus utilisés dans les applications où la performance est critique**. [36]**

III.3. Implémentation :

- ✓ **Arduino Libraires**

Nous devons télécharger un ensemble de bibliothèques sur l'application Arduino ide, afin de contrôler par programmation l'équipement utilisé dans notre projet.

```
// Include required libraries
#include <MFRC522.h>
#include <Keypad.h>
#include <SoftwareSerial.h>
#include <SPI.h>
#include <LiquidCrystal_I2C.h>
```

Figure. III. 8: Arduino libraries.

- ✓ **Initialisation**

Initialisation du mot de passe, tagID d'une carte identifiée, tag ID d'une carte bloquée.

```
char initial_password[4] = {'1', '2', '1', '2'};  // mot de passe
String tagUID = "7C B2 CF 37";  // id carte acces permis
String tagUIDB = "D2 97 D3 31";  //CARTE BLOQUEE
```

Figure. III. 9: Initialisation.

- ✓ **Afficher le message "Scannez carte"**

L'instruction qui permet d'afficher le message « Scannez carte » est :

```
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("SCANNEZ CARTE..");
```

Figure. III. 10: Scannez carte (code source).

- ✓ **Accès permis**

Le système compare l'identifiant de la carte passée par l'utilisateur avec l'identifiant enregistré dans le système précédemment, s'ils ont le même identifiant, le message "accès peremis" apparaît sur l'écran LCD, puis le système demande à l'utilisateur d'entrer son mot de passe.

```
if (tag.substring(1) == tagUID)
{
  Serial.println("Acces permis. ");
  Serial.println("Mot de passe");
  lcd.clear();
  lcd.setCursor(0, 1);
  lcd.print("Acces permis.");
  delay(2000);
  lcd.clear();
  lcd.print("Mot de passe:");
  lcd.setCursor(0, 1);
  RFIDMode = false;
}
```

Figure. III. 11: Accès permis (code source).

- ✓ **Carte bloquée**

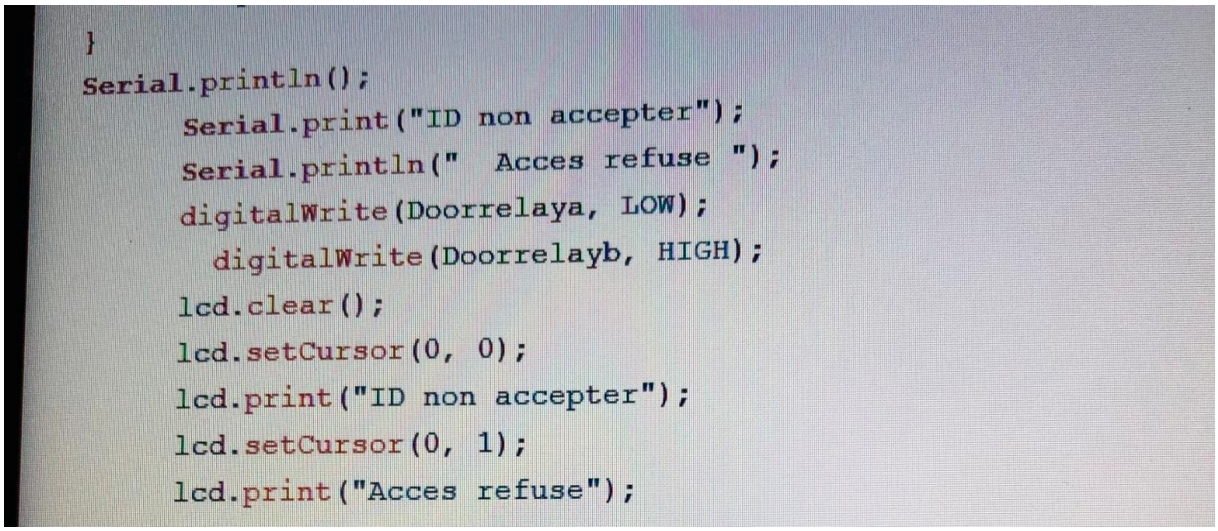
Si l'**ID** de la carte qui a été passée par l'utilisateur est le même que l'**ID** de la carte précédemment bloquée par le système, le système allume la **LED** rouge et l'écran **LCD** nous affiche le message « Carte bloquée contactez Admin ».

```
}
else   if (tag.substring(1) == tagUIDB)
{
     lcd.clear();
    lcd.print("CARTE BLOQUEE");
    delay(3000);
        digitalWrite(Doorrelaya, LOW);
    digitalWrite(Doorrelayb, HIGH);
   // lcd.clear();
     lcd.setCursor(0, 1);
lcd.print("CONTACTEZ ADMIN");
    i = 0;
    RFIDMode = true;
  }
```

Figure. III. 12: Carte bloquée (code source).

- ✓ **Carte non identifiée**

Lorsque vous passée une carte qui n'a pas été précédemment enregistrée dans le système, la LED rouge s'allume et le message suivant apparaît « id non accepter Accés refusé ».



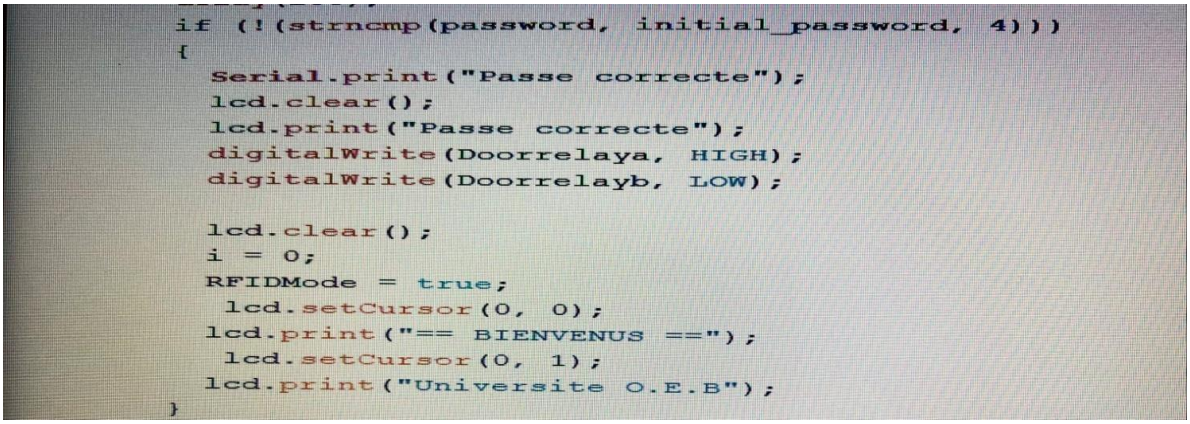
```
}
Serial.println();
      Serial.print("ID non accepter");
      Serial.println("  Acces refuse ");
      digitalWrite(Doorrelaya, LOW);
        digitalWrite(Doorrelayb, HIGH);
      lcd.clear();
      lcd.setCursor(0, 0);
      lcd.print("ID non accepter");
      lcd.setCursor(0, 1);
      lcd.print("Acces refuse");
```

Figure. III. 13: Carte non identifiée (code source).

- ✓ **Mot de passe**

Mot de passe correct :

Le système compare le mot de passe saisi par l'utilisateur avec le mot de passe enregistré dans le Système. Si les deux mots de passe sont identiques, le LED vert s'allume et le message apparaît : « passe correcte » , puis L'écran s'affiche le message suivant « Bienvenus Universite O.E.B».



```
if (!(strncmp(password, initial_password, 4)))
{
  Serial.print("Passe correcte");
  lcd.clear();
  lcd.print("Passe correcte");
  digitalWrite(Doorrelaya, HIGH);
  digitalWrite(Doorrelayb, LOW);

  lcd.clear();
  i = 0;
  RFIDMode = true;
   lcd.setCursor(0, 0);
  lcd.print("== BIENVENUS ==");
   lcd.setCursor(0, 1);
  lcd.print("Universite O.E.B");
}
```

Figure. III. 14: Mot de passe correct (code source).

Mot de passe incorrect :

Si l'utilisateur a saisi mot de passe incorrect, le LED rouge s'allume et le message apparaît « passe incorrect ».

```
else
{
  Serial.println("Passe incorrect");
  lcd.clear();
  lcd.print("Passe incorrect");
  delay(5000);
      digitalWrite(Doorrelaya, LOW);
  digitalWrite(Doorrelayb, HIGH);
```

Figure. III. 15: Mot de passe correct (code source).

III.4. Présentation de l'application

Notre logiciel se présente sous la forme d'un boitier électronique contenant un Arduino, une carte RFID, un afficheur LCD, un clavier électronique, et une LED rouge et verte, ces éléments sont reliés à un jeu de fils. L'aspect final de la boîte est montré dans l'image suivante :

Figure. III. 16: Interface concrète du projet.

Au démarrage du programme l'écran **LCD** nous affiche le message suivant :

Figure. III. 17: Scannez carte.

L'utilisateur passe la carte ou le tag sur le lecteur RFID en suivant le symbole d'aide comme indiqué dans l'image suivante :

Figure. III. 18: Passage du tag.

A cette étape, on distingue 3 cas de la carte:

- **Carte anonyme :**

Si la carte n'a pas été préalablement enregistrée dans le système par l'administrateur, lors du passage de la carte, l'écran LCD affiche le message suivant avec une LED rouge allumée :

Figure. III. 19: Carte anonyme.

- **Carte bloquée :**

Si la carte a été bloquée par l'administrateur pour une raison quelconque (par exemple : la carte est perdue ou endommagée, etc.), ce qui suit apparaît.

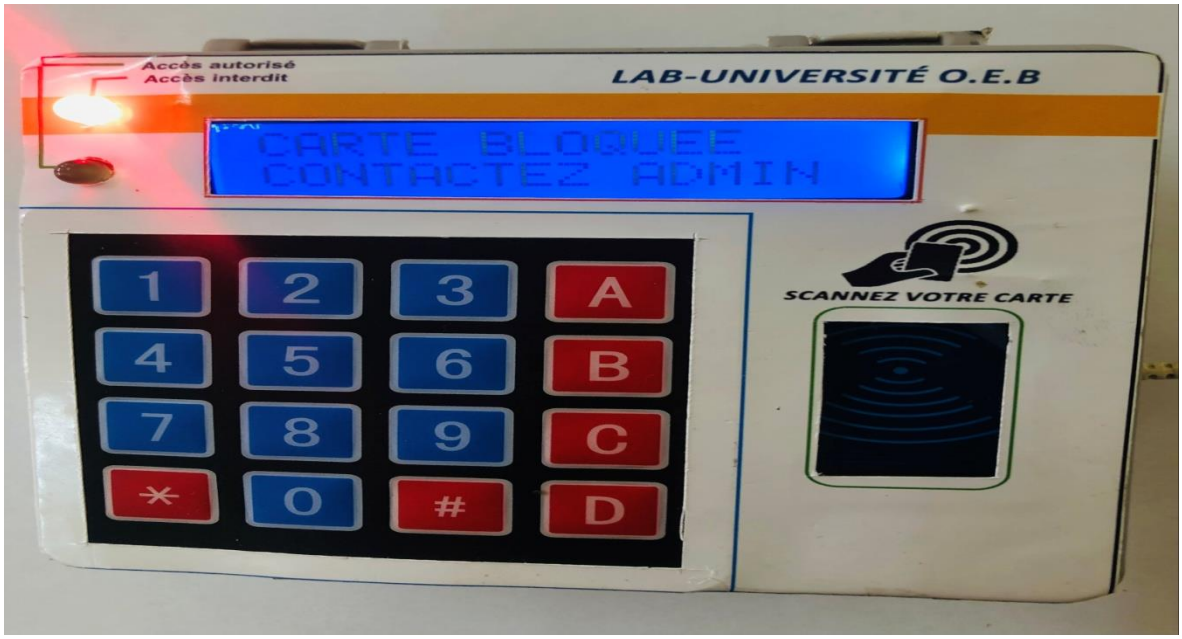


Figure. III. 20: Carte bloquée.

- **Carte identifiée** :

Si la carte est enregistrée dans le système, le message qui s'affiche est le suivant :

Figure. III. 21: Carte identifiée.

Ensuite, le système demande à l'utilisateur d'entrer son mot de passe.

Figure. III. 22: Demande du mot de passe.

Si le mot de passe est correct, le message suivant s'affiche avec une LED verte allumée:

Figure. III. 23: Bienvenus (Université O.E.B).

Si le mot de passe est erroné, le message suivant apparaît avec une LED rouge allumée:

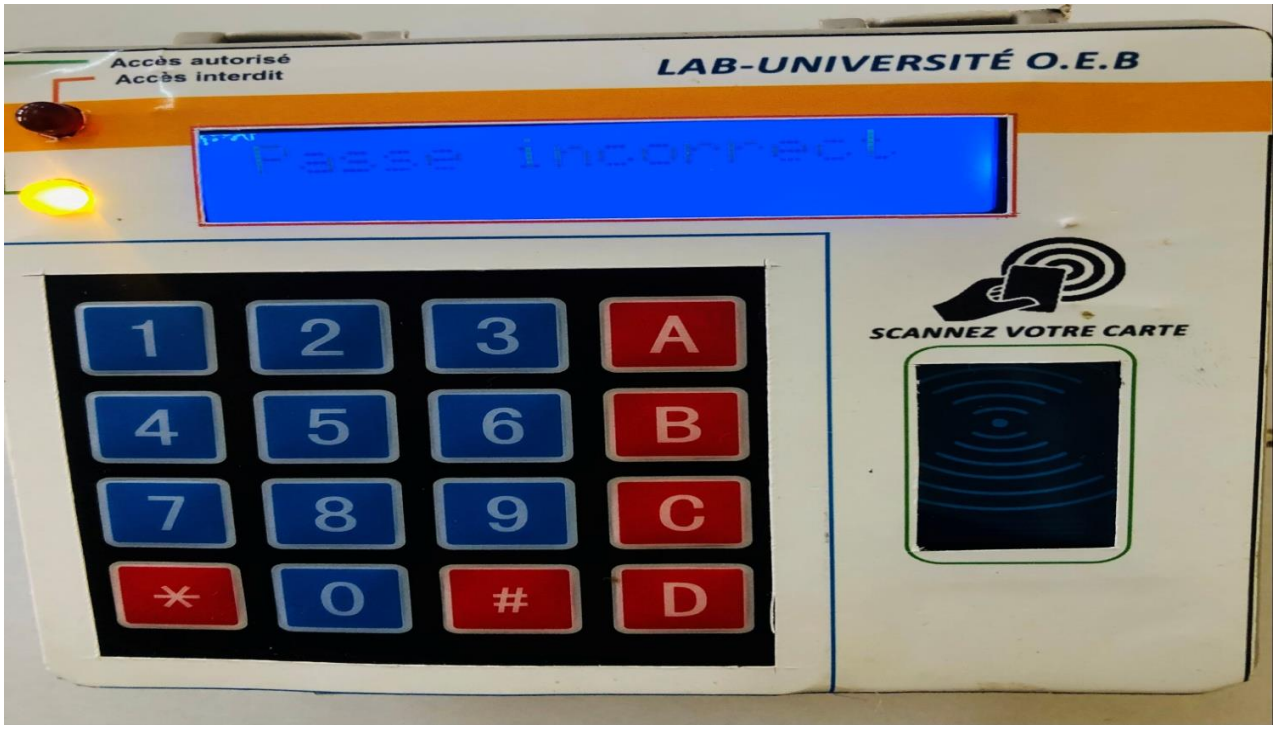


Figure. III. 24: Mot de passe erroné.

III.5. Conclusion :

Dans ce dernier chapitre on a présenté les étapes de création de notre projet qui consiste à l'étude et réalisation d'un système de contrôle d'accès sécurisé à base d'une carte Arduino connecter au module **RFID,** utilisant des différents tags (autorisées et non autorisées) nous avons testé le bon fonctionnement de notre montage par le biais d'un affichage **LCD.**

Nous avons ajouté d'autres témoins de bon fonctionnement tels que les **LED**.

Notre contribution réside dans l'ajout d'un clavier matriciel pour sécuriser en plus notre système d'accès car le tag RFID peut être perdu et n'importe quel individu peut être l'utiliser.

CONCLUSION GENERAL

Dans ce projet, nous avons réalisé un système de contrôle d'accès sécurisé basé sur la technologie RFID et gérer par la carte Arduino dans lequel l'utilisateur devra d'abord scanner la bonne étiquette et ensuite il devra entrer son mot de passe. Nous avons également ajouté d'autres témoins tels que les LED afin que l'utilisateur connaisse comment gérer son système, en plus un afficheur LCD qui garantit l'interaction homme-machine avant d'entrée à des lieux privés et importants tels que les banques, les laboratoires de recherche, les hôtels et les grandes entreprises.

Le système conçu et réalisé de sécurité de contrôle d'accès est basé sur l'identification par radiofréquence a permis d'automatiser la tâche d'ouverture et de la fermeture des portes par l'utilisation d'un microcontrôleur et un lecteur RFID avec l'avantage de garder l'historique d'accès.

Ce projet nous a poussé à apprendre et à utiliser une grande panoplie d'outils comme programmer un microcontrôleur par l'utilisation de l'application Arduino dans la conception de notre circuit électronique parce qu'il est riche en composants nécessaires et convivial et aussi la coordination des composants électroniques pour assurer un haut niveau de sécurité.

L'utilisation de l'Arduino des cartes d'interfaces a grandement facilité la réalisation du système et nous a permis d'obtenir un résultat assez concluant.

REFERENCES BIBLIOGRAPHIQUES

[1] Bruce Schneier, « do we really need a security industry? », deuxième édition, Massachusttes ,boston, 3 mai 2007.

[2] Demain Ecrohert,Foermi Customer,Success Enginier, « Application dans le monde réel»,article,mis à jour :17 octobre 2022.

[3] Solange Ghernaouti, « Cybersécurité Analyser les risques Mettre en œuvre les solut ions »,6éme édition, article.

[4] https://fr.theastrologypage.com/nonrepudiation ,Consulté le 23/03/2023.

[5] https://www.lemagit.fr/definition/Authentification ,Consulté le 23/03/2023.

[6] https://www.checkpoint.com/fr/cyber-hub/what-is-network-security/ , Consulté le 25/03/2023.

[7] Laurent Bloch, Christophe Wolfhugel, Christian Queinnec, Hervé Schauer, Nat Makarévitch , « Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs», EYROLLES, 2éme edition, 2013.

[8] Sofiene Boulares, « Validation des politiques de sécurité par rapport aux modèles de contrôle d'accès », Mémoire de Magister en Informatique, Université du Québec en Outaouais, Aout 2010.

[9] MEMEL EMMANUEL LATHE, « Gestion de droits d'accès dans des réseaux Informatiques », Québec, Canada, 2016.

[10] Fares KHELOUFI, Yacine IKHLEF « généralités sur la sécurité informatique et motivations », Master en Informatique, Université Kasdi Merbah, Ouargla, octobre 2014.

[11] Younis A. Younis, Kashif Kifayat, Madjid Merabti, « An Access control model for cloud computing », School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool L3 3AF, UK.

[12] AINENNAS Faiza, ZIDI Nassima, « contrôle d'accès aux services sensibles au contexte », Mémoire de Master en Informatique, Université Abderahman Mira de Béjaia,2015.

[13] KHELIFA Nor Eddine, « Intégration du modèle de contrôle d'accès RBAC (Role-Based Access control) dans les diagrammes UML (Cas d'Utilisation et Séquence », Mémoire de Magister Informatique, université d'Oran.

[14] NICOLE Kelly, « 3 Types of Access Control: IT Security Models Explained», article, mis à jour: 4th, 2023.

[15] https://www.ekransystem.com/en/blog/mac-vs-dac,consulté le 23/03/2023.

[16] CITRIX staff, «Role Based Access Control overview», article, mis à jour :7 septembre 2020.

[17] KHELIFA Nor Eddine, « Intégration du modèle de contrôle d'accès RBAC (Role-Based Access control) dans les diagrammes UML (Cas d'Utilisation et Séquence », Mémoire de Magister Informatique, université d'Oran ,2017.

[18] KEBA Gueye, GERVAIS Mendy, SAMUEL Ouya, «Access Control Model Based on Dynamic Delegations and Privacy in a Health System of Connected Objects», article. 22 March 2019

[19] https://altec.ch/technologies/les-tags-rfid/ Consulté le 31/03/2023.

[20] https://web.maths.unsw.edu.au/~lafaye/CCM/rfid/rfid-intro.htm, Consulté le 31/03/2023.

[21 https://www.scribd.com/document/467850724/RFID-Contro-le-d-8217-acce-s-par-badge-avec-Arduino#, Consulté le 31/03/2023.

[22] https://www.mikroe.com/rfid-tag-1356mhz, Consulté le 01/04/2023.

[23] https://www.datacarte.com/prod/cartes-blanches-0014-po/, Consulté le 01/04/2023.

[24] https://forum.arduino.cc/t/module-rfid-lecture-recto-verso/521066,Consulté le 02/04/2023.

[25]https://heliantha.ma/iot/39-arduino-module-lecteur-de-cartes-rfid.html,Consulté le 02/04/2023.

[26] http://www.gotronic.fr , Consulté le 02/04/2023.

[27] https://wikifab.org/w/index.php?title=Arc-en-ciel_avec_Arduino&embed=true#!/step/4 ,Consulté le 03/04/2023.

[28] https://plaisirarduino.fr/rfid-avec-arduino/,Consulté le 03/04/2023.

[29] https://docs.arduino.cc/built-in-examples/communication/Dimmer,Consulté le 03/04/2023.

[30] http://www.techmania.fr/arduino/Decouverte_arduino.pdf, Consulté le 02/04/2023.

[31] https://plaisirarduino.fr/afficheur-lcd-comment-lexploiter/, Consulté le 02/04/2023.

[32] http://micol1.free.fr/Arduino/Arduino-lecon25.html,Consulté le 03/04/2023.

[33] https://laurent-audibert.developpez.com/Cours-UML/?page=diagramme-cas-utilisation.

[34] http://docwiki.embarcadero.com/RADStudio/Rio/fr/D%C3%A9finition_des_diagrammes_d%27activit%C3%A9s_UML_2.0.

[35] SUBRAMANIAN, «4×4 Keypad Details with Arduino», article,29 may 2021.

[36] Xukyo, «Utilisation d'un Clavier numérique 4×4 avec Arduino», 5 Mai 2020, article.

[37] https://learn.sparkfun.com/tutorials/installing-arduino-ide/all,Consulté le 16/05/2023.

[38] https://isocpp.org,Consulté le 16/05/2023.

[39] https://docs.arduino.cc/learn/starting-guide/getting-started-with-arduino-tools , Consulté le 17/05/2023.