Design and Implementation of an intelligent system for automatic verification of attendance and authorization in an examination room: Case of the University ULPGL

Article · May 2020

CITATIONS
0

READS
506

2 authors, including:

Vingi Patrick Nzanzu
Covenant University Ota Ogun State, Nigeria
7 PUBLICATIONS **15** CITATIONS

SEE PROFILE

International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 48 No. 2 May 2020, pp. 58-69

http://www.ijisr.issr-journals.org/

Conception et mise en œuvre d'un système intelligent pour la vérification automatique de présence et d'autorisation dans une salle d'examen : Cas de l'université ULPGL

[Design and Implementation of an intelligent system for automatic verification of attendance and authorization in an examination room: Case of the University ULPGL]

Patrick Nzanzu Vingi[1] and Claude Takenga[1-2-3]

[1]Génie Electrique et Informatique, Université Libre des Pays des Grands Lacs, BP 360 Goma, Goma, RD Congo

[2]Infokom GmbH, Entreprise NTIC, Neubrandenburg, Germany

[3]Université Officielle de Ruwenzori, Butembo, RD Congo

ABSTRACT: Attendance control is a standard practice in every educational system. In response to this, methods used to take exam attendance are quite numerous, but emphasis keeps shifting towards automating the process. The University ULPGL (Université Libre des Pays des Grands Lacs) in Goma, Democratic Republic of Congo does apply the traditional manual method for identification and elaboration of attendance lists in exam rooms. This manual process of verifying eligible students and counting copies of participants causes a significant delay. Moreover, in such a system, cheaters may easily take exams for others. To address these issues, an intelligent and efficient system is conceived and developed in this paper. After enrolling all attendees by storing their data along with their unique badge code and/or fingeprint, the designed system automatically takes exam attendance and check for eligibility by applying the RFID and/or fingerprint technologies and searching for a match in the created database. To enhance security, the face image of the registered student for the scanned card or captured fingerprint is displayed in order to enable the supervisor to compare that face with the present student. This process eliminates fraud and saves processing and verification time. 60 students tested the system and the success rate was 100% while reducing the average processing time to 3 and 6 seconds per student instead of 25 seconds in the traditional manual process.

KEYWORDS: Fingerprint, RFID, intelligent system, access control, microcontroller, management system.

RESUME: La vérification de présence est devenue une pratique courante dans tous les systèmes éducatifs. En réponse à cette situation, il existe des nombreuses méthodes de vérification mais l'accent est mis sur l'automatisation du processus. L'Université Libre des Pays des Grands Lacs (ULPGL) à Goma, en République Démocratique du Congo, applique encore la méthode manuelle traditionnelle pour l'identification et l'élaboration des liste de présence dans les salles d'examen. Ce processus manuel de vérification des étudiants éligibles et de comptage du nombre de copies des participants entraîne un retard important. En plus de cela, certaines personnes malhonnêtes peuvent passer des examens à la place des autres. Pour répondre à ces préoccupations, un système intelligent et efficace est conçu et développé dans ce travail. Après avoir inscrit tous les participants en stockant leurs données avec leur code de badge et / ou empreinte digitale uniques, le système enregistre automatiquement les présences à l'examen et vérifie l'éligibilité en appliquant les technologies RFID et / ou d'empreinte digitale en recherchant une correspondance dans la base de données créée. Pour renforcer la sécurité, la photo de la personne enregistrée dans la base de données est affichée sur l'écran afin de permettre au surveillant de se rassurer que ce soit bien la personne porteuse de cette carte. Ce processus élimine toute fraude et permet de gagner en temps de traitement des vérifications et d'enregistrements. 60 étudiants ont testé le système et le taux de réussite a été de 100% tout en réduisant le temps moyen d'exécution à 3 et 6 secondes par étudiant au lieu de 25 secondes avec la méthode manuelle.

MOTS-CLEFS: Empreinte digitale, RFID, intelligent system, contrôle d'accès, microcontrôleur , système de gestion.

Corresponding Author: Claude Takenga

1 INTRODUCTION

Dans de nombreuses institutions et organisations académiques, la présence est un critère très important utilisé à diverses fins. Ces objectifs incluent la tenue de dossiers, l'évaluation des étudiants et la promotion d'une présence optimale et régulière en classe. La vérification de la présence et le contrôle d'accès deviennent de plus en plus populaires dans beaucoup des domaines, et dans toutes les catégories confondues [1, 2]. La capacité de vérifier, de limiter l'accès à des personnes préautorisées pour une salle d'examen d'une manière automatisée, est certainement beaucoup plus attrayante.

De nos jours, prendre la présence des étudiants dans une salle examen d'une manière automatique permet non seulement de tenir un registre de participation mais aussi de faciliter la tâche aux organisateurs d'examen pour classifier les étudiants selon les promotions et les examens passés. Et cette stratégie n'est pas mise en application à l'Université Libre des Pays des Grands Lacs, en raison des divers défis posés par la méthode actuelle de prise des présences. Cette méthode traditionnelle implique l'utilisation de feuilles de papier pour assurer la présence des étudiants. Cette méthode pourrait facilement permettre l'usurpation d'identité et la feuille de présence pourrait être volée ou perdue. Ce processus manuel prend du temps et il est difficile de déterminer le nombre d'étudiants qui ont atteint le pourcentage minimum et qui sont donc admissibles à l'examen. Il est aussi à souligner que lors des examens, la vérification des étudiants en ordre financièrement et admissibles à l'examen sur des listes manuscrites prend énormément du temps, cause des retards et peut facilement induire aux fraudes. De nos jours, la vérification de la présence et l'autorisation d'accès des étudiants dans une salle d'examen est une tâche compliquée à cause du nombre d'étudiants qui peut être considérablement élevé. Ceci peut encore devenir plus complexe si plusieurs promotions doivent passer leurs examens dans une même salle.

Il est donc nécessaire de disposer d'un système qui éliminerait tous ces désagréments. Pour mieux cerner cette équivoque, un questionnement nous traverse l'esprit : Concrètement, y' a-t-il des moyens efficaces permettant un traitement rapide de contrôle ainsi qu'une facilité dans la tâche d'enregistrement et de vérification des présences des étudiants dans une salle d'examen ?

Eu égard à la question susmentionnée, un système intelligent (constitué soit des cartes RFID, des lecteurs de ces dernières ou des lecteurs d'empreintes digitales, soit les deux technologies combinées) est proposé. En supposant que chaque étudiant dispose d'une carte avec transpondeur RFID pour l'application de la technologie RFID, le système devrait assister les surveillants dans l'autorisation d'accès à la salle d'examen et l'enregistrement automatique des présences. Le cœur du système sera conçu sur base des technologies RFID ou/et biométrique (Fingerprint) avec le concours de la plateforme avec microcontrôleur Arduino. Une application web permettra également de configurer, de gérer le système et d'obtenir le dépouillement des présences.

Plutôt que de signer une feuille de présence, les étudiants useront de leurs cartes RFID ou/et passeront leur pouce sur le lecteur d'empreintes digitales pour vérifier s'ils sont admissibles à l'examen. L'empreinte digitale et/ou le code de badge est comparé à une liste d'étudiants préenregistrés et, une fois la correspondance effectuée, l'étudiant sera enregistré comme ayant participé à l'examen.

N'étant surement pas les seuls à nous intéresser à ce domaine dans notre milieu, moins encore dans le monde, citons quelques travaux connexes :

Des millions de dollars sont perdus chaque année dans des organisations à travers le Nigeria en raison de services médiocres rendus à divers clients dans des organisations rapporte [3]. Cela est dû au fait qu'un système de gestion de la présence en bonne et due forme n'est pas en place dans diverses organisations à travers le pays. La gestion des relevés de présence du personnel au quotidien est devenue un défi difficile. Les efforts requis pour générer un rapport mensuel et connaître le nombre cumulé de personnel sont devenus une tâche majeure, car l'évaluation manuelle produit des erreurs et prend également beaucoup de temps. Pour cette raison, un système électronique efficace de présence du personnel utilisant les empreintes digitales est appliqué. Ce processus élimine le besoin de matériaux fixes pour la tenue des dossiers ; cela élimine les problèmes d'usurpation d'identité.

Grégory COSTE dans son article [4] « Sécurité : 10 solutions de contrôle d'accès pour protéger l'entreprise et ses collaborateurs », renseigne que de plus en plus des professionnels mettent désormais en place des solutions de contrôle d'accès par badge RFID, car cette technologie présente bien des avantages :

- Une technologie standardisée et supportée par de nombreux acteurs du marché,
- Un confort de lecture pour l'usager qui a juste à présenter son badge à quelques centimètres du lecteur,
- Une durabilité importante (pas d'usure mécanique),
- Des possibilités de personnalisation importantes,
- Une ouverture à d'autres applications internes (photocopieurs, restaurant d'entreprise, ...),
- Un niveau de sécurité intrinsèque important (carte Desfire® pour la technologie Mifare® par exemple),

- Une bonne résistance aux perturbations et contraintes d'environnement.

Ces badges RFID sont lus sur des lecteurs eux-mêmes connectés à des UTL (Unité de Traitement Local). Ces UTL permettent de raccorder plusieurs têtes de lecture au réseau informatique (un rôle de concentrateur) et elles disposent en générale de l'intelligence locale nécessaire pour autoriser ou refuser une autorisation d'accès. Cette fonctionnalité est indispensable en cas de panne du serveur ou du réseau IP car dans ce cas, la continuité de fonctionnement est assurée. Il ajoute en disant que le contrôle d'accès biométrique permet d'identifier une personne en fonction de ses caractéristiques physiques. Les parties du corps les plus couramment utilisées sont l'œil pour la reconnaissance optique de l'iris et les doigts pour la reconnaissance des empreintes digitales.

La présence est un facteur important pour mesurer l'admissibilité et la tenue des dossiers pour l'évaluation des étudiants. Plusieurs systèmes de vérification et de prise de présence automatisés ont été développés [1, 5]. Ces systèmes sont principalement basés sur un modèle à un seul facteur, ce qui pose une ligne de faille de sécurité. L'utilisation d'un système d'assistance multifactoriel qui utilise la flexibilité de la technologie RFID et la sécurité de la biométrie des empreintes digitales pour gérer les présences des étudiants montre des performances considérables en termes de temps de réponse et sécurité.

Les Nouvelles Technologies de l'Information et de la Communication (NTICs) ont bouleversé notre vie quotidienne. Automobiles, avions, trains, satellites, téléphones portables, portails et portes, maison d'habitation, ... rien de ce qui communique ou se déplace ne peut le faire sans électronique et onde électromagnétique renseigne [6].

2 MATERIELS, METHODES ET PRESENTATION DU SYSTEME

2.1 PRESENTATION ET DESCRIPTION DE L'EXISTANT

Chaque génération ayant ses besoins et défis particuliers, nous prenons en compte les réalités et facteurs existant en ville de Goma spécifiquement à l'Université Libre des Pays de Grands Lacs Goma (ULPGL Goma). Lorsque les examens sont organisés à l'UPLGL, l'autorisation d'accès à la salle d'examen et la vérification de la présence des étudiants est une tâche fastidieuse. Elle prend énormément de temps, elle réduit parfois la concentration et oblige les surveillants à constituer des listes selon la promotion de chaque étudiant.

Le système proposé fournit une solution aux problèmes de vérification d'admissibilité et d'enregistrement des présences des étudiants en utilisant un logiciel de gestion des présences qui interface un dispositif constitué soit des lecteurs de carte RFID ou d'empreinte digitale ou soit hybride. Les informations de l'étudiant (Numéro matricule, photo, nom, post nom, prénom, âge, sexe, adresse, le code de badge et l'empreinte digitale) sont enregistrées en premier dans la base de données. La carte RFID est lue via un lecteur RFID et l'empreinte est capturée en utilisant un lecteur d'empreinte digitale. Ces éléments sont ensuite comparés aux informations préalablement enregistrées dans la base de données.

2.2 CONTROLE D'ACCES AVEC LA TECHNOLOGIE RFID

Le contrôle d'accès par badge magnétique ou code-barres, longtemps utilisé, n'existe pratiquement plus aujourd'hui. Notons que la technologie en vogue est désormais celle qu'intègrent des solutions de contrôle d'accès par badge RFID. L'identification par radiofréquences, également connue sous l'acronyme RFID, est une technologie de lecture et d'écriture à distance, par fréquences radio. Par sa principale propriété, celle de réaliser une communication sans contact, elle apparaît au début du XXIème siècle comme une technologie émergente dans la gestion des flux d'une économie globale, en particulier dans le domaine de la traçabilité des objets, des animaux, mais aussi celui de l'identification des personnes. Dès les années 2000, cette technologie semble être arrivée à un point crucial de maturité et son avenir économique s'annonce prometteur [7].

Le principe de fonctionnement de cette technologie est de plus simple. En plus d'une partie de stockage et de traitement, un système RFID est composé de deux entités qui communiquent entre elles :

- Un tag ou étiquette intelligente (aussi appelé transpondeur), associé à l'élément à identifier. Il est capable de répondre à une demande venant d'un lecteur.
- Une station de base ou lecteur RFID qui a pour mission d'identifier l'étiquette. Le lecteur envoie une onde électromagnétique en direction de l'élément à identifier. En retour, il reçoit l'information renvoyée par l'étiquette.
- Un ordinateur de stockage et de traitement des informations recueillies par le lecteur (facultatif), [8].

Trois types de puce RFID peuvent être distingués :

- Les puces passives : elles fonctionnent sans batterie et sont activées au moyen d'un lecteur émetteur-récepteur qui leur transmet des ondes magnétiques (ex. : badges RFID).
- Les puces actives : elles possèdent leur propre batterie et transmettent de façon autonome des informations qu'elles enregistrent au capteur.
- Les puces intelligentes : elles sont munies d'un système de sécurité qui permet de crypter les informations qu'elles contiennent. Les données pour être accessibles nécessitent une identification (ex. : carte bancaire). [9]

La RFID, comment ça marche ?

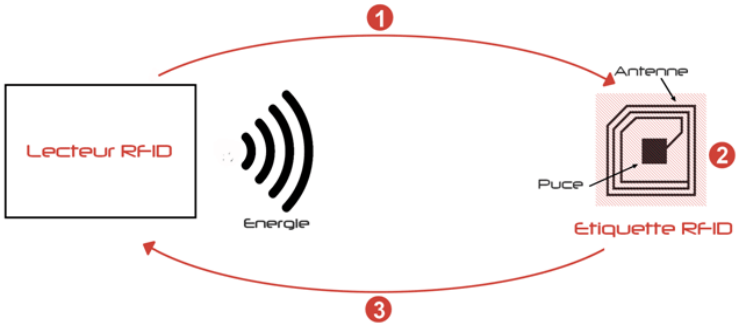


Fig. 1. Fonctionnement basique de l'étiquette RFID

① Le lecteur envoie un signal à la puce lui demandant des informations

② L'antenne capte le signal, le transfert à la puce

③ La puce renvoie les informations à l'antenne, qui les transferts au lecteur.

2.3 CONTROLE D'ACCES AVEC LA TECHNOLOGIE BIOMETRIQUE (FINGERPRINT)

Comme toute technologie, la RFID possède ses propres limites. La diffusion de l'information pose problème pour toutes les questions sur la sécurité de la vie privée. Une carte non sécurisée peut être facilement copiable pour récupérer ou modifier les données sensibles, [10]. Certaines conditions peuvent généralement poser des problèmes avec les appareils électroniques : eau, décharges d'électricité statique, la foudre et les aimants de haute puissance peuvent poser des problèmes pour les systèmes RFID, [11].

Pour pallier ces insuffisances des technologies RFID, les systèmes biométriques sont prônés. Un système biométrique permet d'identifier une personne ou vérifie l'admissibilité d'une personne « à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main, ...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche), [1, 12]. Les empreintes digitales - appelées aussi dermatoglyphes - sont une signature que nous laissons derrière nous à chaque fois que nous touchons un objet. Les motifs dessinés par les crêtes et plis de la peau sont différents pour chaque individu ; c'est ce qui motive leur utilisation dans pléthore des secteurs de la vie courante, [13].

Plusieurs méthodes sont employées pour reconnaître les empreintes digitales : localisation des minuties, traitement de textures, etc.

- Localisation des minuties : cette méthode ne retient que l'emplacement des minuties les plus pertinentes. Elle est peu sensible aux déformations des doigts entre plusieurs vérifications (doigts plus ou moins appuyés sur le capteur).
- Traitement de textures : des paramètres issus de certaines propriétés de la texture des empreintes (orientation, fréquence, etc.) sont comparés. Cette méthode permet un traitement très rapide, et donc un temps de réponse très court.

Les principales étapes avec la localisation des minuties sont illustrées par la Fig. 2 :

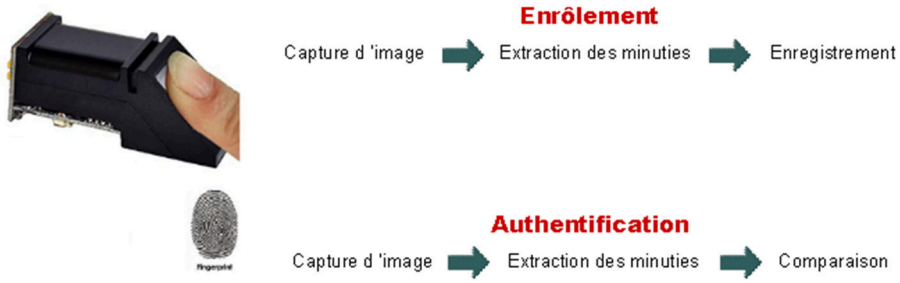


Fig. 2. Principales étapes d'extraction et comparaison d'empreintes digitales

2.4 CONCEPTION DU SYSTÈME

En vue de permettre une fluidité dans le processus de vérification de présence des étudiants dans une salle d'examen, arrive la réflexion de recourir à un système permettant de connaitre avec exactitude la liste de tous les étudiants dans la salle d'examen et la promotion de tout un chacun. Le système est destiné à contenir des données liées aux différents flux ayant trait avec la présence et la participation à l'examen. Le but reste et demeure celui de créer un outil d'aide à la vérification de présence et l'autorisation automatique d'accès à la salle d'examen. Le système ici proposé est baptisé « SPCheckUP » (pour Student Présence Check-up).

L'étudiant scanne la carte/badge RFID ou place le doigt au lecteur fingerprint et selon la décision du microcontrôleur/base de données, soit la porte de la salle ou le dispositif tourniquet laisse entrer l'étudiant s'il est en ordre, soit la porte ne laisse pas passer en allumant la lampe jaune ou rouge selon le cas, (Fig.3). Le bloc de vérification de l'éligibilité de l'étudiant à l'examen est un indicateur rapide au surveillant de l'examen : une LED verte s'allume si l'étudiant est en ordre, une LED jaune s'allume si l'étudiant est enregistré mais n'est pas en ordre (frais scolaire) et en fin une LED rouge s'allume si l'étudiant n'est pas enregistré dans la base de données. En plus de cela, en entrant, la photo de l'étudiant s'affiche pour permettre au surveillant de se rassurer que l'examen ne soit pas fait par une autre personne.

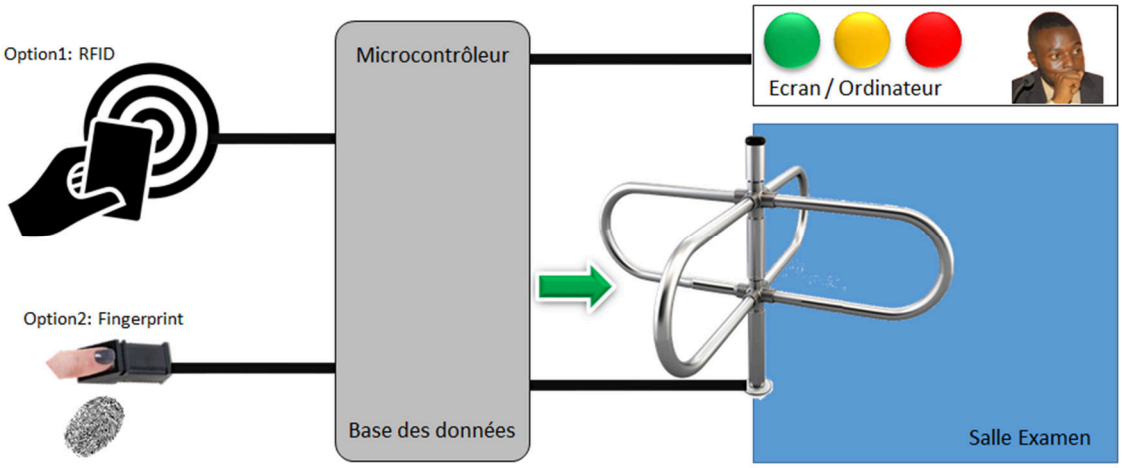


Fig. 3. Système proposé : automatisation de l'accès à la salle d'examen

Le système repose sur deux grandes parties : une partie " application web " permettant de traiter les informations et les rendre disponible et accessible pour ceux qui en ont besoin (notamment les organisateurs d'examens, les différentes facultés, ...) ; une partie matérielle constituée par la carte Arduino, de module RFID, de module d'empreinte digitale et d'un module WIFI pour transmettre au système les informations de chaque étudiant.

Nous proposons trois systèmes différents qui seront implémentés et testés dans ce travails :

- Implémentation avec technologie RFID, dont l'organigramme est illustré par la (Fig.4)
- Implémentation avec technologie Fingerprint, dont l'organigramme est illustré par la (Fig.5)
- Implémentation avec technologie Hybride RFID-Fingerprint, dont l'organigramme est illustré par la (Fig.6)

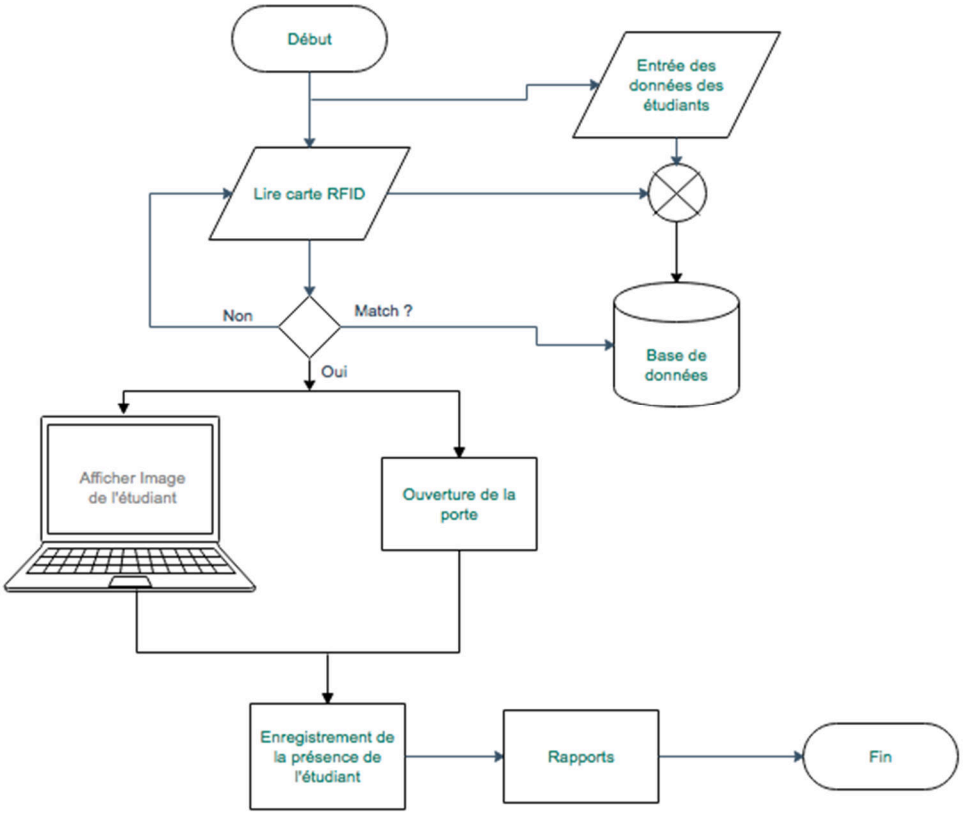


Fig. 4. Option1 : Organigramme du système avec technologie RFID

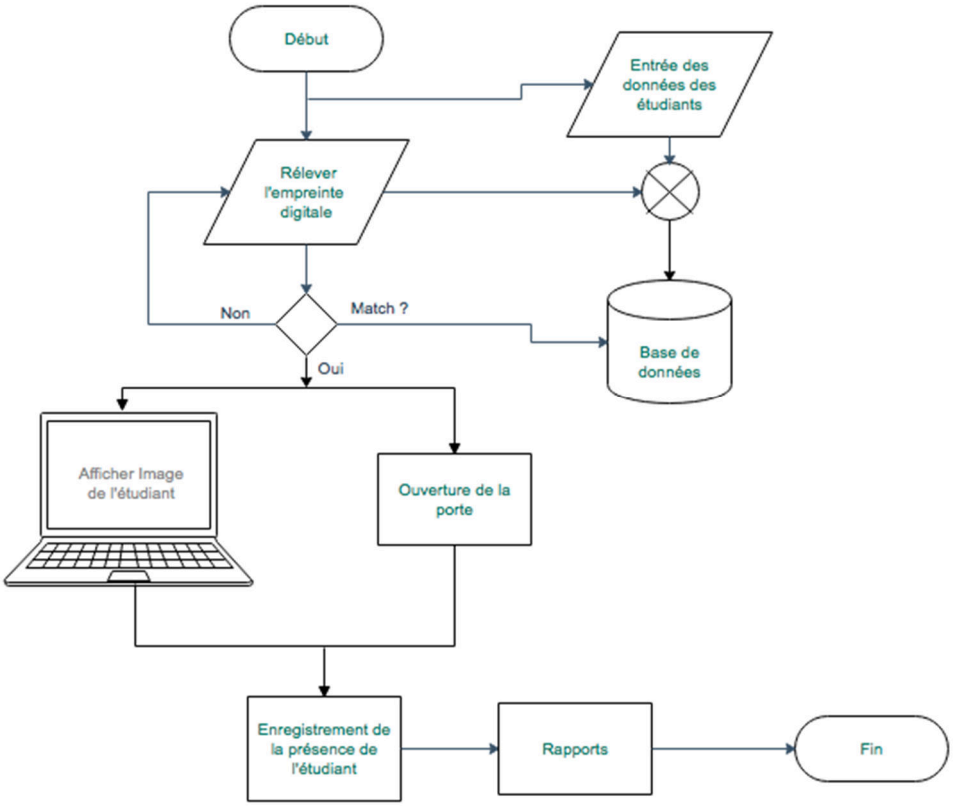


Fig. 5. Option2 : Organigramme du système avec technologie Fingerprint

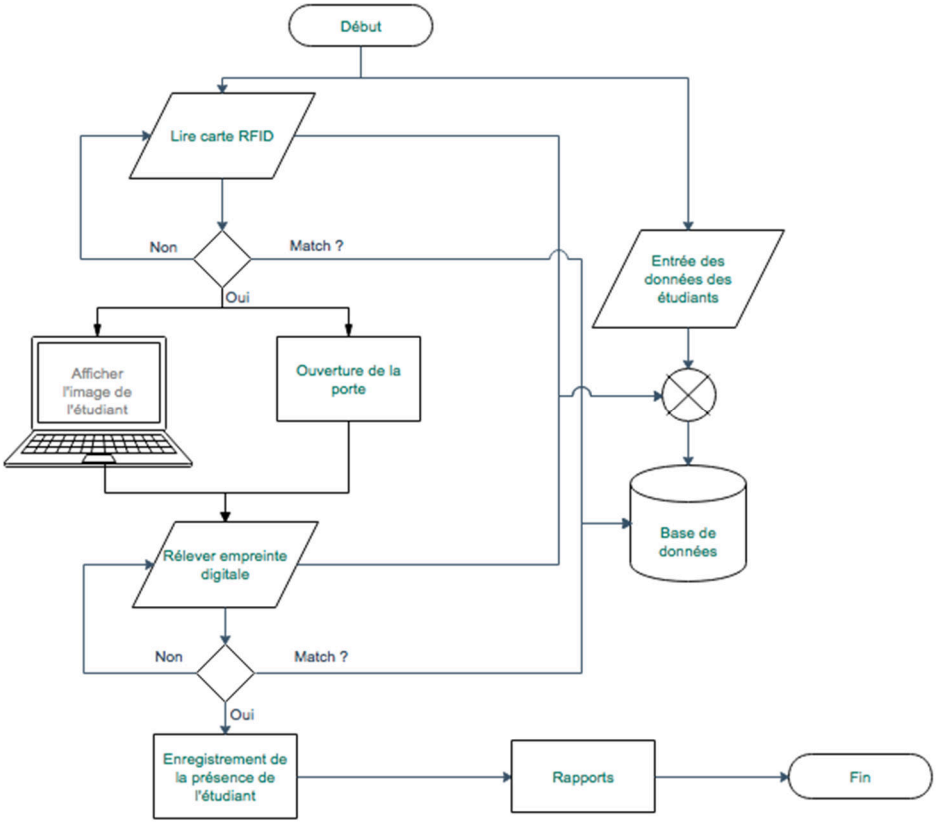


Fig. 6. Option3 : Organigramme du système avec Technologie hybride RFID-Fingerprint

Pour montrer comment les enchainements se succèdent et à quel moment les acteurs secondaires sont sollicités, voici le graphe représentant les séquences du système (Fig.7).

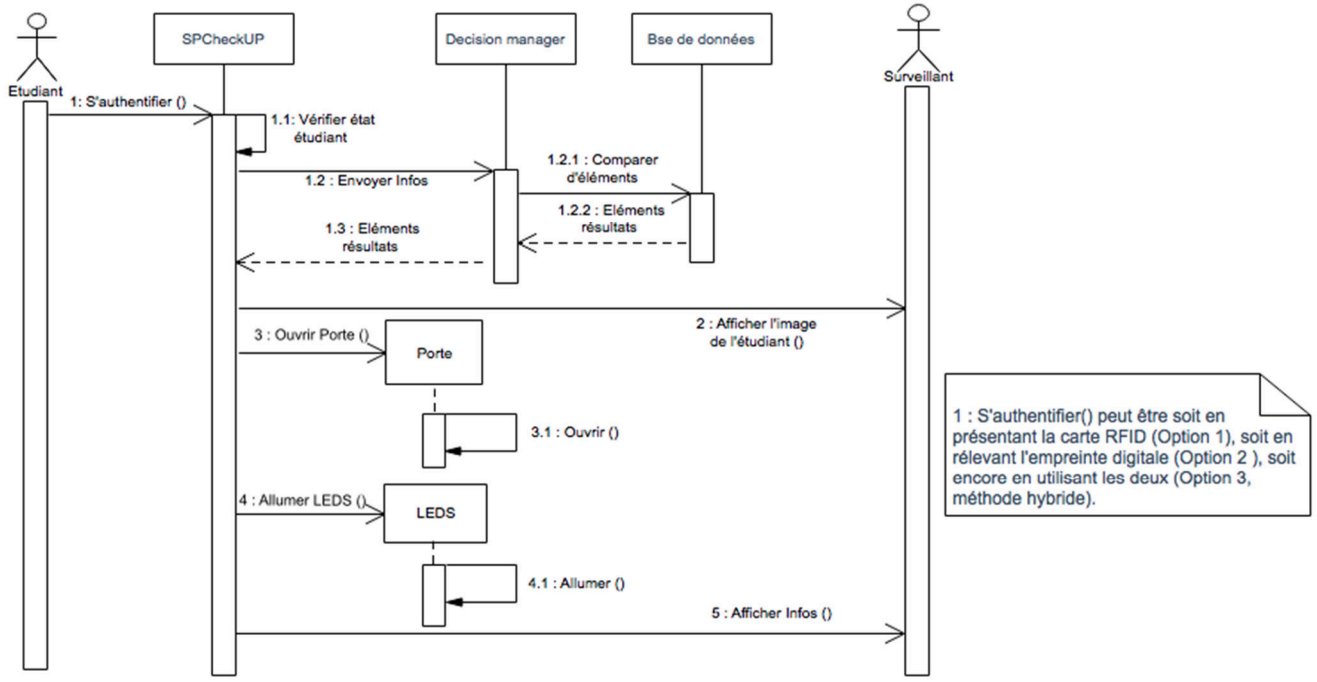


Fig. 7. Option3 : Organigramme du système avec Technologie hybride RFID-Fingerprint

2.5 IMPLÉMENTATION DU SYSTÈME

Pour mieux illustrer le système proposé sur le plan physique, nous listons ici les matériels dont nous avons besoin pour sa mise en place et nous présentons une maquette fonctionnelle représentant le système ici proposé :

- Une carte Arduino, dans notre cas une carte Arduino MEGA
- Un module RFID (lecteur et étiquettes)
- Un lecteur d'empreintes digitales permettant aux étudiants de s'identifier et d'enregistrer leur présence dans la salle d'examen et aussi de confirmer leur participation à l'épreuve du jour lors de la remise des copies d'examens
- Des tags / cartes RFID en forme des badges dont disposera chaque étudiant
- Un lecteur d'empreintes digitales (fingerprint)
- Un module (Shield) WIFI permettant la communication et le transfert de données via internet
- L'administration du système, facilitant la gestion des accès, les droits, la politique du système et l'organisation des données
- Un bloc de vérification de l'éligibilité de l'étudiant à l'examen avec 3 LEDs (Light Emitting Diodes), verte, jaune et rouge
- Un servomoteur pour ouvrir la porte d'une manière automatique
- Quelques fils de pontage

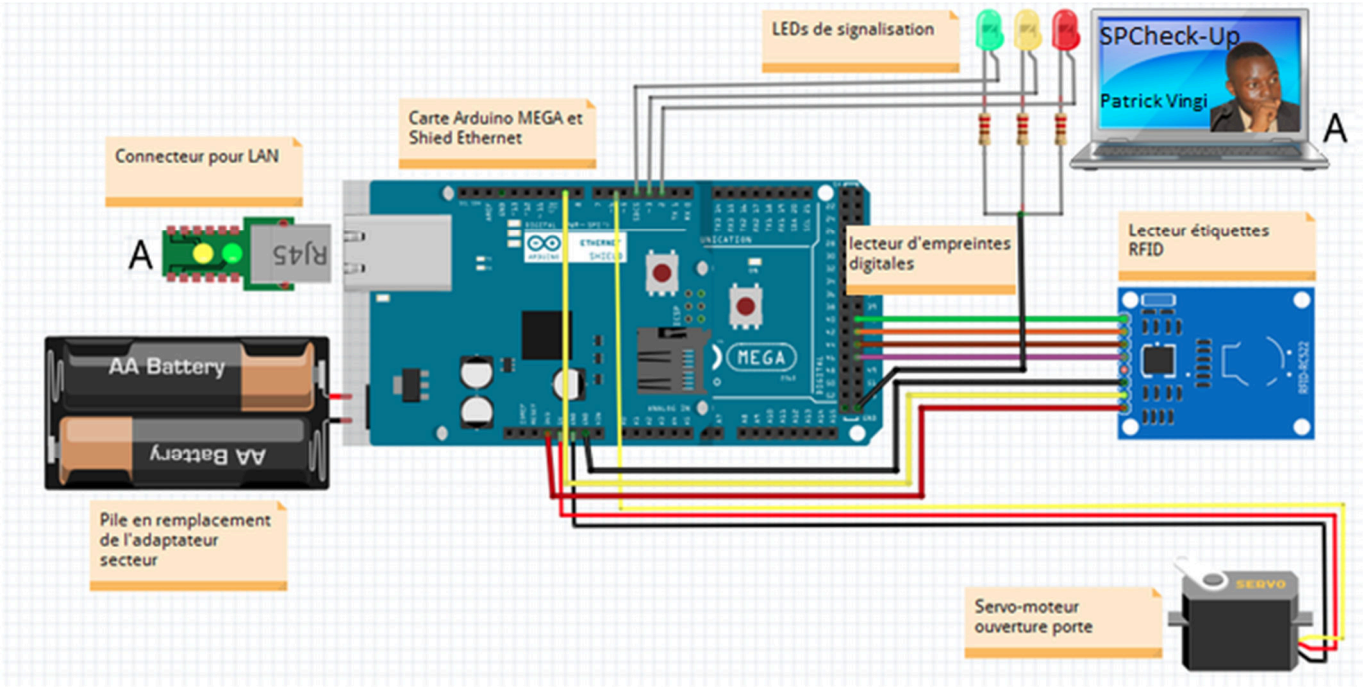


Fig. 8. Maquette fonctionnelle du système

3 RESULTAT

La phase d'inscription est une phase préalable et administrative dans laquelle l'administrateur doit s'authentifier pour accéder au système. L'empreinte digitale, code de badge RFID de l'étudiant ainsi que toutes ces autres données sont entrées pour la première fois dans la base de données en vue de l'enregistrement des présences des étudiants. Comme il a été susmentionné, notre système intègre une application web servant d'interface homme – machine permettant aux utilisateurs du système d'effectuer aisément différentes tâches. Les captures d'écran suivantes donnent un aperçu général de l'application web, partant de l'accueil au dépouillement des données. D'où la (Fig. 9), qui nous montre la page d'authentification.

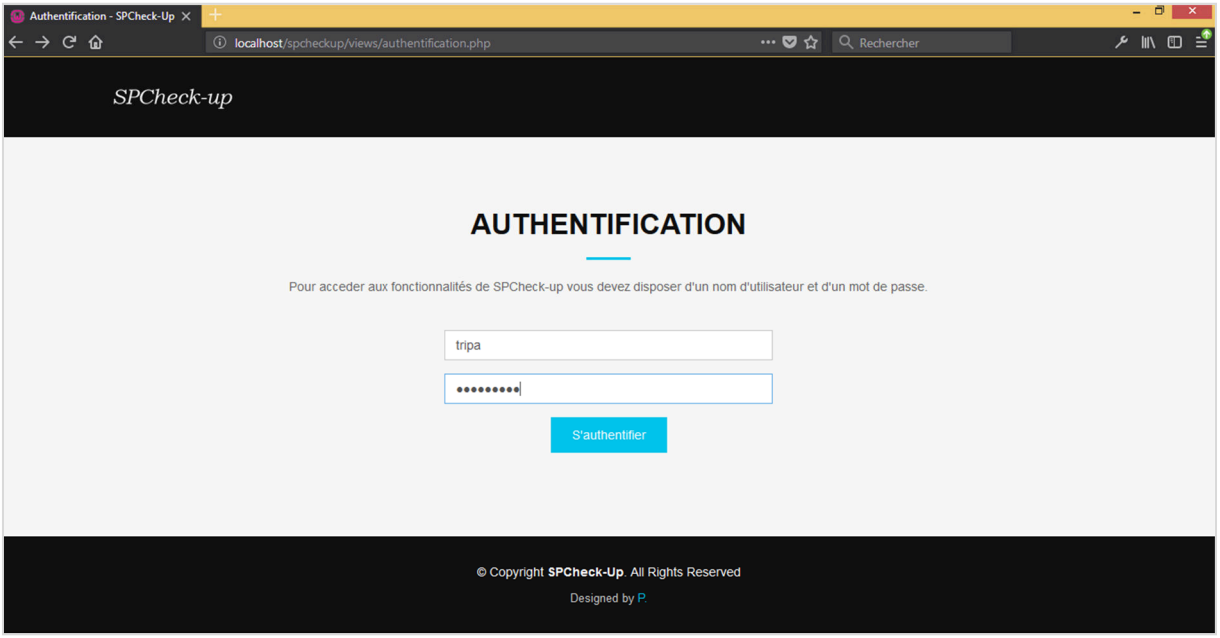
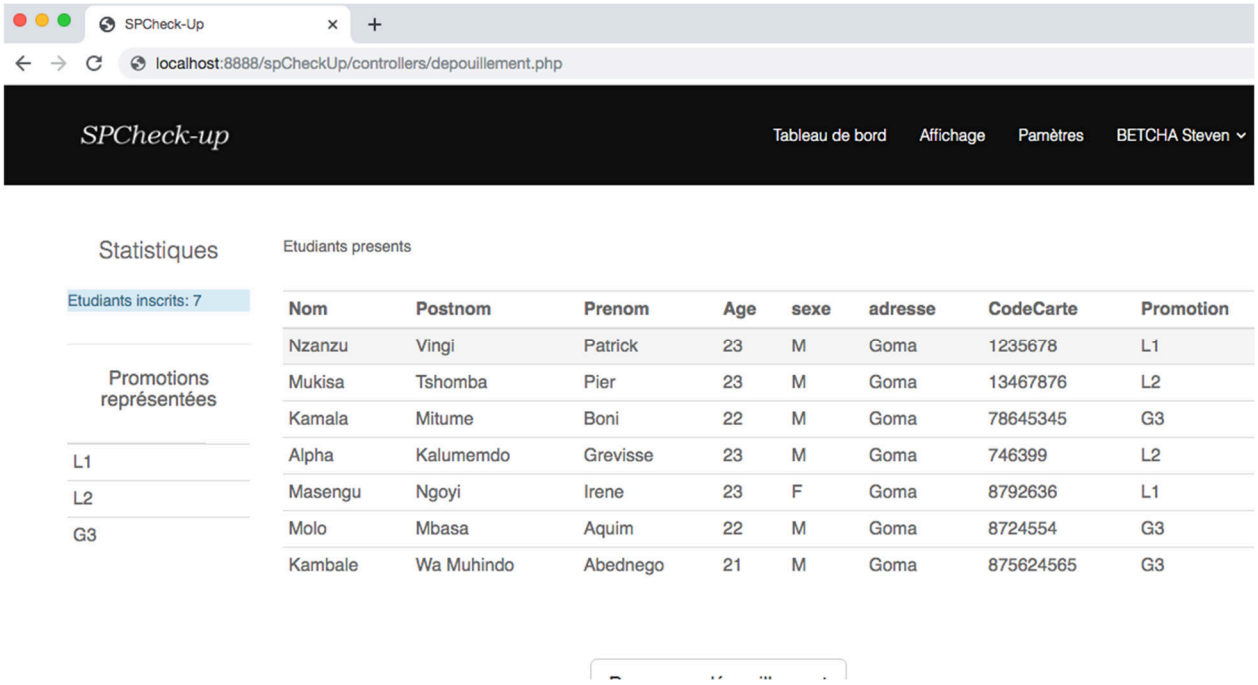


Fig. 9. Page d'authentification

Les étudiants étant préalablement inscrits et enregistrés dans le système, la correspondance (d'empreinte digitale / identification de rfid) de l'étudiant capturé est comparée aux modèles d'empreinte digitale ou code de badge sockés. La présence de l'étudiant est automatiquement enregistrée s'il y a correspondance, sinon, une alerte de cas suspect est émis par le système en affichant la lampe correspondante. La page du rapport des participants à l'examen est présentée avec la (Fig.10).



Nom	Postnom	Prenom	Age	sexe	adresse	CodeCarte	Promotion
Nzanzu	Vingi	Patrick	23	M	Goma	1235678	L1
Mukisa	Tshomba	Pier	23	M	Goma	13467876	L2
Kamala	Mitume	Boni	22	M	Goma	78645345	G3
Alpha	Kalumemdo	Grevisse	23	M	Goma	746399	L2
Masengu	Ngoyi	Irene	23	F	Goma	8792636	L1
Molo	Mbasa	Aquim	22	M	Goma	8724554	G3
Kambale	Wa Muhindo	Abednego	21	M	Goma	875624565	G3

Fig. 10. Page de dépouillement des participants à l'examen

Les résultats du test montrent que le système est efficace et à réponse rapide, le temps de latence est considérablement réduit. Il n'y avait aucune fausse identification des étudiants, peu de cas de faux rejet qui ont été acceptés plus tard et seuls les étudiants préinscrits ont été authentifiés.

4 DISCUSSION ET CONCLUSION

Le système a été testé à l'aide des données collectées auprès de 60 étudiants de la faculté des Sciences et Technologies Appliquées de l'Université Libre des Pays des Grands Lacs Goma en République Démocratique de Congo. Ils ont été subdivisés en 4 groupes de 15 étudiants chacun d'une manière aléatoire. Un groupe de contrôle qui accède à la salle d'examen d'une manière traditionnelle sans aide du système intelligent, et 3 groupes d'intervention qui utilisent le nouveau système selon les (Figs. 4,5,6). Dans ces 3 groupes d'intervention, un groupe pour tester la technologie avec RFID, un groupe pour tester la technologie fingerprint et un dernier groupe pour tester le système hybride rfid-fingerprint. La comparaison de ces 4 groupes est effectuée suivant deux critères majeures : le taux d'échec/réussite dans l'identification et aussi du temps déployé pour chaque étudiant.

- Taux de fausses correspondances : Il s'agit du pourcentage de fois où le système de contrôle de présence génère une fausse acceptation, ce qui se produit lorsqu'un individu est mal associé à un autre utilisateur. D'après les tests effectués avec le système, il n'y avait aucune fausse correspondance, l'accès n'étant pas accordé aux mauvais utilisateurs. (0% pour les 3 technologies), Tableau 1.
- Taux de faux positifs : Cela se produit lorsque le système le système de contrôle de présence trouve un résultat correspondant à un motif d'empreinte ou code badge qui n'a pas été enregistré dans le système.
- Taux de faux négatifs : Cela se produit lorsque le système de contrôle de présence ne trouve aucun résultat positif ou erroné pour un étudiant enregistré dans le système. Avec la technologie fingerprint, si le doigt n'est pas bien positionné sur le lecteur de fois des erreurs d'identification se produisaient, et cela induisait à 9% de taux de faux négatifs. Mais après le deuxième essaie l'identification réussissait.

Tableau 1. Comparaison taux d'échec/réussite dans l'identification des étudiants

	Option1 : RFID	Option1 : Fingerprint	Opption3 : RFID-Fingerprint
Taux de fausses correspondances	0%	0%	0%
Taux de faux positifs	0%	0%	0%
Taux de faux négatifs	0%	9% (0% après ajuster le doigt)	8% (0% après ajuster le doigt)

Concernant le temps déployé, le tableau 2, nous présente les résultats : la vérification et autorisation manuelle prend en moyenne 25 secondes par étudiant, en utilisant le RFID seul le temps d'exécution est réduit à environs 3 seconde. Pour la technologie avec empreinte digital, le temps d'exécution et de 6 secondes en moyenne, supérieur à rfid car le doigt doit être bien positionné sur le lecteur pour éviter les erreurs d'identifications, situation qui arrivait dans les 9 % des cas et menaient au deuxième essaie.

Tableau 1. Comparaison du temps d'exécution du système manuel et du système automatisé

Étudiants	Vérification et autorisation manuelles (secondes)	Vérification et autorisation automatisées avec RFID (secondes)	Vérification et autorisation automatisées avec Empreinte (sec)	Vérification et autorisation automatisées Hybride RRFID-Fingerprint (sec)
1	26	3	4	10
2	25	4	6	11
3	27	3	6	8
4	24	4	5	7
5	23	2	4	9
6	26	2	6	10
7	24	3	4	8
8	22	2	4	10
9	24	4	6	11
10	27	3	8	13
11	26	3	5	7
12	23	2	4	12
13	26	2	6	10
14	25	4	9	11
15	28	3	6	13
Moyenne	25	2,9	6	10,2

Comparativement à la prise de présence manuelle dans une salle d'examen, il ressort que le système ici proposé est de loin performant en raison du temps de réponse et la rapidité d'obtention des rapports. Approximativement, il faut en moyenne 3, 6 ou 10 secondes pour permettre à un étudiant d'accéder à la salle d'examen et d'enregistrer sa présence, alors que pour un système manuel, il faut en moyenne 25 secondes.

Le système vérifie l'éligibilité, autorise et enregistre automatiquement les présences aux examens. Le prototype est à mesure de capturer de nouvelles empreintes digitales, nouveaux code badges à stocker dans la base de données. La performance du système est donc acceptable et sa mise en œuvre intégrale serait envisagée, notamment en raison de la brièveté de son temps d'exécution et de la production de rapports. Tous ceux qui ont testé le système étaient satisfaits, ravis et intéressés par le produit développé pour une utilisation lors des examens à l'Université Libre des Pays des Grands Lacs Goma.

REFERENCES

[1] Kennedy O. Okokpujie, Etinosa Noma-Osaghae, et al., Design and Implementation of a Student Attendance System Using Iris Biometric Recogniton, 2017 International Conference on Computational Science and Computational Intelligence, 2017
[2] J.-M. Manach, La Vie Privee, un Probleme de Vieux Cons ?, Lile: FYP Éditions, 2010
[3] J. Elijah, A. Mishra, U. Gana, M. C. Udo et M. A. Abiodun, «Staff Monitoring System Using Biometric,» International Journal Of Engineering And Computer Science, vol. VI, n° %15, pp. 21448-21458, 5 May 2017
[4] G. COSTE, «controle-acces,» 27 Septembre 2018.
[En ligne]. Available: https://www.appvizer.fr/magazine/operations/securite/controle-acces. [Accès le 15 Novembre 2019].
[5] A. Aliyu, O. M. Olaniyi, J. K. Gana et C. Durugo, «A Multifactor Student Attendance Management System Using FingerprintBiometrics and RFID Techniques,» chez International Conference on Information and Communication Technology and Its Applications , Minna, 2016
[6] Institut Europeen pour le Developpement des Relations Sociales, «L'impact des nouvelles technologies sur la qualité de vie au travail,» Institut Europeen pour le Developpement des Relations Sociales, pp. 1-2, 23 Août 2018.
[7] D. Paret, RFID en ultra et super hautes fréquences : UHF-SHF - Théorie et mise en oeuvre, Paris: Dunod, 2008.
[8] Interfas, «ETIQUETTES ET TECHNOLOGIE RFID,» 26 Octobre 2018. [En ligne]. Available: https://www.interfas.fr/vos-applications/technologie-rfid/. [Accès le 16 Novembre 2019].
[9] High Tech Info, «Comment lire une puce RFID,» 21 Février 2018.
[En ligne]. Available: http://www.high-tech-info.fr/lire-puce-rfid. [Accès le 16 Novembre 2019].
[10] D. D. Santos, « Comprendre la rfid en 10 points » 29 Février 2016.
[En ligne]. Available: https://sbedirect.com/fr/blog/article/comprendre-la-rfid-en-10-points.html. [16 Novembre 2019].
[11] A. Liu, M. Shahzad, L. Xiulong et L. Keqiu , RFID Protocol Design, Optimization and Security for the Internet of Things, Londre: The Institution of Engineering and Technology, 2017
[12] S. Bleay, R. Croxton and M. de Puit, Fingerprint Development Techniques Theory and Application, Hoboken: John Wiley & Sons Ltd, 2018
[13] Biometrie-Online, «Biometrie-Online.Net,»
[En ligne]. Available: https://www.biometrie-online.net/technologies/empreintes-digitales. [Accès le 16 Novembre 2019].