République Algérienne Démocratique et Populaire
Université Abou Bakr Belkaid– Tlemcen
Faculté des Sciences
Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en Informatique

Option : *Réseau et Systèmes Distribués (R.S.D)*

Thème

Mesures de sécurité dans un système distribué destiné au vote automatique

Réalisé par :

- DAOUDI Ibrahim
- BOULENOUAR Bouchra

Présenté le 30 Juin 2020 devant le jury composé de MM.

- *Mme MALTI Djawida* *(Présidente)*
- *Mr. MATALLAH Houcine* *(Encadrant)*
- *Mr. SETTOUTI Ahmed Khalid Yassine* *(Examinateur)*

Année Universitaire: 2019-2020

بسم الله الرحمانِ الرحيم

Remerciements

Nous remercions tout d'abord Dieu qui, avec sa permission, on a pu réussi ce travail, Et notre encadreur Mr. MATALLAH Houcine pour son aide si précieuse tout au long de la préparation de notre projet de fin d'études. Nous tenons à remercier aussi nos familles, nos amis, nos collègues et toutes personnes ayant contribué de près ou de loin à la réussite de notre projet.

Nous tenons aussi à remercier Mme MALTI Djawida et Mr SETTOUTI Ahmed Khalid Yassine d'avoir nous honorés de leur présence et d'être les membres de jury de notre travail.

Dédicaces

Je dédie ce travail en premier lieu à mes chers parents sans qui je n'aurai jamais pu être là.

Ainsi à tous mes professeurs qui ont fait leur travail durant mon cursus en informatique dans la faculté des sciences à Tlemcen.

À ma collègue Boulenouar Bouchra .

À ma famille qui m'a toujours aidé et soutenu tout au long de mes études.

À tout le peuple Algérien qui a participé au mouvement du HIRAK (22 février 2019).

DAOUDI Ibrahim

Dédicaces

Je dédie ce travail à mes parents, mes estimés pour eux sont immenses, je vous remercie pour tout ce que vous avez fait pour moi. Que dieu vous préserve une longue vie heureuse.

A mes très chères sœurs Amina et Hadjer et très chère frère Mohammed Islem à qui je souhaite une vie pleine de bonheur, de prospérité et de réussite. A mon binôme Ibrahim.

A tous mes amis : Mohammed Yacine, Samira, Amine, Chaimaa et Amira . Je vous dédie ce travail et vous souhaite un avenir à la hauteur de vos ambitions. Que notre amitié dure

A Toute ma famille, Tous ceux que j'aime, qui m'aiment et me combler de conseils A tous ceux qui un jour ont pensé à moi

Les plus beaux mots ne sauraient exprimer ma redevance

Boulenouar Bouchra

ملخص

تكلف الانتخابات ذات نطاق واسع للدول ميزانية كبيرة، بالإضافة إلى أنها يمكن أن تكون محطة شك بشأن الشفافية للمرشحين غير الناجحين. ولهذا فان مشروعنا يعمل على تحقيق تطبيق يقوم بمعلوماتية التصويت يتركز على خوارزميات أمنية تعمل بمبدأ التحقق من المصدر بنسبة خطئ سلبي ضئيلة جدا لضمان شفافية الانتخابات. كما يحوي البرنامج على أنظمة ترصد عالية الدقة تقوم بتحديد هوية المهاجم في حين تم الهجوم في ظروف سير الانتخابات.يتيح هدا البرنامج الانتخاب في مراكز اقتراع تحوي حواسيب مجهزة بقارئات بصمات الأصابع وإظهار النتائج والقيام بالإحصاء عنها.

الكلمات المفتاحية :

النزاهة ، التتبع ، المصادقة ، الأمان ،البيومتري ، التشفير ، الانتخابات ، إخفاء الهوية

Résumé

Les élections à grande échelle coûtent aux pays un budget important et elles peuvent mettre en doute la transparence pour les candidats non élus. Par conséquent, notre projet vise à réaliser une application qui automatise le vote, en se concentrant sur des algorithmes de sécurité qui fonctionnent avec le principe de vérification de la source, à très faible taux d'erreur (négatif) pour assurer la transparence des élections. Également, le programme contient des systèmes de surveillance, à grande précision, et qui identifient l'attaquant au cours des élections. Ce programme permet l'élection dans les bureaux de vote qui contiennent des ordinateurs équipés de lecteurs d'empreintes digitales et affiche les résultats, en réalisant des statistiques à leur sujet.

Mot clés :

Intégrité, Traçabilité, Authentification, Sécurité, Biométrie, Cryptographie, Election, Anonymat

Abstract

Large-scale elections cost countries a large budget plus they can be doubting point of transparency for unsuccessful candidates. Therefore, we realized an application that informs voting focusing on security algorithms that work with the principle of verifying the source with a very small negative error rate to ensure the transparency of the elections. The program also contains high-definition surveillance systems that identify the attacker while the attack took place during the elections. This program allows for election in polling centers that contain computers equipped with fingerprint readers, show results, and perform statistics on them.

Keywords:

Integrity, Traceability, Authentication, Security, Biometrics, Cryptography, Election, Anonymity

Sommaire

Introduction générale

Tous les pays du monde en général et l'Algérie en particulier, dépensent de très grands budgets pour les élections à l'échelle nationale (APN, Présidentielle) et même pour les élections à l'échelle locale (APW, APC). De plus, les élections qui sont faîtes d'une manière classique, peuvent être suspendues par des obstacles et contraintes imprévues comme par exemple le cas du COVID-19. D'un autre côté, la transparence des élections a été revendiquée à plusieurs reprises par plusieurs parties et principalement par le mouvement populaire Algérien (HIRAK du 22 Février 2019) qui rêvait de l'établissement d'un état de droit avec une vraie démocratie concrétisée par l'organisation des élections transparentes. Dans cette optique, on propose comme étant des informaticiens un ensemble d'outils et techniques qui permettent de faciliter les tâches socioprofessionnelles pour fournir des résultats fiables et crédibles et en particulier les élections de tout genre. Notre PFE a pour but de concevoir et développer un système complètement autonome sous le nom technique VAO (Vote Assisté par Ordinateur), afin d'effectuer un vote automatique en minimisant toute intervention humaine pour une sécurité maximale. Notre travail vise un certain nombre d'objectifs comme :

- Minimisation du nombre des bulletins nuls en conservant seulement les enveloppes blanches

- Permet au citoyen de voter dans le centre le plus proche, sans déplacements.

- Minimisation des charges du personnel et économisation de toute la logistique mise en place pour assurer les élections.

- Gain du temps considérable pour dévoiler les résultats.

- Garantie de la transparence des élections.

Notre mémoire contient deux chapitres qui définissent les méthodes de défenses employées dans notre projet de fin d'étude qui sont (Biométrie, Mesures de sécurité employées). Le chapitre conception récapitule l'analyse des besoins ainsi que l'architecture fonctionnelle de notre application. Le dernier chapitre, définit et décrit le système développé.

I) CHAPITRE 1 : Système d'authentification

I.1) Introduction

Dans ce chapitre on met en œuvre un système d'authentification pour les bureaux de vote basé sur la **biométrie** afin d'assurer la transparence des résultats finaux.

I.2) Définition de la biométrie

La biométrie regroupe l'ensemble des techniques informatiques visant à reconnaitre automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales, etc.). Elles se rapprochent ainsi de ce qui pourrait être défini comme un identificateur unique universel, permettant, de fait, le traçage des individus [2].

I.3) Domaines d'application de la biométrie

Ce sont des projets informatiques qui nécessitent un grand niveau de sécurité en authentification comme par-exemple (e-Bank, vote électronique, e-Cryptographie, e-commerce, transactions bit coin etc.). En Algérie on peut trouver la biométrie dans les domaines suivants :

- *Sécurité biométrique :*

Comme la connectivité continue à tendance à se répandre dans le monde entier, il est clair que les anciennes méthodes de sécurité ne sont tout simplement pas assez fortes pour protéger ce qui est le plus important. Heureusement, la technologie biométrique est plus accessible que jamais auparavant, prête à apporter une sécurité améliorée et une plus grande commodité à tout ce qu'il faut protéger [3].

- *Contrôle frontalier / Aéroports :*

Contrôle des frontières par identification biométrique dans les aéroports est un domaine clé d'application pour la technologie biométrique. Quiconque voyage par avion peut vous dire des points de contrôle de sécurité que les passages frontaliers sont certains des endroits les plus frustrants à devoir traverser. Heureusement, la technologie biométrique aide à automatiser le processus [3].

- *Biométrie résidentielle :*

Les innovations récentes en matière de mobilité et de connectivité ont créé une demande de biométrie dans les foyers et les poches des consommateurs. Les smart-phones avec capteurs d'empreintes digitales, les applications qui permettent la reconnaissance faciale et vocale, les portefeuilles mobiles : ce sont les moyens de plus en plus populaires que les consommateurs du monde entier trouvent en biométrie dans leur vie [3].

- *Biométrie financière :*

Parmi les applications les plus populaires et les plus répandues de la technologie biométrique. L'identification financière, la vérification et l'authentification dans le commerce contribuent à rendre les opérations bancaires, les achats et la gestion des comptes plus sûrs, pratiques et responsables [3].

- *Empreintes digitales et verrous biométriques :*

Verrouillage biométrique à empreintes digitales : Si vous avez quelque chose à protéger, pourquoi ne pas opter pour une solution biométrique de contrôle d'accès Physique. Celle-ci est une méthode d'authentification plus robuste que les clés, les cartes-clés et les NIP pour une raison simple : elle est ce que vous êtes, pas ce que vous avez [3].

- *Biométrie de la santé :*

La biométrie offre non seulement une sécurité et une commodité partout où elle est déployée, mais dans certains cas elle apporte une organisation accrue. Dans le domaine de la santé, cela est particulièrement vrai. Les dossiers de santé sont quelques-uns des documents personnels les plus précieux, et les médecins ont besoin d'y accéder rapidement [3].

- *Justice :*

La technologie biométrique et la justice ont une histoire très longue, et de nombreuses innovations très importantes en matière de gestion d'identité ont suscité cette relation bénéfique. Aujourd'hui, la biométrie légale est vraiment multimodale ; l'empreinte digitale, la reconnaissance faciale et la reconnaissance vocale jouent tous un rôle crucial dans l'amélioration de la sécurité publique et l'identification des personnes recherchées [3].

- *Contrôle d'accès logique :*

Le contrôle d'accès logique est un domaine d'application majeur pour la technologie biométrique. Lorsque nous disons : « Il est temps de tuer le mot de passe », c'est la technologie dont nous parlons. Qu'il s'agisse de sécuriser les applications sur votre smart phone, d'accéder à un email de travail ou de permettre une politique BYOD efficace [3].

- *Biométrie mobile :*

Les solutions de biométrie mobile vivent à l'intersection de la connectivité et de l'identité. Elles intègrent soit une ou plusieurs modalités biométriques à des fins d'authentification ou d'identification, et profitent de la portabilité des smart-phones, des tablettes, et d'autres types d'ordinateurs de poche [3].

- *Temps et pointage :*

Des solutions biométriques pour la gestion du temps existent pour suivre les mouvements du personnel, avoir un rapport précis sur les heures de travail de chacun, et optimiser le rendement des ressources humaines. Et ce en installant une pointeuse biométrique Au niveau des entités, sociétés, entreprises et autres organismes [3].

I.4) Système d'authentification dans VAO

La biométrie joue le rôle d'un identificateur pour les votants dans le système qui gère le vote avec présence d'un lecteur d'empreinte digitale. Un votant effectue son vote seulement après avoir introduit sa propre empreinte qui sera validée par la vérification automatique de cette dernière en étant une empreinte d'un citoyen intégré dans la liste électorale.

I.5) Objectifs de Biométrie dans le vote électronique

La biométrie est introduite dans le vote électronique pour réaliser les buts cités ci-dessous :

- Garantir que chaque opération d'ajouter un vote dans la base de données implique toujours la présence physique d'un citoyen enregistré dans la liste électorale (toute personne ayant une carte de vote pouvant participer). C'est-à-dire toute utilisation de la machine de vote par le bureau à distance ne peut aboutir (la présence physique est obligatoire), de ce fait un pirate aura des difficultés pour altérer les résultats finaux.

- Interdire la possibilité de votes virtuels car ces derniers ne possédant pas une empreinte pour pouvoir être validés.

I.6) Conclusion

Le Contrôle de vote par le lecteur d'empreinte digitale nous garantit un bon niveau de sécurité en authentification. Mais il existe toujours des failles qui guide l'attaquant à utiliser les programmes du système sans passer par la procédure d'authentification. Dans le schéma ci-dessous, un pirate peut effectuer un vote en se connectant directement à l'environnement VAO sans passer par l'interface graphique du système :

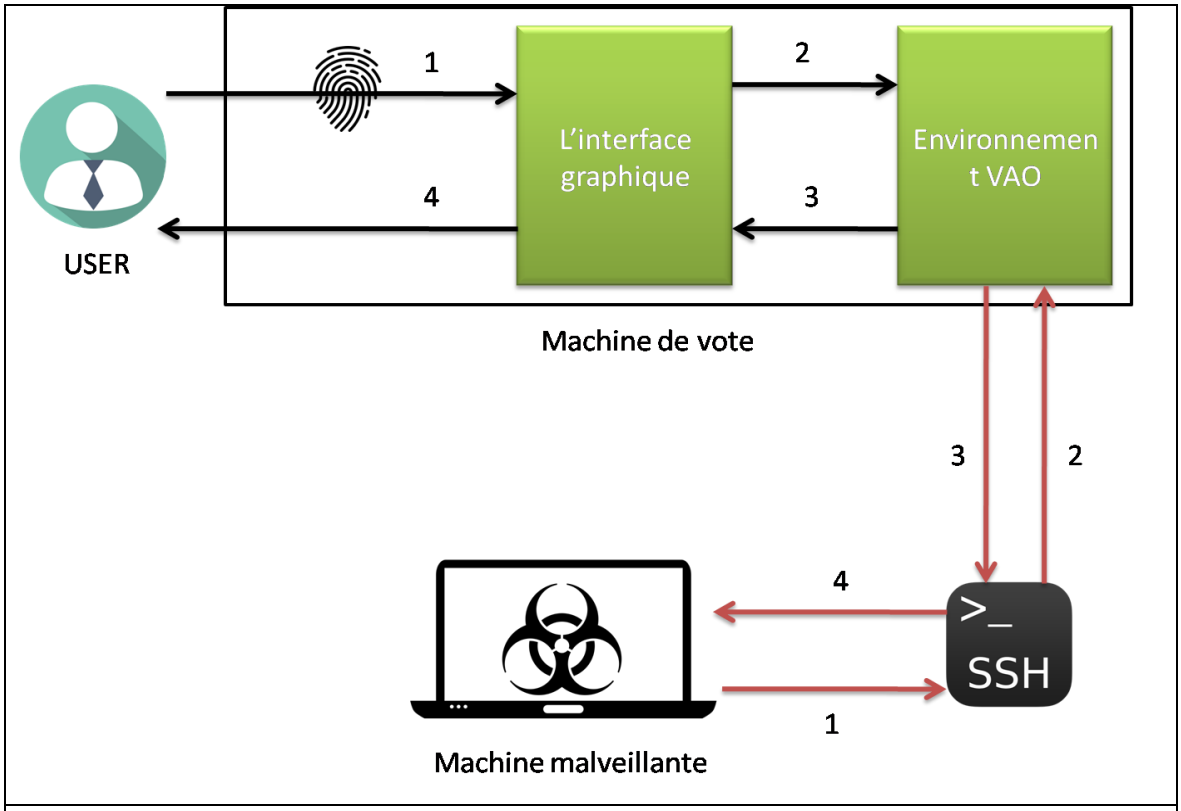


Figure 1.1 : Attaque de déviation de la pointeuse digitale

De plus, avec la création d'imprimante 3D, un pirate peut créer une fausse empreinte digitale d'un votant pour s'identifier d'une manière malveillante.

Pour cela, On développe d'autres techniques de sécurité pour neutraliser ces types d'attaques.

II) CHAPITRE 2 : Mesures de sécurité

II.1) Introduction

L'objectif ciblé dans ce chapitre, est la substitution de l'humain par l'environnement VAO qui exige la validation par la pointeuse digitale. Pour cela, on met en œuvre des politiques de sécurité dans quatre niveaux essentiels qui peuvent être des portes pour les attaquants qui sont : Web, Réseau, Système d'exploitation et Base de données.

II.2) Mesures de sécurité existantes

- Antivirus [13].
- Sauvegarde [13].
- Contrôle des sauvegardes (reprise, redémarrage) [13].
- PROXY + Logiciel administration réseau [13].
- Mots de passe par poste informatique [13].
- Système d'authentification / identification informatique [13].
- Firewall (Parefeu) + Routeur filtrant [13].
- VPN (Réseau privé virtuel) [13].
- Cryptage / chiffrement de données [13].
- Plan de sécurité du SI (connexions, modem, …) [13].
- Maintenance (matériel, clim, électrique, accès, …) [13].
- Administration base de données (modification, accès, …) [13].
- Test de sécurité (envoi de données parasites, …) [13].

II.3) Système de cryptographie

Afin de garder la confidentialité et l'intégrité des données, on s'appuie d'avantage sur la cryptographie

- Le système utilise le cryptogramme AES-256 Le cryptogramme le plus résistant à la cryptanalyse dans le monde jusqu'à ce jour. « L'AES n'a pour l'instant pas été cassé, même théoriquement, au sens où il n'existe pas d'attaque significativement plus efficace que la recherche exhaustive quand le chiffrement est correctement utilisé [11]. »

- Le cryptogramme repose sur un type de clé invisible qui n'est jamais utilisé précédemment (Les autres cryptogrammes utilisés reposent sur la clé symétrique ou asymétrique).
- La technique de cryptographie à clé invisible consiste à créer un cryptogramme qui prend en entré le message, et de sortir le chiffré ou l'inverse **si vous avez la permission d'utilisation** sinon il retourne FALSE.
- La Clé de chiffrement est déclarée dans le code source qui est généré automatiquement avant qu'il va être supprimé après la compilation en code binaire illisible.
- Le cryptogramme retourne un résultat si les conditions suivantes sont satisfaites :
  - Le programme est propriétaire d'une seule machine réelle dans le monde. Par rapport aux machines virtuelles Il ne fonctionne plus à cause de la possibilité qu'un attaquant arrive à modifier UUID par celle de la machine propriétaire de ce dernier programme.
  - Il retourne le résultat d'opération (Cryptage / Décryptage) si cette opération est parmi les opérations incluses dans l'algorithme du logiciel VAO.

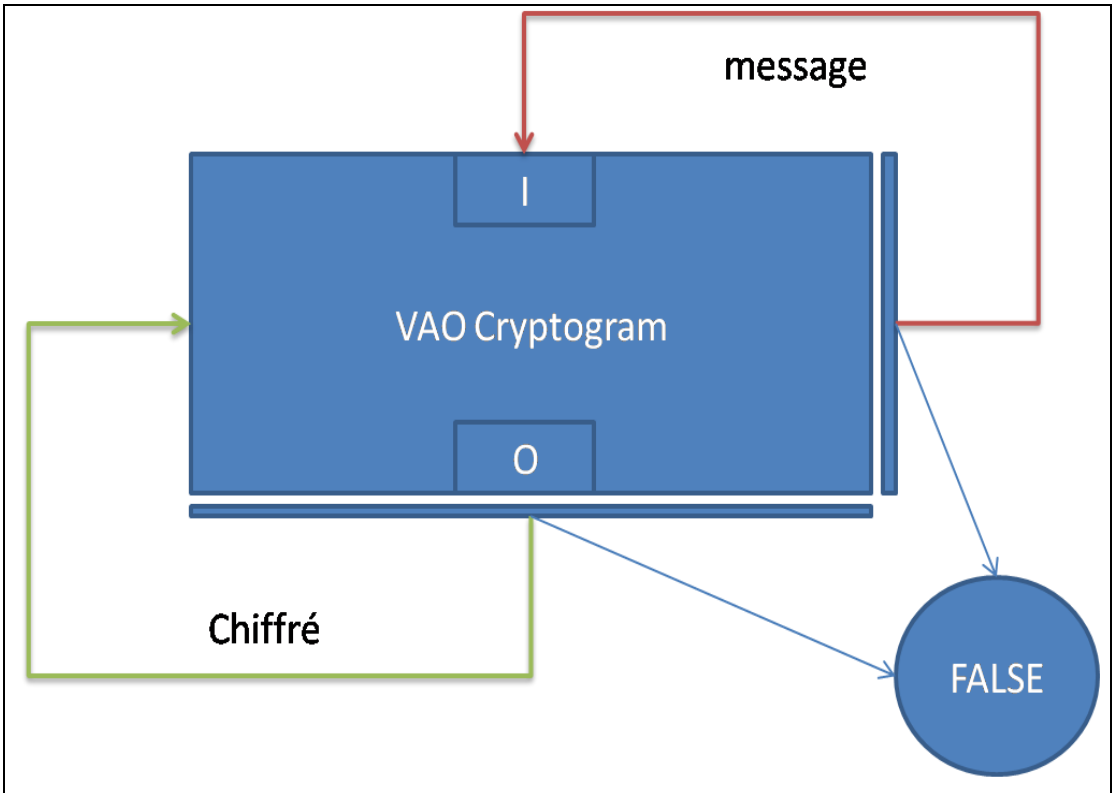


Figure 3.1 : Diagramme d'opération de chiffrement et déchiffrement dans VAO

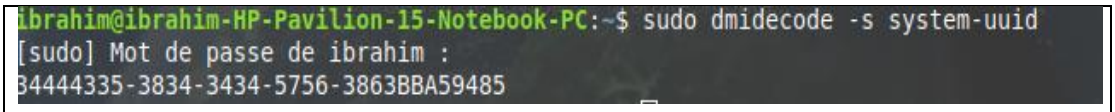


Figure 3.2 : Lire le UUID d'une machine sous Linux

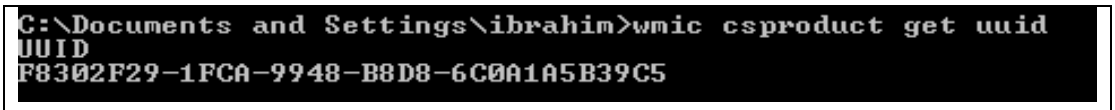


Figure 3.3 : Lire le UUID d'une machine sous Windows

II.4) Au niveau BDD

Dans ce sous-chapitre on définit les attaques possibles qui visent le SGBD (Système de Gestion de Base de Données) de l'application afin de fausser les résultats finaux, ainsi que les mécanismes de sécurité utilisés au niveau SGBD pour neutraliser ces attaques.

La sécurité de la base de données commence par une réflexion sur les usages et la population d'utilisateurs accédant à celle-ci, ainsi que sur la manière dont la connexion s'effectue [5].

Le tableau ci-dessous contient le schéma relationnel de la base des données :

Table	***Propriétaire***	***Les attributs***				***Les déclencheurs***
Election	*SYSTEM*	***Name***	***Type***	***Default value***	***Description***	
		Titre	*Vachar(30)*	*Not null*	*Primary key*	
		Description	*Varchar(50)*	*Not null*	*Brève description*	
		Min-Sign	*Number*	*0*	*Le nombre minimal légal assemblé par un candidat*	
		Type	*Enum*	*(Humaine, Subjective)*	*Humaine : un vote pour un humain* *Subjective : un vote sur une loi par exemple*	
Candidat		***Name***	***Type***	***Default value***	***Description***	
		Nom	*Vachar(30)*	*Not null*	*Primary key*	
		Description	*Varchar(50)*	*Not null*	*Brève description sur le programme*	

		Nb_Voix	*Number*	*0*	*Nombre des voix assemblé*	
		Election	*Vachar(30)*	*Not null*	*Foreign key references Election (Titre)*	
		Compte	*Vachar(30)*	*Not null*	*Foreign key references Compte(Code).*	
Time table		***Name***	***Type***	***Default value***	***Description***	
		Sign-start	*Date*	*Date-système*	*La date et l'heure de début de la phase compagne électorale.*	
		Sign-End		*Date-système+15jours*	*La date et l'heure de fin de la phase compagne électorale.*	
		Election-start		*Date-système+20jours*	*La date et l'heure de début de la phase élection.*	
		Election-duration	*Time*	*Une heure*	*Le délai de la phase élection.*	
		Election	*Vachar(30)*	*Not null*	*Foreign key references Election(Titre)*	
Vidéo		***Name***	***Type***	***Default value***	***Description***	
		Titre	*Vachar(30)*	*Not null*	*Titre pour le vidéo*	
		Source	*Vachar(30)*	*Not null*	*Primary key*	
		Nb-Sign	*Number*	*0*	*Le nombre des signatures assemblé par un candidat par ce vidéo*	

		Candidat	*Vachar(30)*	*Not null*	*Foreign key reference Candidat(Nom)*	
Vote	*VOTANT*	***Name***	***Type***	***Default value***	***Description***	*Au moment d'insertion dans la table vote, le déclencheur incrémente le nombre des voix pour le candidat concerné par le vote.* *Dans le cas de suppression le déclencheur fait la décrémentation.* *Chaque votant peut voter une seule fois s'il vote pour la deuxième fois, le vote précédent va être annulé.*
		Compte	*Vachar(30)*	*Not null*	*Le code de compte d'utilisateur qui effectue le vote au candidat* *Foreign key references Compte(Code)*	
		Candidat		*Not null*	*Le nom de candidat concerné par le vote* *Foreign key references Candidat(Nom)*	
Doute	*POLICE*	***Name***	***Type***	***Default value***	***Description***	*Si quelqu'un arrive à utiliser une carte douteuse pour voter, alors son vote va être annulé.*
		RFID	*Vachar(30)*	*Not null*	*Le RFID de la carte perdue*	
Compte	*SYSTEM*	***Name***	***Type***	***Default value***	***Description***	
		Code	*Vachar(30)*	*Not null*	*Primary key*	
		Login	*Vachar(30)*	*Null*		
		Password	*Vachar(30)*	*Null*		
		Rôle	*Enum*	*Contient tous les rôles*		

				d'application)		
		State	*Enum*	*(voted, not voted, not assigned)*	*Voted : l'utilisateur de compte est déjà voté* *Not voted : le compte est nouveau* *Not assigned : le compte n'a pas encore effectué à un utilisateur*	
		RFID	*Vachar(30)*	*Null*	*Numéro de la carte RFID*	
		FPID	*Vachar(30)*	*Null*	*Hach d'empreinte utilisateur*	

II.4.A)Utilisateurs et Privilèges

Pour garantir un bon niveau de sécurité qui empêche un pirate à modifier les données dans la table candidat et la table vote, on définit les utilisateurs et ces privilèges suivants dans la base de données :

- *Présidence :*

Afficher la table candidat et manipulation total des tables Election, TimeTable, Candidat dans la phase pré campagne.

- *Votant :*

Ajouter dans la table Vote après affection d'un Rôle dont leur nom reste un secret d'entreprise IE (sont des décisions prises par un ordinateur et appliqués par toutes les machines dans le réseau sans d'être connu par un humain). Pour éviter qu'un utilisateur malveillant profite de récupérer le nom du rôle qui permet d'ajouter dans la table vote, alors il peut créer un script qui ajoute des milliers des voix automatiquement pour un candidat précis.

- *Police :*

Ajouter et supprimer une carte dans la table Doute, Quand un votant perd sa carte de vote biométrique, il réclame la perte chez la POLICE afin de l'ajouter dans la table doute. Pour que si le voleur vote avec cette carte, le système capte qu'elle est douteuse et annule le vote effectué.

- *Journaliste :*

Ajoute une vidéo de conférence pour un candidat, il admet un mot de passe parmi les secrets d'entreprise IE, pour garder la cohérence de la table vidéo. Si cet utilisateur n'admet pas un mot de passe protégé, un pirate peut accéder à la BDD puis ajouter pour un candidat une vidéo qui n'a aucune relation avec ce dernier.

Les bases de données du système sont installées au niveau des serveurs de bureaux de vote, le programme suit les étapes suivantes chronologiquement :

1. Création des tables de la base de données.
2. Création d'un trigger système qui permet de modifier les nombres de voix des candidats au moment d'insertion dans la table vote.
   Ainsi que pour la suppression et la modification (utilisateur VOTANT admet seulement les privilèges d'ajouter dans la table vote).
3. Attribuer les privilèges aux utilisateurs de la base de données.
4. Créer un profile qui permet à chaque utilisateur de faire une seule tentative de connexion, avant que le compte soit verrouillé pendant un demi-jour.
5. Affecter ce profile à tous les utilisateurs de la base de données afin d'annuler tous les essais d'analyse pour deviner les mots de passe.
6. Retirer les privilèges de connexion au compte système (REVOKE CONNECT FROM SYSTEM) afin de limiter les droits sur la base des données à tout le monde.

Avec ces mesures de sécurité, un pirate va trouver des difficultés pour modifier les données.

II.5) Au niveau système d'exploitation

On définit les mesures de sécurité dans le système d'exploitation d'une machine du réseau, si un pirate arrive à utiliser cette dernière par un Shell à distance.

Pour cela on rend le super utilisateur dans ces machines comme les autres, c'est-à-dire limiter les droits d'utiliser l'ordinateur dans un délai défini (dans notre cas c'est le délai de vote).

II.5.A)Protocole SISP

II.5.A.a) Définition

SISP (Super Information Security Protocol) est un protocole de sécurité informatique en contrôle d'accès, utilise des techniques de traçage de eBPF, pour fonder des systèmes de filtrage des requêtes dans les programmes sensibles dans un logiciel, l'objectif de ce protocole c'est d'annuler toute technique d'utilisation de logiciel VAO ailleurs d'un script web.

II.5.A.b) Les composants

Les composants nécessaires pour réaliser le protocole SISP sont cités dans la liste suivante :

- Le traceur eBPF.
- *Le serveur de trace.*

C'est un serveur Java TCP multi thread écoute sur le port 1010, Il contient 3 threads qui répondent aux requêtes suivantes revenantes de localhost (127.0.0.1) :

- Path of [PID] : retourne l'emplacement du processus dans leur id = PID dans l'ordinateur.
- Args of [PID] : retourne comment la commande qui lance le processus dans leur id = PID elle est écrite. Si la commande peut être exécutée (permission du vao OK) sinon envoyé 0.
- Trace of [PID] : envoie la trace des appels jusqu'à le processus en question (le client).
- EXIT : arrête le serveur d'une manière légal, concernant la manière illégale c'est toute une requête EXIT qui n'arrive pas de l'horloge du VAO, alors le serveur envoie au client un message d'erreur ou l'arrêter à travers la commande KILL.

II.5.A.c) Les threads du serveur de trace :

Le serveur de trace est composé de trois threads dont leur rôle est de garantir la traçabilité du SHELL afin d'assurer un bon niveau de sécurité en contrôle d'accès. On peut citer ces threads ci-dessous :

- *SnooperEXEC*

Trace tous les appels systèmes effectué dans l'ordinateur, sauf qu'il occupe d'un travail d'un root-kit qui doit respecter les lois suivantes :

- Ne pas afficher le message en clair dans un appel système pour le cryptage.
- Ne pas afficher la trame dans un appel système pour le masquage ou le démasquage.

- *Snooper OPEN*

Liste les appels des scripts à tout moment, par exemple quand on lance un script PHP à travers le navigateur, ce thread capte l'action en même temps.

- *Anti-virus*

Occupe d'interruption de tous les appels systèmes illégaux exécutés par un humain qui sont les suivants :

- Toute commande KILL pour interruption du serveur de trace ou n'importe quel programme de logiciel va être automatiquement annulée.
- Interdiction totale des installations des paquets durant l'opération de vote.
- Une interdiction de téléchargement des paquets sauf l'environnement VAO qui arrive du serveur El-Mouradia. (C'est la racine qui occupe d'organiser le réseau d'une manière automatique).
- Interdiction de modification d'arborescence dans le dossier de logiciel. (Ajouter ou supprimer ou renommer ou modifier les positions des fichiers et les dossiers).
- Impossible d'éditer les fichiers de logiciel avec CAT, ECHO et les éditeurs du texte.
- Interdiction de tous les appels système dangereux.
- Monopolisation de tous les traceurs eBPF au serveur de trace seulement.
- Pas d'arrêt d'ordinateur durant l'opération de vote.
- Interruption de toute compilation ailleurs de fonctionnement automatique du système.
- Interruption de toute commande qui renvoie le pid du serveur de trace qui sont PGREP JAVA ou PWDX [RANDOM] ou PS –a [RANDOM].

II.5.A.d) Les limites du thread anti-virus

Ce processus ne peut pas réaliser une bonne manière de défense, car il réagit seulement avec les commandes à réaction lourde, ou les commandes à grande durée de vie, le problème se pose sur les commandes rapides qui sont incontrôlable par ce processus de défense.

- *Les commandes à réaction lourde*

Sont des commandes qui prennent un délai pour être exécuté comme les traceurs d'eBPF.

- *Les commandes à grande durée de vie*

Toute une commande qui peut être terminé par le signal du clavier "CTRL+C".

- *Les commandes rapides*

Sont les commandes qui donnent un résultat durant un temps insensé par un humain par exemple :LS, KILL, etc.

Pour améliorer l'anti-virus, Il faut infecter les commandes rapides afin de les temporiser avant d'être exécuté. Pour cela on envisage une autre mesure de défense supplémentaire qu'on nomme « Virus Informatique défensif »

II.5.B)Virus informatique défensif

II.5.B.a) Notion du virus informatique

Le terme virus informatique c'est à dire un pseudo programme injecte leur code dans le code d'un autre programme afin de le saboter.

II.5.B.b) Notion du virus informatique défensif

Un virus informatique défensif est un programme qui injecte son code dans des commandes linux spécifiques afin de les monopoliser pour être utilisées par les algorithmes du VAO, en plus ces commandes ne sont pleinement utilisées que par VAO c'est à dire qu'un utilisateur (humain) ne peut pas manipuler ces dernières commandes librement.

Tout cela est temporaire (le virus informatique défensif ne s'exécute que pendant un intervalle de temps, durant le vote).

II.5.B.c) Mécanisme d'infection

Il infecte la commande système X (X peut être LS ou RM …), en passant par les étapes suivantes :

- Créer son code source dans un fichier X.c
- Compiler ce dernier en fichier binaire X.exe avec suppression de X.c
- Renommer la commande X par Y (Y est un secret d'entreprise IE)
- Déplacer X.exe à l'emplacement de la commande X

Par la suite quand un utilisateur tape la commande X sur le SHELL, c'est le programme X.exe (Virus) qui sera exécuté, et toute commande qui vise à toucher le fonctionnement du système retourne un message d'erreur après annulation. Si la commande X ne vise pas le système VAO, elle va appeler la commande Y comme il est présenté dans la figure :

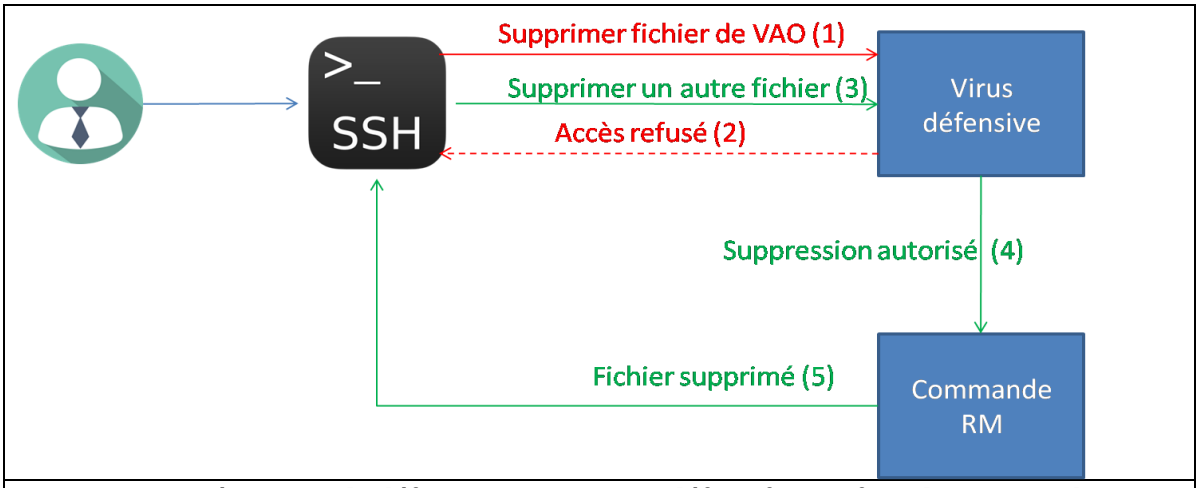


Figure 3.4 : Mécanisme de défense pour un Virus défensif qui infecte la commande «rm» pour sécuriser les fichiers VAO contre la suppression.

Avec cette technique on peut contrôler l'exécution de tous les commandes système rapides, mais le problème c'est que dans un système d'exploitation il n'existe pas que les commandes, il existe aussi des primitives du Shell comme (KILL, ECHO, etc.). L'exécution des primitives du Shell ne peut pas être contrôlées par ce type de virus défensifs, d'où une question sur l'existence d'une amélioration de cette version de virus afin de contrôler l'exécution de ces derniers.

II.6) Au niveau web

Avec le protocole SISP, N'importe quel programme de VAO peut être utilisé seulement par un script de web, dans ce sous-chapitre on définit comment assurer que l'appelant de programme c'est l'interface graphique original du VAO.

II.6.A)Mécanisme de sécurité au démarrage

Au démarrage d'application web, elle envoie une requête de type APP-UID au serveur afin de générer un identifiant à cette dernière.

Le serveur écoute sur 127.0.0.1. Quand il reçoit la trame APP-UID, Il interroge Constitution.class (c'est un programme inclus dans l'environnement de VAO contient les secrets d'entreprise IE) pour savoir s'il y'a un identifiant d'interface graphique. Si la réponse est oui la requête va être rejetée. Sinon il génère APP-UID et l'envoi au client, puis il lance une commande qui change le code source de constitution.java pour sauvegarder la valeur d'APP-UID dans Constitution.class.

II.6.B)Mécanisme sécurité au niveau Client

Le script qui va être lancé après la validation de vote par l'empreinte digitale envoie la donnée APP-UID initialisé au démarrage d'application en lecture seule, seulement par la fonction vao-AJAX qui va être la liaison entre l'interface graphique et les autres processus au serveur PHP, vao-AJAX est caractérisé par :

- Elle refuse tous les appels dans leurs sources n'est pas un clic sur l'un des boutons de l'interface graphique.
- Communique avec PHP avec la méthode POST.

II.6.C) Mécanisme de sécurité au niveau Serveur

Quand le script PHP reçoit une requête http, il applique la loi suivante :

Toute une requête http arrivant d'une autre page ou avec l'utilisation du Shell (la commande CURL) ou avec la navigation manuelle doit être refusée. Donc il faut accepter que les requêtes http qui arrivent de la fonction vao_AJAX.

II.7) Au niveau réseau

Dans ce sous-chapitre, On définit les mesures prises en utilisant firewall et un V.P.N pour assurer une sécurité acceptable au niveau du réseau VAO.

II.7.A) Protocole PASTRY

Le protocole PASTRY réalise une table de hachage distribué sur un réseau pair à pair organisé en un anneau virtuel de nœuds [6]. Il est basé sur l'algorithme de plaxton qui utilise les préfixes [7].

Pour router les messages, Pastry utilise trois composants : une table de routage qui est constituée de b colonnes et l lignes tels que b représente la base numérique et l la longueur de l'identifiant, un ensemble de voisins (neighborhood set) et un ensemble de feuilles établies (leaf set) [7].

II.7.B) Protocole Super-VPN

Ce protocole consiste, que chaque nœud source pour transmettre un message à une destination, il doit suivre un chemin des sauts entre des nœuds intermédiaires qui n'ont aucune relation avec le vote électronique. Conclu par résolution d'un problème d'acheminement PASTRY, en considérant les identifiants des nœuds du réseau sont des secrets d'entreprise IE. La source englobe le message en N couches de chiffrement en mettant N le nombre des sauts. A chaque saut, une couche s'enlève jusqu'à la destination.

II.7.C) Architecture du réseau

L'architecture du réseau VAO est une architecture hiérarchique. Le Serveur EL-Mouradia est la racine qui génère les environnements VAO propriétaires à chaque machine du réseau. Il est relié avec les serveurs niveau Wilaya (dans notre cas quarante-huit serveurs un par chaque wilaya au niveau national) occupent d'un rôle intermédiaire entre les serveurs centre de vote et le serveur EL-Mouradia pour but que le serveur racine travaille seulement avec les serveurs wilaya. Concernant les serveurs centre de vote sont des ordinateurs qui se trouvent dans les centres de vote, ils occupent de servir le service web et la gestion de la base de données à tous les machines de vote dans le centre (deux à trois machines par bureau) comme elle est montré dans la figure ci-dessous.

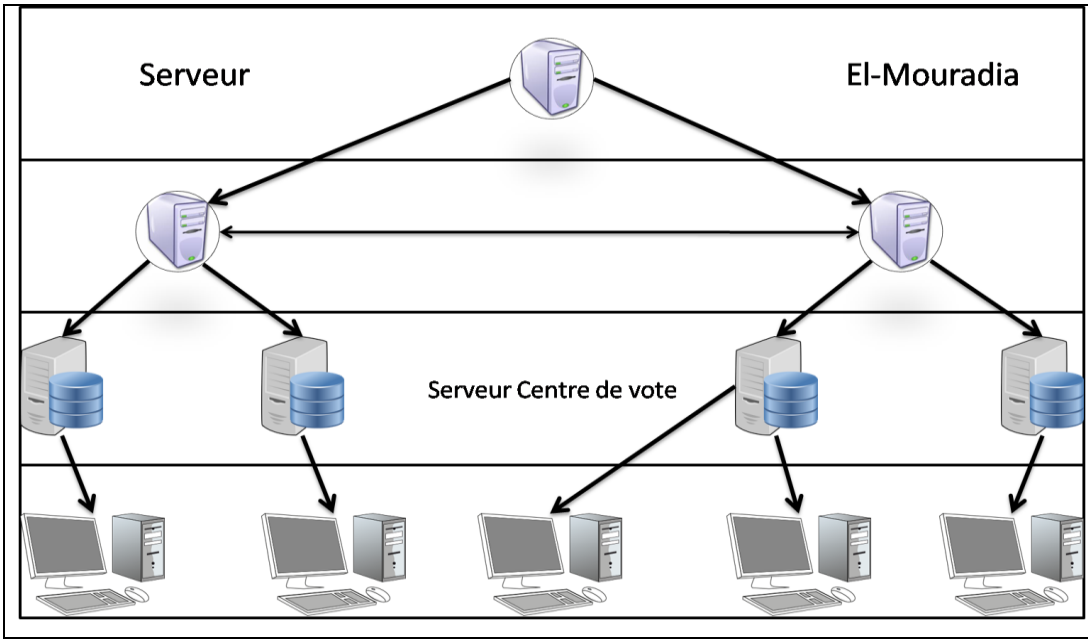


Figure 3.6 : architecture du réseau VAO

Les centres de vote dans le réseau admettent un LAN filaire ayant pour but d'assurer une bonne mesure de sécurité au niveau de chaque centre. Son architecture interne est comme suite :

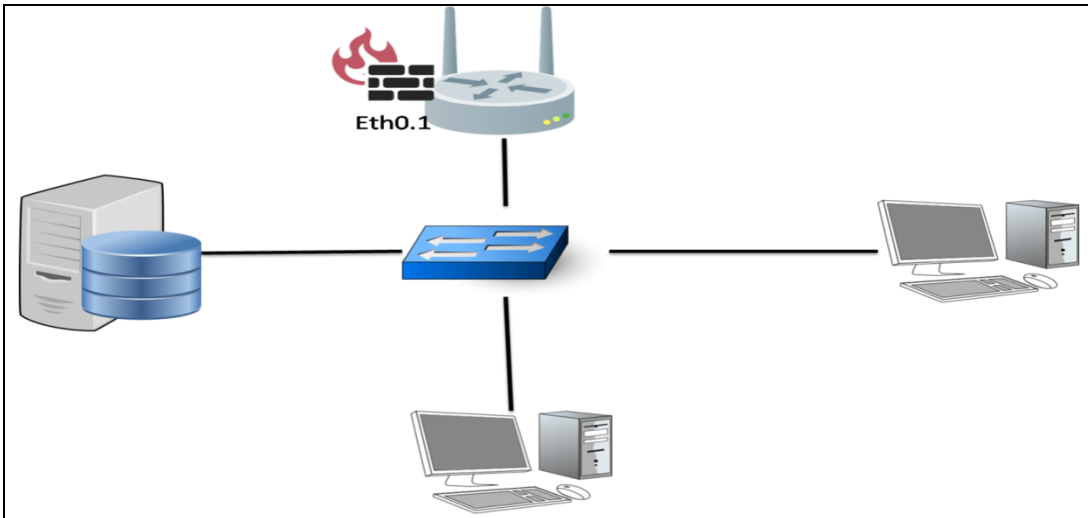


Figure 3.7 : Architecture d'un réseau LAN pour un centre de vote

II.7.D) Mécanisme de communication

Au début, le réseau VAO est anonyme pour cela, chaque machine du réseau suit les étapes suivantes pour acheminer les messages :

1. Chiffrer la trame en clair par leur cryptogramme.

2. Intégrer le masque désigné par le serveur EL-Mouradia sous Constitution.class au résultat de chiffrement comme une autre couche de codage et une preuve que l'émetteur est une machine du réseau VAO.
3. Envoyer le résultat à travers le protocole Super VPN.

Dans la destination, le processus inverse déclenche pour avoir le message, la figure suivante visualise le mécanisme de communication.

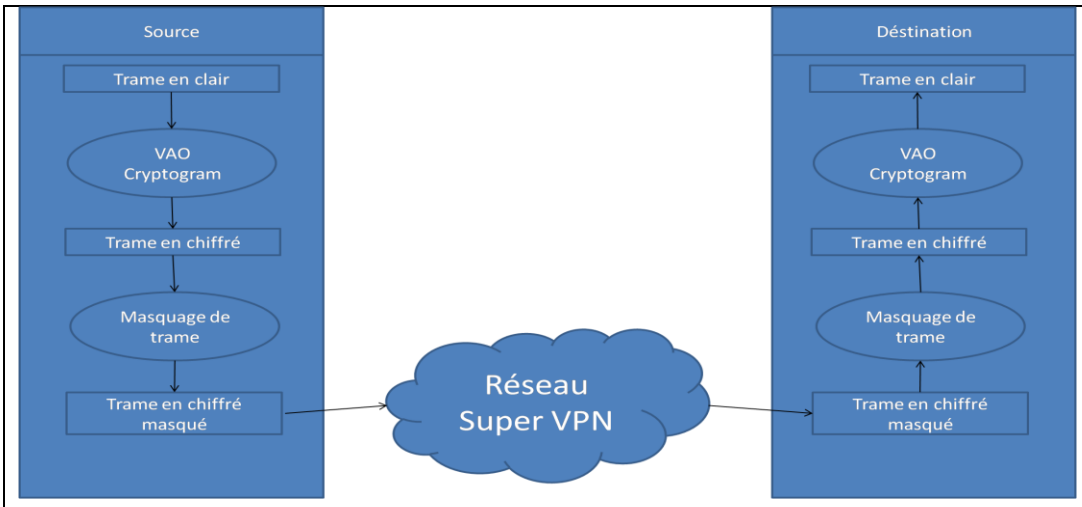


Figure 3.5 : Mécanisme d'acheminement des messages entre l'émetteur et le récepteur

II.7.E)Déroulement automatique de la communication

Quand la campagne électorale d'une élection à grande échelle s'achève, les aides administrateurs préparaient les centres de vote alors

- *15 min avant l'ouverture des centres*

Le serveur El-Mouradia engendre les environnements VAO en mode déconnexion qui contient :

- Les secrets d'entreprise IE.
- L'algorithme de masquage qui prend comme informations primitives le masque (une chaine des caractères découpé en N coupes avec N aléatoire dans des positions tirage au sort).
  Dans la source : l'algorithme concatène les coupures dans des positions randomisé au niveau la trame pour obtenir la trame masquée.

Dans la destination : L'algorithme connait les coupures donc il repère ces derniers dans la trame reçue puis l'enlever, si une coupure n'est pas repérée alors l'émetteur n'est pas une machine du réseau VAO et la trame sera rejetée.

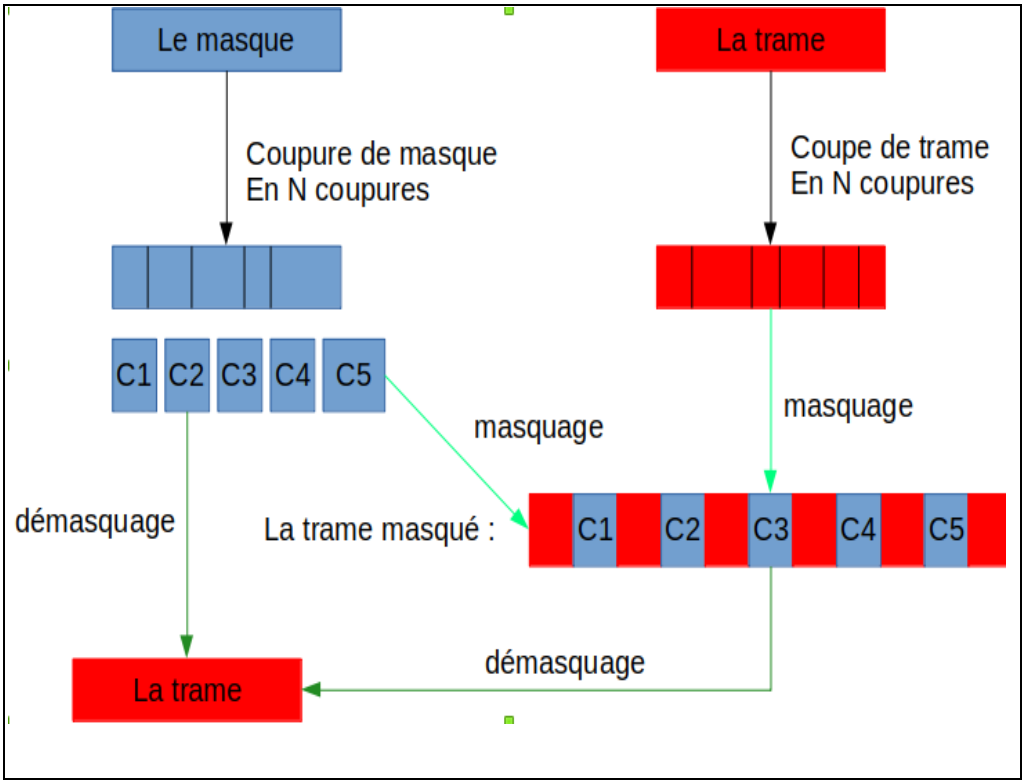


Figure 3.8 : Schéma qui présente le principe de fonctionnement d'algorithme du masquage et démasquage

- Anti DDOS : comme son nom l'indique, c'est un programme transmis par une machine dans le réseau au moment de réception d'ouverture d'un socket client, Leur objective c'est d'annuler toute une connexion aux serveurs du réseau par des machines qui ne sont pas autorisés administrativement par configuration de leurs pares-feux.

- *10 min avant l'ouverture*

Le serveur El-Mouradia propage les environnements à tous les machines du réseau

- *Déroulement de vote*

Le serveur El-Mouradia se déconnecte, puis chaque serveur wilaya informe leurs voisins d'un numéro de port qui reste un secret d'entreprise IE changé à chaque

communication sous le nom technique SPC (Self Port Communication), ensuite il configure leur firewall pour accepter que les messages qui arrivent au serveur wilaya dans le port SPC, Concernant les serveurs centre de vote, ils acceptent que les messages qui arrivent pour le port SPC de leur serveur wilaya. Après chaque communication le serveur change leur SPC et reconfigure leur pare-feu et envoie un message de mise SPC à tous les voisins.

- *Un votant arrive pour effectuer un vote*

Si l'intéressé effectue un vote dans le même centre d'inscription alors l'opération de validation d'empreinte faîtes comme elle est définit précédemment, sinon il a besoin d'une validation à distance.

- *La validation d'empreinte à distance*

Pour cela la machine de vote envoie l'empreinte dans un paquet avec cinq couches de chiffrement dans le réseau à travers leur serveur centre de vote, puis au serveur wilaya départ, puis au serveur wilaya destination, puis le serveur centre d'inscription de votant, puis à l'ordinateur où l'empreinte d'intéressé est sauvegardée, à chaque saut une couche s'enlève. Puis la validation se fait à distance et la réponse est retournée à la machine de vote qui effectue la voix.

Cette communication n'est pas effectuer par le protocole d'anonymat SUPER-VPN.

- *La validation d'une voix*

Quand le vote est validé, La machine envoie les requêtes qui permettent de faire la mise à jour de la table vote à leur serveur du centre pour que cette dernière va être exécuté avec toute transparence.

- *La durée du vote est terminée*

Chaque serveur centre de vote envoie la table candidat sous format JSON à leur serveur wilaya, pour que le destinataire calcule et conclut la table candidat pour la wilaya et envoie le résultat au serveur EL-Mouradia.

Le serveur EL-Mouradia arrive à se connecter pour assembler les tables candidats de chaque wilaya et conclut le résultat final en suivant la loi de changer @ip à chaque réception par des adresses renseignées dans Constitution.class.

La communication entre les serveurs dans les derniers moments se faite à travers le protocole SUPER-VPN.

II.8) Conclusion

Dans ce chapitre, on peut assurer une protection en quatre niveaux : réseau et système d'exploitation, web et base des données pour notre logiciel contre les menaces du cyber attaque afin de protéger les données contre les modifications, par définition de plusieurs barrières de sécurité, c'est-à-dire, quand un attaquant arrive à percer une barrière, il trouve d'autres devant lui.

III) CHAPITRE 3 : Conception

III.1) Introduction

Dans ce chapitre, nous présenterons les objectifs de notre application, ce qui nous amène à identifier les possibilités du système et les besoins des utilisateurs que nous allons schématiser dans les diagrammes de cas d'utilisation global et des diagrammes de séquences détaillés [1].

III.2) Définition d'application

C'est une application web semi hébergé mono plateforme Sécurisé fonctionne pour des clients possédant des systèmes d'exploitation cœur UNIX. Elle est crée pour gérer et garder la transparence des votes en générale.

Une application web semi-hébergé est une application web installée sur un ordinateur possède deux serveurs web logiques :

- Serveur web publique occupe en plus de la mise à jour de la base des données.
- Serveur web privé : c'est un serveur web local dans la machine non visible au public qui occupe de la cryptographie et les appels systèmes et le callback (la vision temps réelles de changements dans la base des données).

Cette application est servie à des clients possédant des serveurs web privés.

III.3) Services offerts par cette automatisation

Cette application va nous offrir des services nécessaires pour couvrir les besoins d'automatisation d'une manière chronologique qui sont les suivantes :

- Création du compte administrateur
- Création d'une élection
- Consultation des vidéos de conférence et affectation des signatures électorales pour les candidats dans la phase de précampagne électorale
- Affichage des statistiques en temps réel des résultats au niveau wilaya et affectation d'un vote dans la phase d'Election
- Gestion d'une élection
    - Ajout ou suppression d'un candidat dans la phase précampagne électorale

- Ajout des comptes des votants
- Enregistrement d'un ordinateur comme machine de vote avant la phase d'élection
- Déclaration d'une carte volée comme une carte douteuse

- Validation de son propre compte votant

III.4) Analyse et spécification des besoins fonctionnels

III.4.A) Analyse fonctionnelle

III.4.A.a) Analyse des besoins :

Cette partie est un recueil des besoins du système à réaliser. Pour pouvoir clarifier les besoins des utilisateurs de notre application [1].

III.4.A.b) Besoins fonctionnels

C'est les fonctionnalités du système, Ce sont des besoins spécifient le comportement d'entrée/sortie d'application [1]. Les besoins fonctionnels de notre application sont :

- Chacun a la possibilité de créer un compte administrateur.
- Chaque administrateur doit créer une élection (informer le système qu'il a besoin de gérer un processus électorale).
- Il peut aussi engager des aides administrateur.
- Un votant peut valider son propre compte.
- Chaque utilisateur peut faire des opérations sur le système en respectant l'ordre chronologique suivant :
  - *A la phase pré-campagne électorale :*

    C'est la phase qui sépare la création d'une élection et le démarrage de la phase compagne électorale dans cette phase :
    - Le journaliste peut créer une vidéo de conférence pour un candidat à condition de la présence de l'intéressé
    - Le votant peut voir les vidéos de conférence qui concerne les candidats et effectue des signatures électorales
    - L'administrateur peut créer un candidat ou un compte d'un votant.

Aussi il peut retirer un candidat à condition la présence physique de ce dernier.

- *A la phase compagne électorale :*

Dans cette phase les aides administrateurs peuvent enregistrer des ordinateurs comme des machines du vote.

- *A la phase Election :*

C'est la phase qui sépare l'ouverture et la fermeture des centres de vote dans la phase tous les utilisateurs peuvent voir les résultats du vote en temps réel et effectuer des voix, et pour l'agent policier d'ajouter ou retirer des cartes douteuses.

Remarque : Chaque utilisation d'application sauf la connexion et la création d'une élection et création du compte doit être inclut la validation par la pointeuse digitale pour assurer qu'elle est utilisée par une personne physique réelle

III.4.B) Analyse non fonctionnelle

Nos besoins non fonctionnels à travers notre application sont :

- *Sécurité :*

Le vote électronique est un projet informatique sensible. Comme tous les projets de même catégorie il faut des algorithmes de sécurité très sophistiqué en traçabilité. Ce qui guide à réaliser un bon niveau de sécurité en contrôle d'accès pour but de garder l'intégrité des statistiques finales.

- *Interface :*

Avoir une application qui respecte les principes des Interfaces Homme/Machine (IHM) tels que l'ergonomie et la fiabilité [1].

- *Extensibilité :*

L'application va être apte au changement par ajout des autres options de tel sorte qu'elle utilise l'empreinte d'utilisateur en authentification dans le cas de disponibilité de la pointeuse digitale sinon elle utilise automatiquement les mots de passe tapés en utilisant des **claviers virtuels variants** pour le système de preuve.

- *Convivialité :*

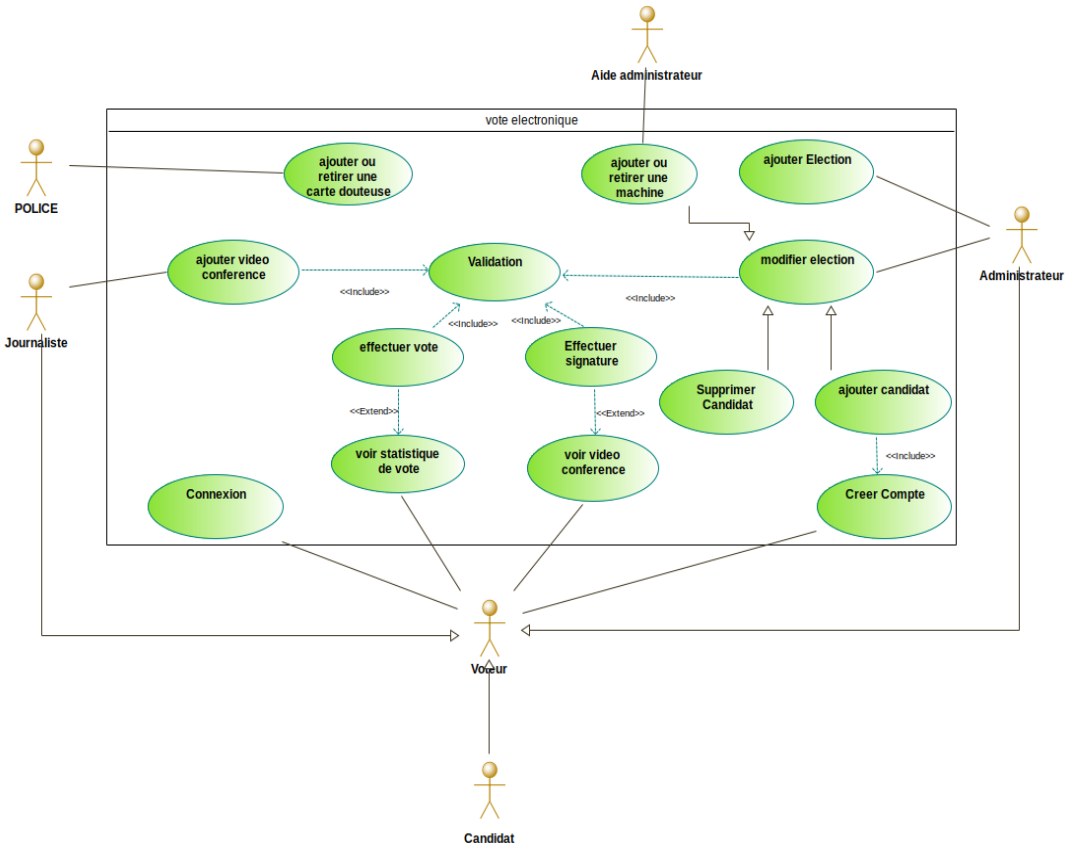
L'application doit être simple et facile à manipuler surtout pour les gens âgés.

III.5) Présentation du langage UML

UML (Unified Modeling Language), Ou Langage de modélisation unifiée, est un langage de modélisation graphique à base de pictogrammes (c'est un dessin figuratif ou une représentation graphique, il est utilisé pour rendre explicite un objet ou un message dans les langues écrites. C'est également un symbole d'écriture ou un signe linguistique dans les langues non écrites [12]). Il est utilisé en développement logiciel, et en conception orientée objet. UML est couramment utilisé dans les projets d'ingénierie des logiciels [1], Il comporte plusieurs diagrammes :

- Diagramme des cas d'utilisation
- Diagramme de classe
- Diagramme d'objets
- Diagrammes de séquence
- Diagramme état transaction
- Diagramme d'activité
- Diagramme de déploiement

III.6) Diagramme des cas d'utilisation



Figures 2.1 : Diagramme des cas d'utilisation globale pour l'application de vote électronique

III.7) Diagrammes de séquence

- *Ajouter Candidat ou effectuer une signature électorale*

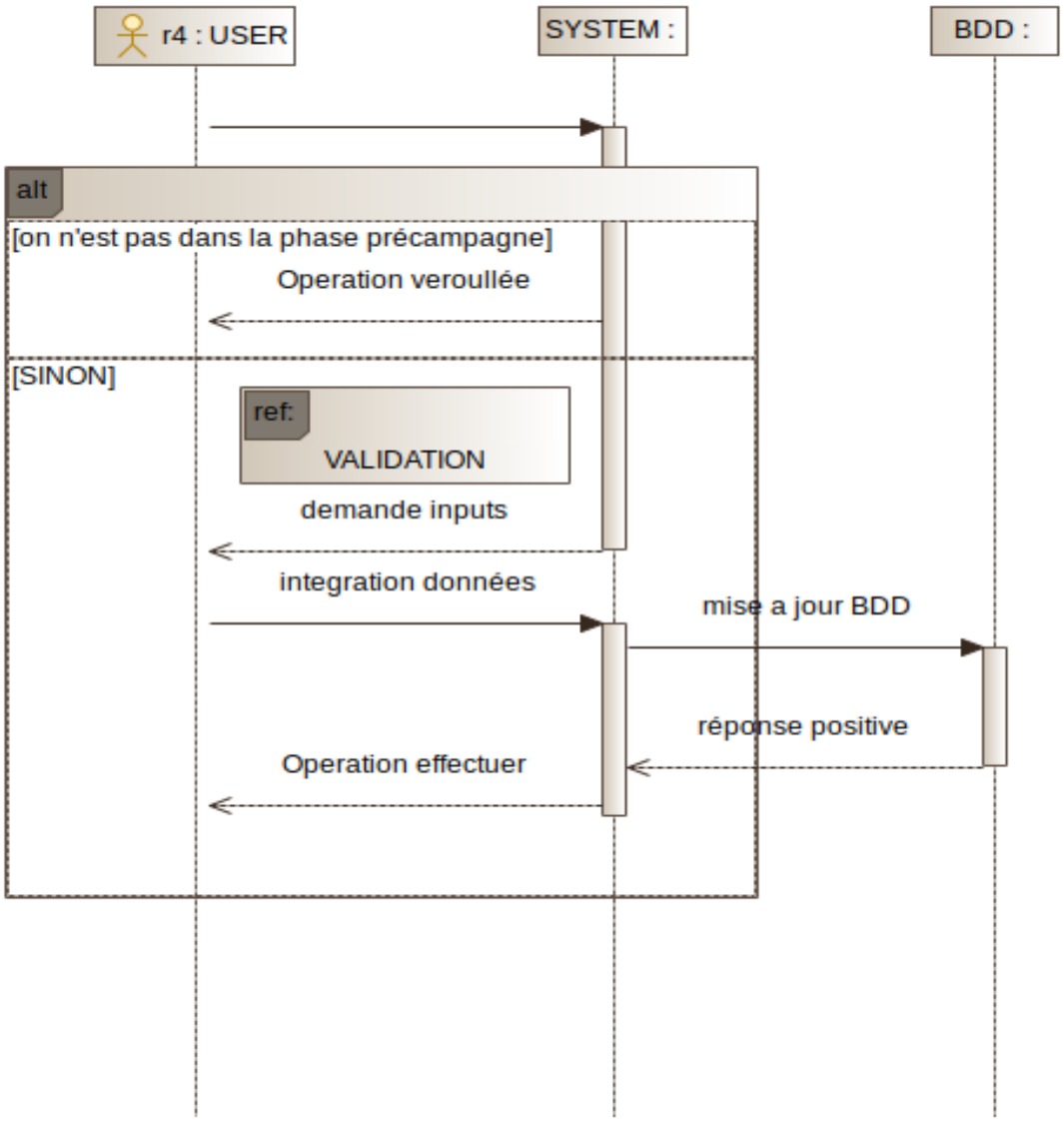


Figure 2.2 : Diagramme de séquence pour les opérations ajouter candidat et effectuer signature électorale

- *Supprimer Candidat ou ajouter une vidéo de conférence*

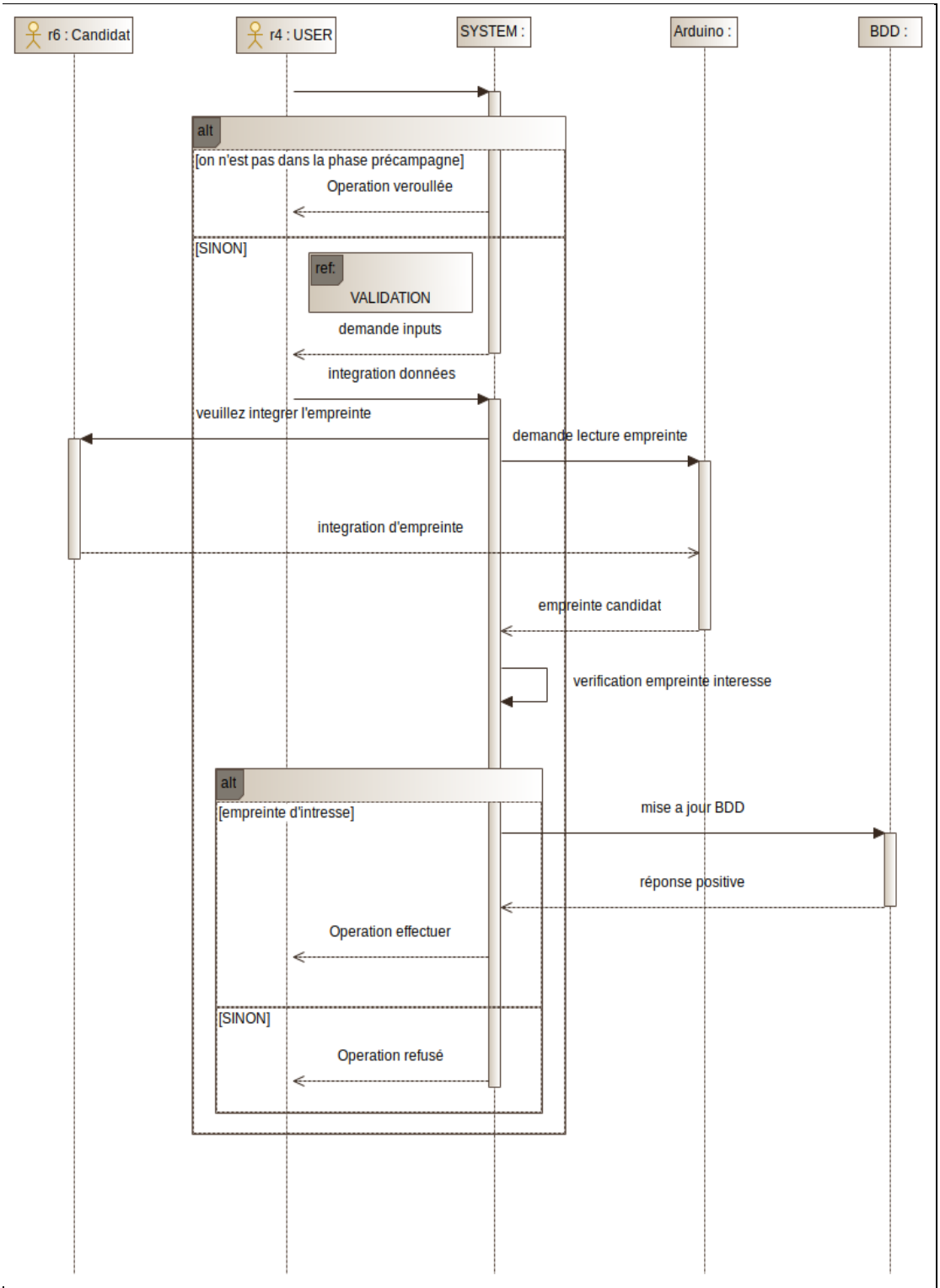


Figure 2.3 : Diagramme de séquence pour Supprimer Candidat ou ajouter une vidéo de conférence

- *Effectuer un vote*

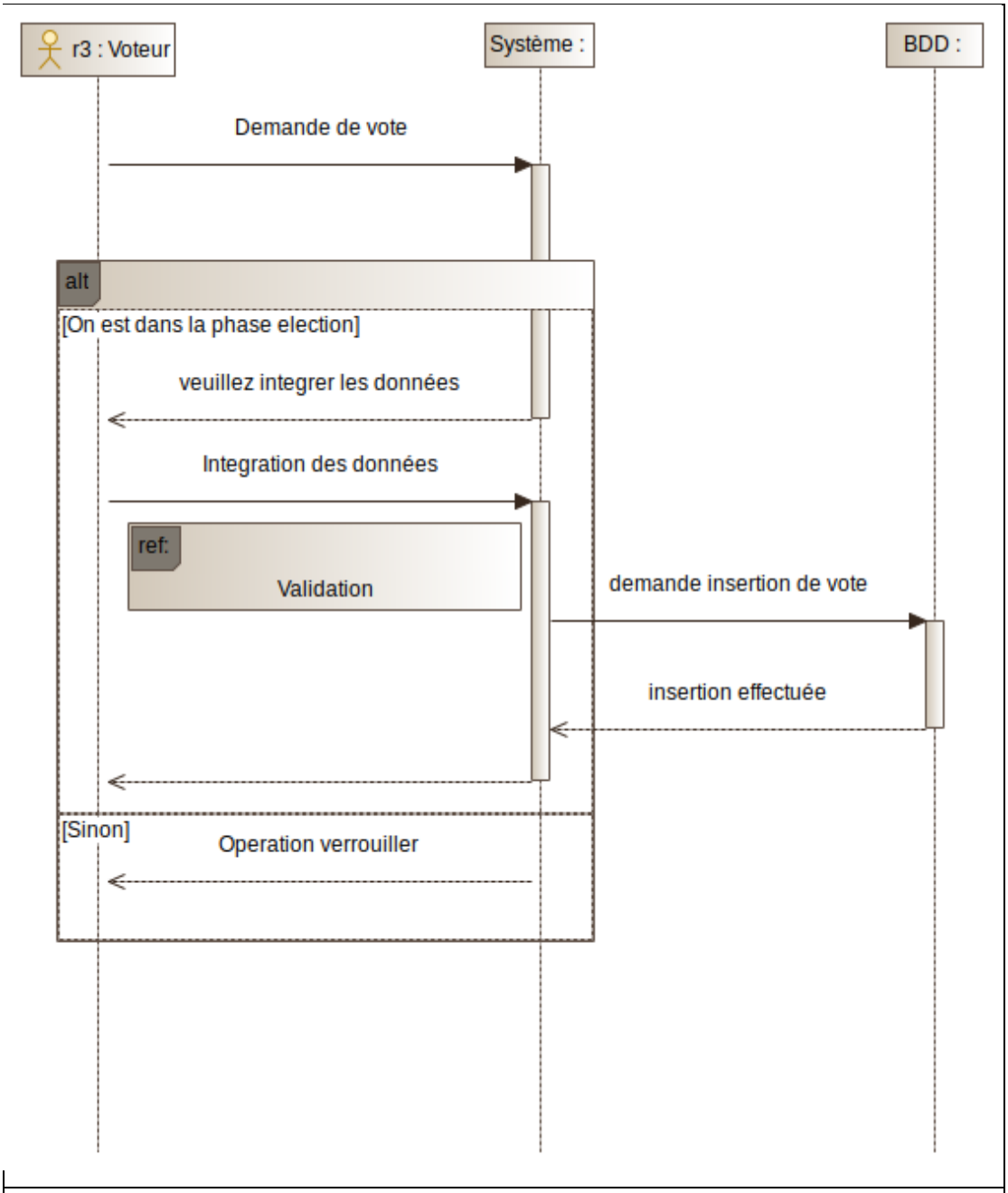


Figure 2.4 : Diagramme de séquence pour Effectuer Vote

- *Connexion*

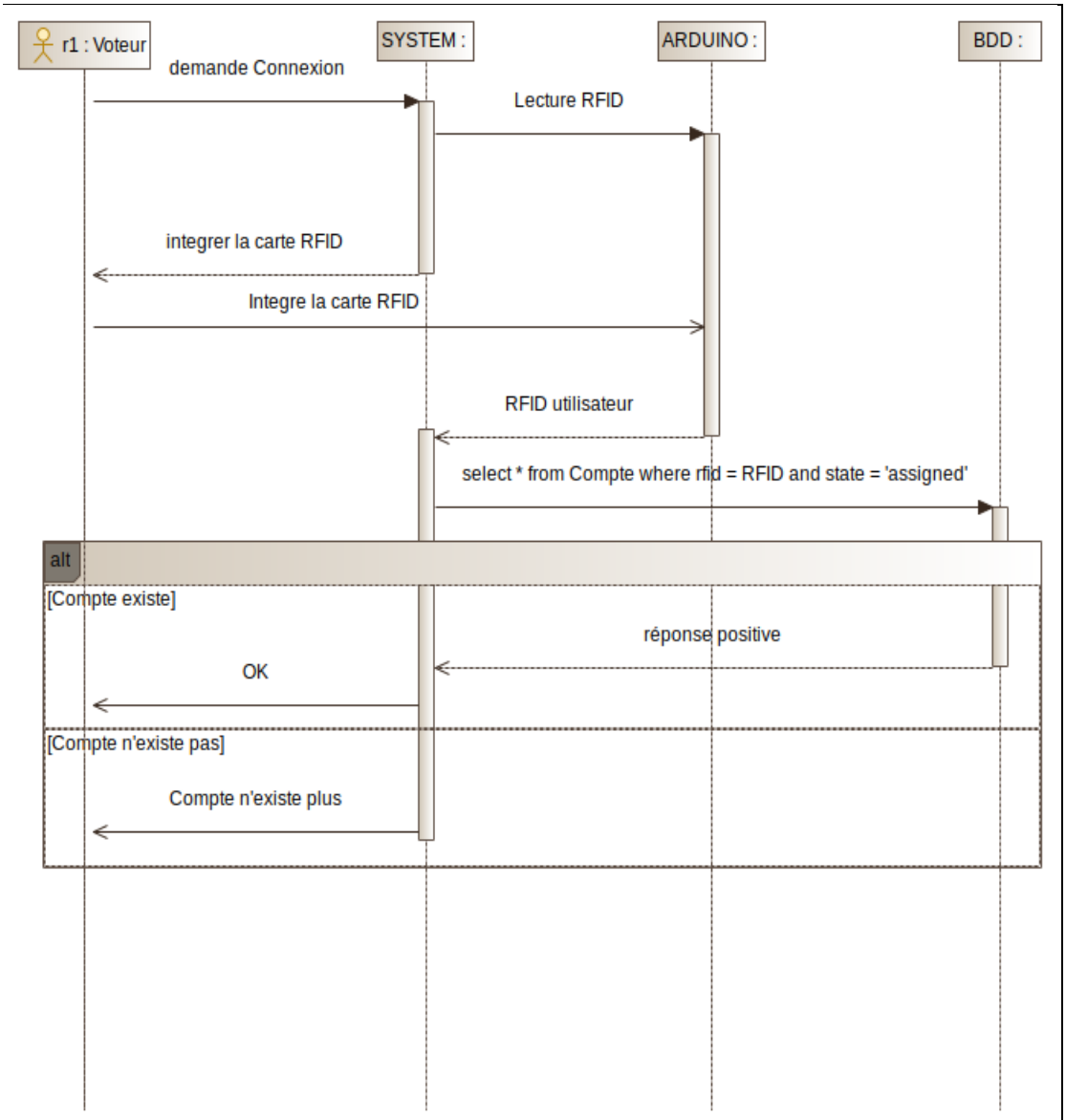


Figure 2.5 : Diagramme de séquence pour la connexion

- *Inscription*

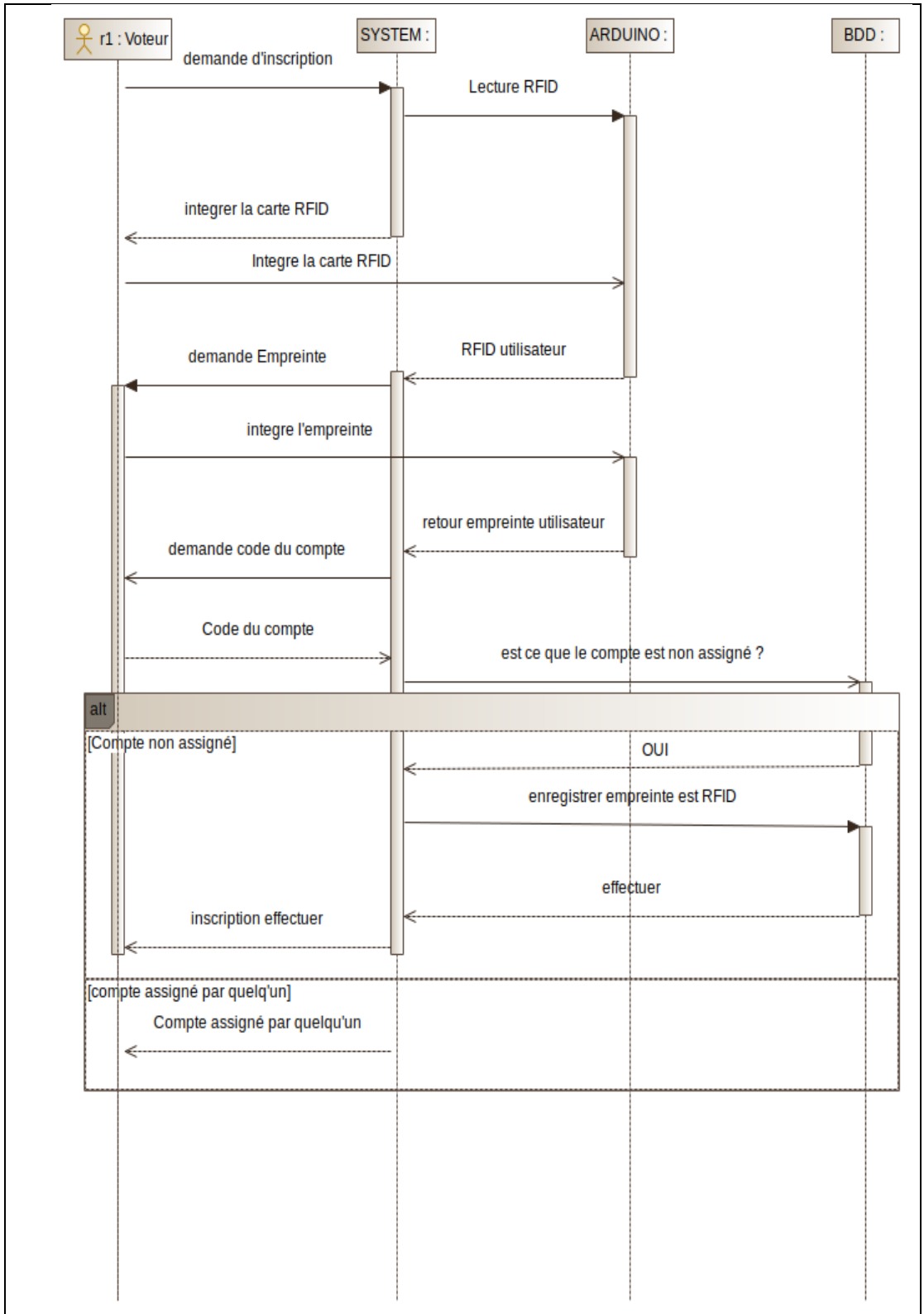


Figure 2.6 : Diagramme de séquence pour l'inscription

- *Validation*

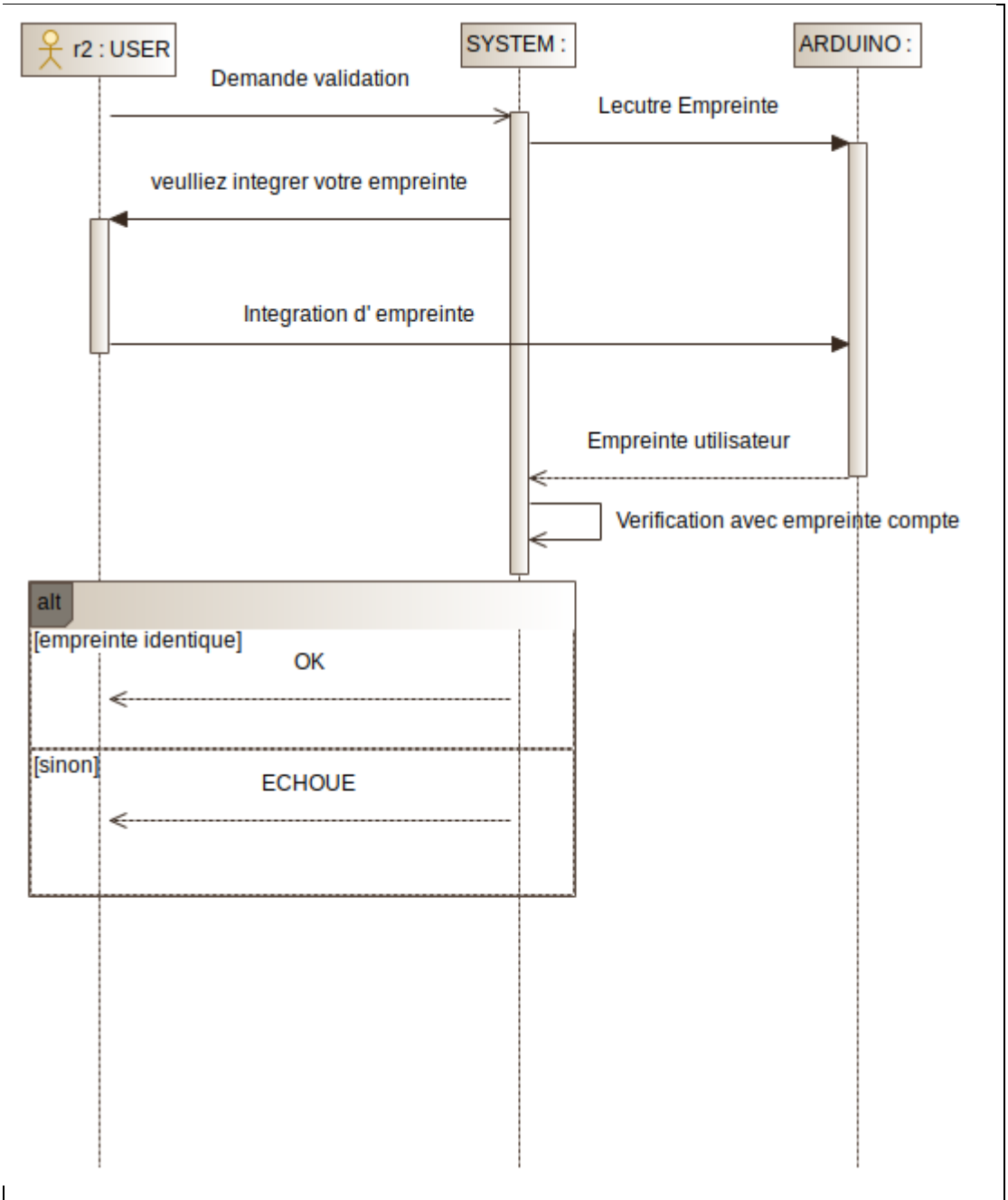


Figure 2.7 : Diagramme de séquence pour la validation

III.8) Diagramme de classe

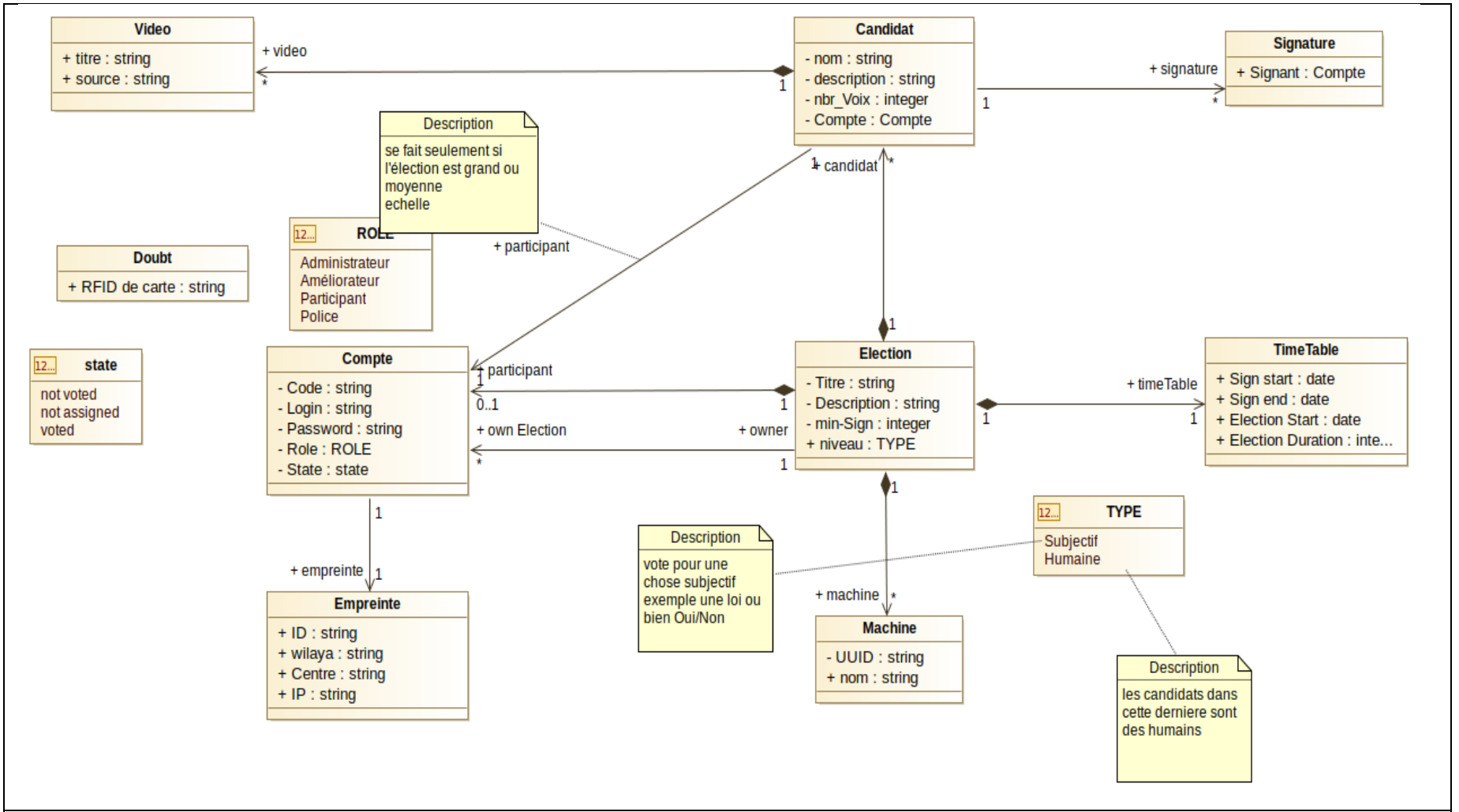


Figure 2.8 : Diagramme de classe pour le système VAO

II.9) Conclusion

On a défini dans ce chapitre, les principaux besoins des utilisateurs, ainsi qu'une petite notion sur le fonctionnement du système sécuritaire implémenté dans cette dernière.

IV) CHAPITRE 4 : Développement

IV.1) Introduction

Dans ce chapitre, on définit l'environnement matériel et logiciel dans lequel notre PFE a été développé.

IV.2) Outils de développement

Notre projet aide des outils matériels et logiciels pour être réalisé. Le tableau ci-dessous montre tous les outils utilisés dans notre cursus de projet.

Outils	Catégorie	Logo / image	Description
Le serveur XAMPP	Outils Logiciels		Le serveur Apache est un logiciel libre open source qui est initialement développé par un groupe de développeurs de logiciels et maintenant il est maintenu par Apache Software. Fondation. Apache HTTP est un serveur distant (ordinateur) si quelqu'un demande des fichiers, des images ou des documents en utilisant son navigateur, il servira ces fichiers aux clients utilisant des serveurs HTTP. Principalement les sociétés d'hébergement utilisent cette application pour créer un serveur VPS et un hébergement partagé pour leurs clients. (Ganesan, 2017) [9].
Environnement Node js			C'est un serveur web qui utilise le java-script coté serveur
Le serveur Node atlas			C'est un outil de NODE JS utilisé pour créer un serveur web peut servir

			jusqu'à cent milles client simultanément
Oracle 10g Entreprise Edition			C'est un SGBD (Système Gestion BDD) utilise des techniques d'administration des bases de données adapté pour administrer la base de données du vote électronique
Environment ARDUINO			Arduino Software (IDE) permet d'écrire des programmes pour fonctionner des systèmes embarqués.
Environnement PROCESSING IDE			C'est un environnement java utilisé comme intermédiaire entre la carte ARDUINO et les autres programmes du VAO
Notepad++			Notepad++ est un éditeur de code source. Ce programme, codé en C++ avec STL et win32 API, a pour objet de fournir un éditeur de code source de taille réduite mais très performant [10].
Traceur eBPF :			C'est une machine virtuelle sous le KERNAL UNIX, à plusieurs utilités parmi les : - Tracer les appels système avec la commande EXECSNOOP elle visualise les commandes lancées, leurs PID (PROCESS ID), le PID de lanceur, et comment la commande a été écrite sur le SHELL - Tracer les fichiers ouverts avec la commande OPENSNOOP qui visualise les chemins et les PID des processus lancés par un programme open-source comme (.PHP, .PY, .JS, etc.)

			- Visualiser les trames reçus par l'ordinateur avec TCPACCEPT - Visualiser les trames transmit avec TCPCONNECT
Arduino UNO	Outils Matériels		C'est un microcontrôleur ATmega328 programmable permettant de faire fonctionner des composants (moteurs, LEDS, Capteurs, etc.). Elle possède des ports permettant par exemple de se connecter à ordinateur ou de s'alimenter. [8]
La carte MFRC522			C'est un lecteur de carte RFID utilisé dans le cadre de VAO pour lire la carte du vote RFID des votants
Capteur d'empreinte digital GT511c3			C'est un outil biométrique programmable capte les empreintes des doigts humains
Les resistances			C'est un composant électronique ou électrique dont la principale caractéristique est d'opposer une plus ou moins grande résistance à la circulation de courant électrique. [8]
Les leds			Ce composant électronique est en train de faire sa place les sources d'éclairage. Elles sont utilisées que dans un nombre restreint de domaines. - Eclairage des téléphones portables, blocs autonomes de sécurité, borne de balisage routier.

			- En production de lumière blanche. - En trichromie, les fabricants trouvent des solutions compactes de linéaires ou petits projecteurs à changement de couleur [11].
Platine d'essai			La platine d'essai est composée d'un boitier en plastique comportant des lignes et des colonnes de trous, comme il est montré dans la figure 4, sous lesquelles courent des rails de cuivre. Ces rails vous permettent de connecter rapidement et facilement les composants [8]. Les rails latéraux sur la grande longueur sont généralement utilisés pour fournir la source d'alimentation PWR et la masse GND. Ils sont parfois libellés avec un symbole (+) ou (-) [8].
Les straps			Les straps représentés sur la figure sont essentiels pour utiliser votre platine d'essai. Ce sont des fils isolés assez courts qui permettent de relier vos composants aux rangées de votre platine d'essai, à d'autres composants, et à votre carte Arduino, Un strap n'est pas différent d'un fil en général, mais il est généralement coupé court en possède en général des broches isolées à ses extrémités [8].
Buzzer			C'est un composant électronique fonctionne créer pour but d'émission des signaux sonores avec des fréquences programmable par l'utilisateur. Il est utilisé généralement dans les alarmes

Concernant les langages utilisés sont les langages du web (Java script, PHP, HTML5, CSS3). A côté du langage C et Java pour les taches qui utilisent les secrets d'entreprise IE.

IV.3) Branchements ARDUINO

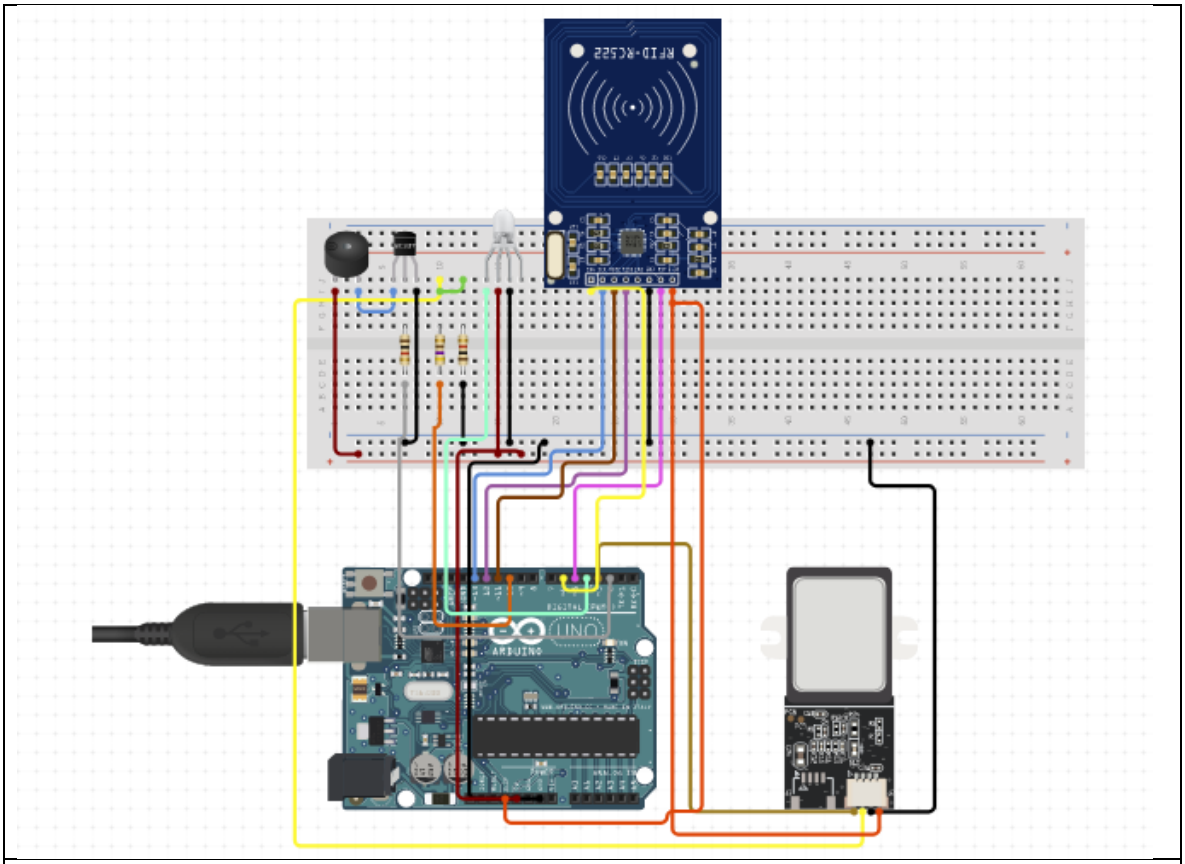


Figure 4.1 : Branchement Arduino pour le système VAO

IV.4) Interface graphique

- Consultation de l'interface :

Figure 4.2: Interface du vote en mode biométrique

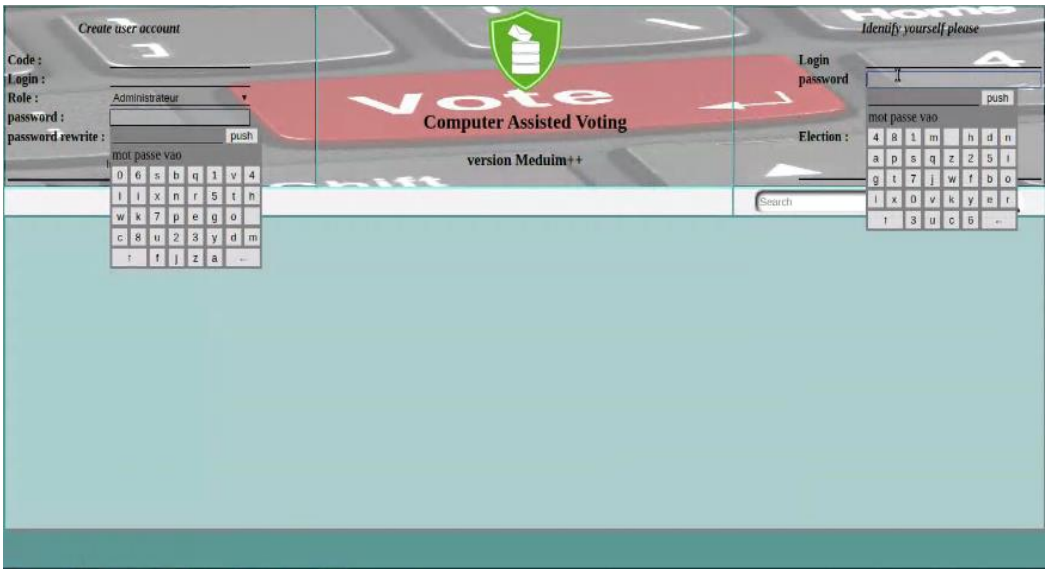


Figure 4.3: Interface graphique en mode mot de passe

- Créer un administrateur :

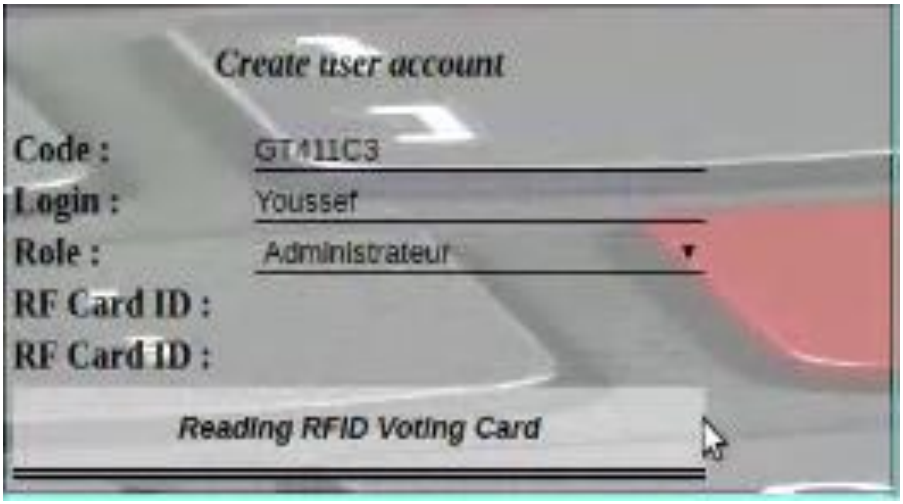


Figure 4.4 : Création de l'administrateur Youssef sous le code d'inscription "GT411C3"

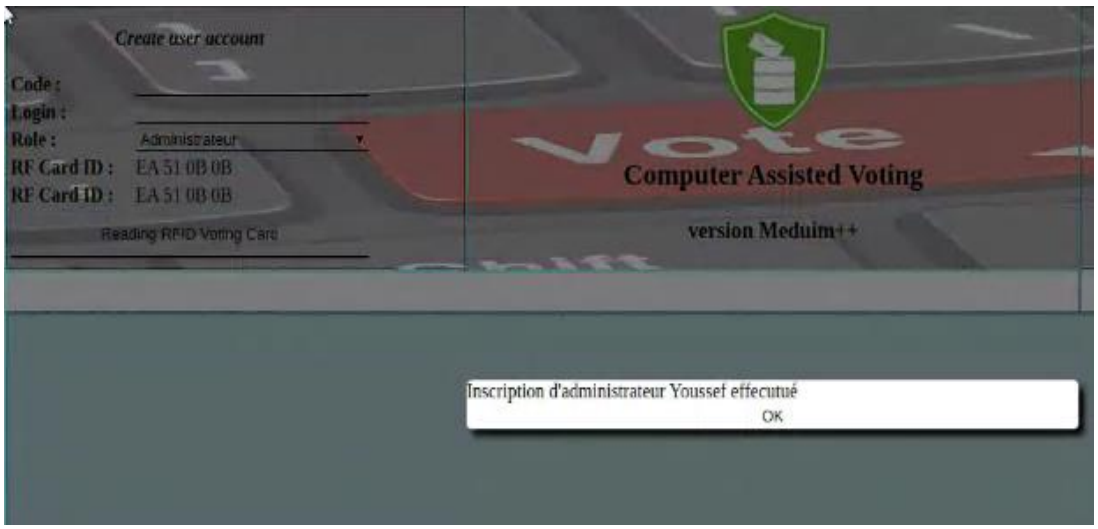


Figure 4.5 : Inscription d'un administrateur réussi

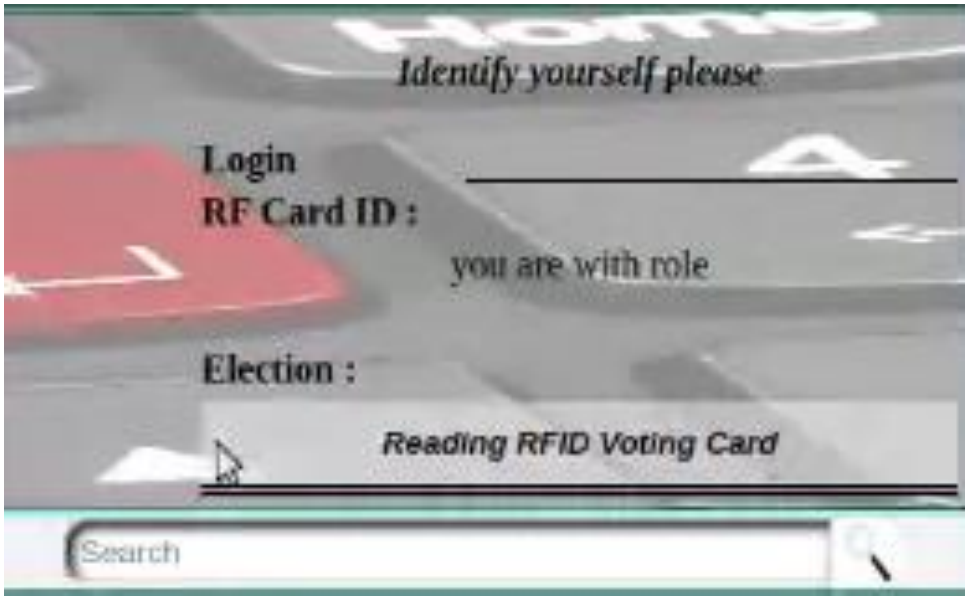


Figure 4.6: Authentification d'un administrateur

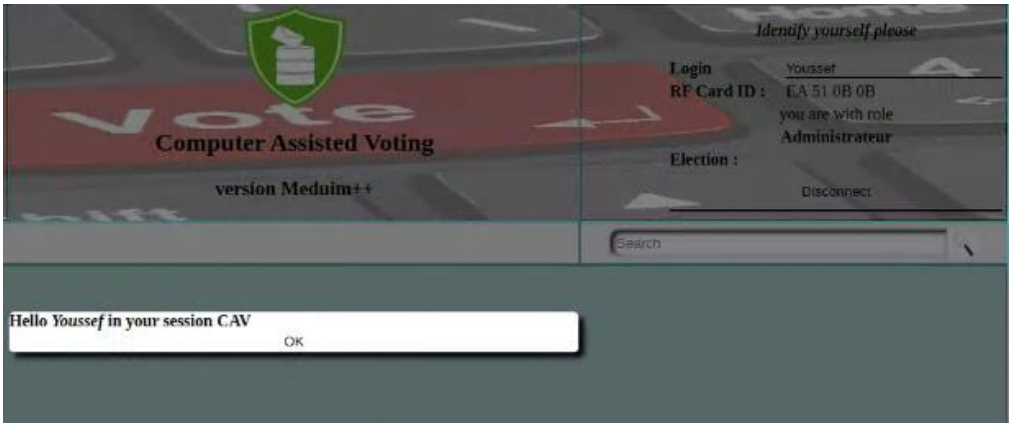


Figure 4.7 : Authentification d'un administrateur réussi

- Créer un compte participant :

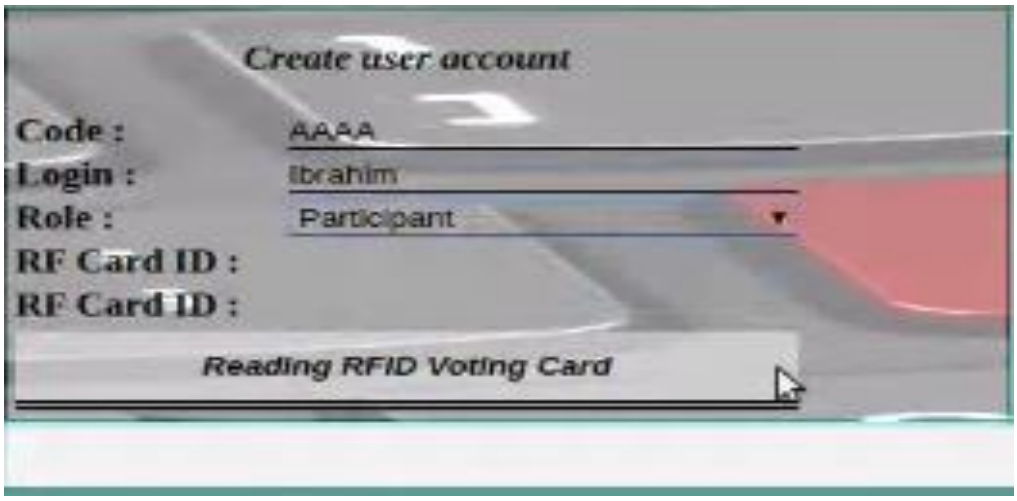


Figure 4.8: Création d'un compte participant

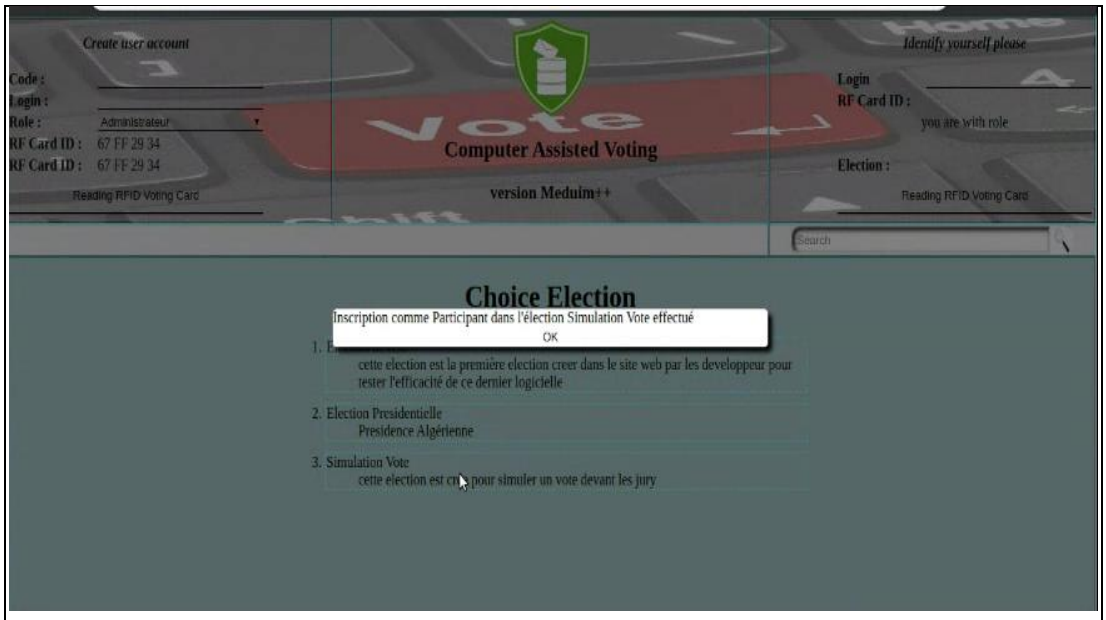


Figure 4.9: Inscription d'un participant réussi

- Créer une élection :

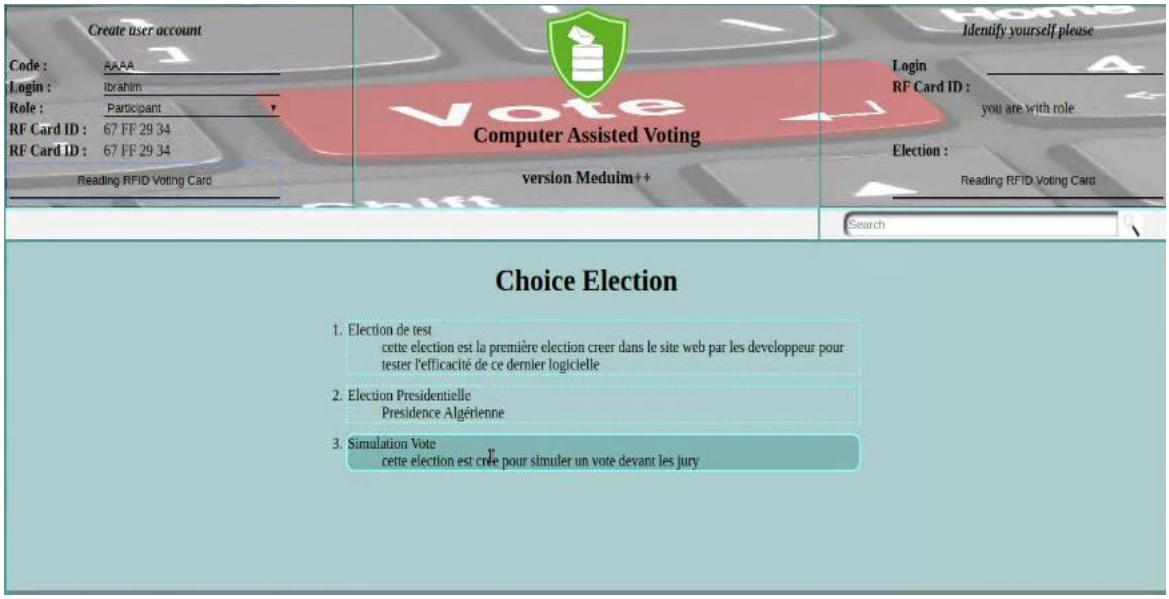


Figure 4.10 : Choix l'élection ou vous voulez participer

.

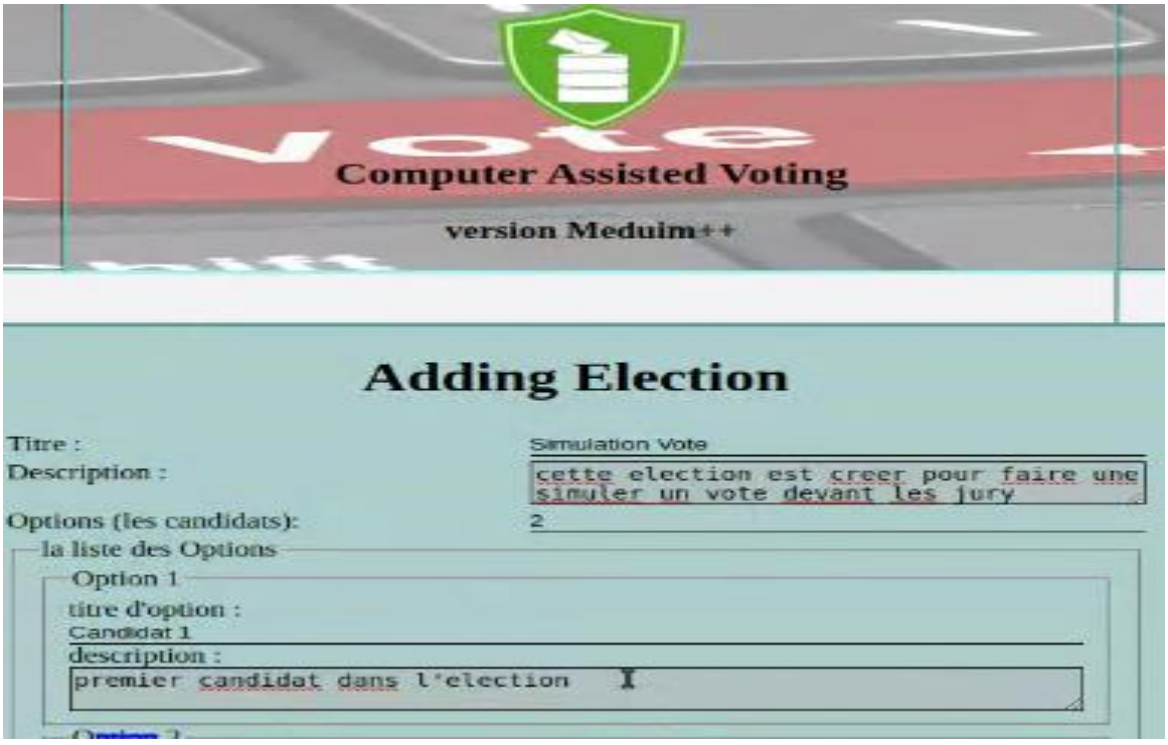


Figure 4.11 : Ajout d'une élection

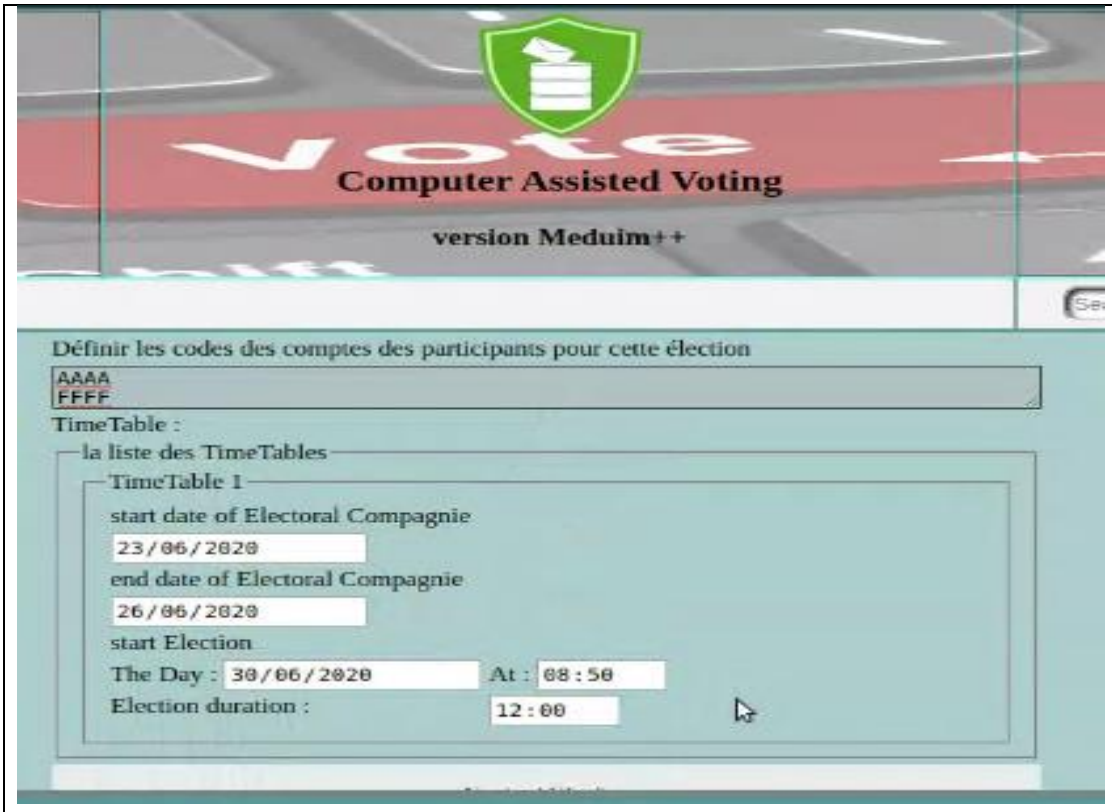


Figure 4.12: Ajout d'une élection

- Effectuer un vote :

Figure 4.13: Réalisation d'un vote

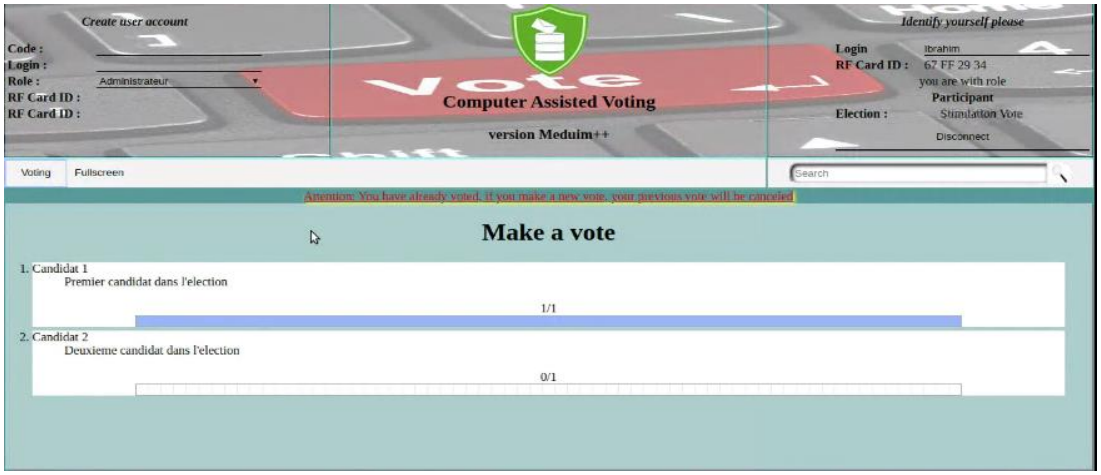


Figure 4.14 : Interdiction d'effectuer un autre vote pour le même votant

IV.5) Conclusion

Ce chapitre consistait à démontrer les différentes fonctionnalités du système développé. Les différents scénarios d'une élection ont été proposés. Plusieurs services pour sécuriser un réseau d'un système gérant le vote électronique, ont été proposés. Le but est l'organisation des élections représentatives des voix et des opinions des votants.

Conclusion générale

Le travail réalisé dans le cadre de ce projet de Master en Informatique, option « Réseaux et Systèmes distribués » propose une solution technique afin de sécuriser un processus très sensible qui est le ”Vote électronique”. Nous avons commencé le manuscrit, par définir la biométrie qui permet d'élever le niveau de sécurité avec quelques domaines d'applications en Algérie. Puis, nous avons donné quelques détailles, par la suite, comment des élections à grande échelle sont organisées par notre système informatique en scindant l'opération en trois phases successives (phase précampagne électorale - phase campagne électorale - phase élection). Le chapitre « mesures de sécurité » nous a permis de définir quelles sont les mesures à mettre en œuvre pour assurer des élections transparentes. Ensuite, nous avons opté pour des techniques de défense à plusieurs niveaux (Web, Système d'exploitation, Réseau et la base de données). Enfin, nous avons défini le matériel biométrique et la carte Arduino UNO utilisée pour ce système et les branchements qui ont été fait. A cause de la crise de Covid-19 et la fermeture des frontières, nous avons rencontré une multitude de difficultés pour acquérir les différents équipements, comme la pointeuse digitale non disponible au niveau national. La fermeture des bibliothèques et les espaces de travail de l'université était aussi une contrainte qui a empêché d'élever le niveau de collaboration et le travail en équipe. Pour en conclure, on affirme que les objectifs ciblés à l'entame du PFE, ont été largement atteints, comme :

- Assurer la transparence de l'opération ;
- Gagner en temps pour dévoiler les résultats ;
- Voter dans le centre le plus proche, sans déplacements.
- Minimiser le nombre des bulletins nuls au maximum ;
- Minimisation des charges du personnel et matériels habituels pour organiser les élections.

Perspectives de projet :

Le travail est ambitieux, prometteur mais sensible, il peut être développé et enrichi sur plusieurs plans, dont on cite quelques unes :

- Création d'une équipe de développement qui se compose de plusieurs départements informatiques, où chaque département est spécialisé dans une tâche comme le département réseau, département Ethical-Hacking, Web etc... et autres comme sciences humaines, sciences politiques, le droit, etc…

- Être indépendant dans le cadre de la technologie c'est à dire des DATA-CENTER et un réseau personnel pour l'Algérie afin de garantir la disponibilité du système dans les élections.

- Le vote à domicile destiné à des personnes âgées ou des malades alités ou pour garantir le déroulement de vote dans un environnement épidémique. Ce type de vote ne peut se faire que dans un vote électronique.

Enfin, nous souhaitons que nos efforts soient valorisés en prenant en considération notre système VAO par les autorités officielles de l'état. Le renforcement du système de sécurité nous permettra d'enrichir nos expériences pour développer d'autres systèmes informatiques stratégiques.

Dans ce mémoire on a présenté les mesures de sécurité à mettre en œuvre pour défendre notre système contre les attaques informatiques sans oublier que le bon Dieu est le meilleur savant et protecteur. Le seul risque persistant est la défaillance des administrateurs de l'application, vu qu'ils ont accès aux algorithmes du système, qui va leur donner la possibilité de développer une version pour faire gagner un candidat précis.

وَاللهُ الحَفِيظُ العَلِيمُ

Bibliographie

[1] : Application client/serveur pour le suivi des patients diabétiques, Chapitre Conception, Ilyes Benabdellah , Université Hadj Lakhdar Batna

[2] : https://www.editions-tissot.fr/droit-travail/dictionnaire-droit-travail-definition.aspx?idDef=802&definition=Biométrie&fbclid=IwAR1SZlj2g6-KuW_TItg_mjGcas2GjwiAQTZ5xeVVM0U4NrgT6YeR4W0iPYg visited 01/06/2020

[3] : https://www.solutionsinformatiques.dz/?Applications-de-la-Biometrie-en-Algerie&fbclid=IwAR2Sy-19H131E8Kk1_uzzPeAm4C1MJ4vSprq4qGKdV5HdyveK4sr_rZf1Pw&lang=fr Visité le 02/06/2020

[4] : UML un outil pour le génie Logiciel, Mahdaoui Latifa, Ghenaiet Née Abdat Nabila, ISBN : 978-9947-850-01-5, page 36

[5] : http://www.journaldunet.com/solutions/securite/analyses/07/0917-9-etapes-securiser-sgbd.shtml visité le 03/06/2020

[6] : https://tel.archives-ouvertes.fr/tel-01750356 Visité le 15/06/2020

[7] : Chapitre 3 sur les Réseaux structurés, BELHOUCINE Amin, Enseignant à l'université de Tlemcen

[8] : Conception et réalisation d'une ferme intelligente, BENMANSOUR Zine-El Abidine, BENABED Abdel-Kader Djallal, Université Abou Bekr Belkaid

[9] : Conception et réalisation d'une plateforme Web dédiée à la résolution des problèmes industriels ,Mimouni Younes, Toualbia Abderrahmane, Université Abou Bekr Belkaid Tlemcen

[10] : Conception et réalisation d'un modèle de regroupement d'apprenants basé sur une classification multi-label, ZIAYA Marwa, Université de 8 Mai 1945 – Guelma -

[11] : https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard visité le 27/06/2020

[12] : https://www.anthedesign.fr/webdesign-2/pictogramme/ visité le 03/07/2020

[13] : https://phgarin.wordpress.com/2008/07/27/liste-de-mesures-de-securite-informatique/?fbclid=IwAR1kpPTrwHIr5FaHyt7PeBoUVB60jSKGCM6hS_qjjJrYtyWs7Ds31FFmrzo visité le 04/07/2020

Liste des figures

Liste des tableaux

Liste des abréviations

A :

AES : Advanced Encryption Standard

APP-UID : Application Unified IDentifer

AJAX : Asynchronous JavaScript And Xml

E :

eBPF : Extended Berkeley Packet Filter

H:

HSPL: Hidden Source Programming Languages

I:

IE: Informatics Elections

P:

PHP: Hypertext Preprocessor

S:

SCP: Self Communication Port

SSH: Secure Shell

SISP: Super Information Security Protocol

T:

TCP: Transmission Control Protocol

V:

VAO: Vote Assisté par Ordinateur

VPN: Virtual Personal Network

Abstract

Large-scale elections cost countries a large budget plus they can be not transparent for not designated candidates. Therefore, we realized an application that informs voting focusing on security algorithms that work with the principle of verifying the source with a very small negative error rate to ensure the transparency of the elections. The program also contains high-definition surveillance systems that identify the attacker while the attack took place during the elections. This program allows for election in polling centers that contain computers equipped with fingerprint readers, show results, and perform statistics on them.

Keywords:

Integrity, Traceability, Authentication, Security, Biometrics, Cryptography, Election, Anonymity

Résumé

Les élections à grande échelle coûtent aux pays un budget important et elles peuvent mettre en doute la transparence pour les candidats non élus. Par conséquent, notre projet vise à réaliser une application qui automatise le vote, en se concentrant sur des algorithmes de sécurité qui fonctionnent avec le principe de vérification de la source, à très faible taux d'erreur (négatif) pour assurer la transparence des élections. Également, le programme contient des systèmes de surveillance, à grande précision, et qui identifient l'attaquant au cours des élections. Ce programme permet l'élection dans les bureaux de vote qui contiennent des ordinateurs équipés de lecteurs d'empreintes digitales et affiche les résultats, en réalisant des statistiques à leur sujet.

Mot clés :

Intégrité, Traçabilité, Authentification, Sécurité, Biométrie, Cryptographie, Election, Anonymat

ملخص

تكلف الانتخابات ذات نطاق واسع للدول ميزانية كبيرة، بالإضافة إلى أنها يمكن أن تكون محطة شك بشأن الشفافية المترشحين غير الناجحين .ولهذا فان مشروعنا يعمل على تحقيق تطبيق يقوم بمعلوماتية التصويت يتركز على خوارزميات أمنية تعمل بمبدأ التحقق من المصدر بنسبة خطئ سلبي ضئيلة جدا لضمان شفافية الانتخابات. كما يحوي البرنامج على أنظمة ترصد عالية الدقة تقوم بتحديد هوية المهاجم في حين تم الهجوم في ظروف سير الانتخابات.يتيح هدا البرنامج الانتخاب في مراكز اقتراع تحوي حواسيب مجهزة بقارئات بصمات الأصابع وإظهار النتائج والقيام بالإحصاء عنها.

الكلمات المفتاحية :

النزاهة ، التتبع ، المصادقة ، الأمان ،البيومتري ، التشفير ، الانتخابات ، إخفاء الهوية