RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ MOHAMED BOUDIAF - M'SILA

FACULTÉ : MATHÉMATIQUES ET INFORMATIQUE

DÉPARTEMENT : INFORMATIQUE

N° :……

DOMAINE : MATHÉMATIQUES ET INFORMATIQUE

FILIERE : INFORMATIQUE

OPTION : RTIC

Mémoire Présenté Pour L'obtention Du Diplôme

De Master Académique

Par: Yousfi Izzeddine

THEME

Conception et réalisation d'un système de vote à distance. Cas d'étude : Département d'informatique

Soutenu publiquement devant le jury composé de :

Mr : Chikouche Nourddine	Université M'SILA	Président
Mr : Mehenni Tahar	Université M'SILA	Encadreur
Ms : Saoudi Lalia	Université M'SILA	Examinateur

Année Universitaire 2020/2021

Dédicace

Je dédie Ce mémoire A mes chers parents

ma mère et mon père

Pour leur patience, leur amour, leur soutien et

leurs encouragement. A mes frères.

A mes amies et mes camarades.

Sans oublier tous les professeurs que ce soit du

Primaires, du moyen, du secondaire ou de

L'enseignement supérieur

Y. Izzedddine

Remerciements

Avant tout nous remercions dieu le tout puissant qui nous a donné la force, la patience et le courage pour qu'on puisse accomplir ce modeste travail.

Nous remercions profondément notre encadreur monsieur **Tahar Mehenni** pour ses suivis et ses précieuses orientations dans notre travail et Nous voudraient vous remercier pour tous vos conseils et vos remarques intéressantes.

Nous exprimons nos reconnaissances à tous personnes qui a contribué de près ou de loin à l'achèvement de ce

travail; nos enseignants, nos amis, nos collègues de Faculté des Mathématiques et de l'Informatique.

Nous remercions également les membres de jury d'avoir accepté juger ce modeste travail

Y. Izzedddi

Table de matières

Liste des figures

Liste des Tableux

INTRODUCTION GÉNÉRALE

L'Internet a connu une croissance exponentielle cette dernière décennie. Les entreprises, les administrations publiques, les groupes de la société civile et les citoyens dépendent tous de l'Internet pour faire des affaires, du réseautage, de la recherche et maintes autres activités.

Aujourd'hui, on peut effectuer sur Internet des opérations bancaires, des achats ou des dons, signer des pétitions, présenter des demandes de permis et payer ses impôts. Parce qu'il peut transformer les modes de prestation de services, notamment en améliorant la communication et l'accès à l'information, et parce qu'il peut créer ou élargir des espaces participatifs, l'Internet a aussi suscité de l'intérêt comme facteur d'accessibilité au processus électoral.

En outre, du fait qu'il influence d'autres aspects de la vie politique, comme les campagnes électorales, les collectes de fonds, le recrutement de membres, les manifestations, le lobbying et l'accès à l'information pour les médias et les citoyens, l'Internet prend de plus en plus d'importance dans le domaine électoral et continuera sans doute d'avoir un grand impact sur la nature de la démocratie dans le monde. [1]

Avec l'émergence du concept de « démocratie électronique », il peut être utile d'explorer davantage la capacité de l'Internet d'améliorer le processus électoral pour les partis, les groupes, l'administration électorale et, bien sûr, les citoyens. Cependant, les préoccupations entourant le vote par Internet sont encore nombreuses, principalement en ce qui concerne la confiance du public à l'égard de la sécurité du processus de vote.

L'une des applications qui devrait profiter actuellement de ces avancées technologiques est le vote. En effet, les élections et les référendums traditionnels nécessitent le déplacement de tous les participants au vote or, il est difficile de convaincre tout le monde de faire le déplacement alors qu'il serait si facile de voter de chez soi, de façon électronique.

Les avantages seraient multiples : un plus grand nombre de participants grâce à l'aisance de cette opération impliquée par le non-déplacement et la simplicité du processus, le dépouillement automatisé et donc plus rapide, le coût d'organisation réduit à cause de l'élimination des dépenses associées à l'établissement des bureaux de vote et le personnel qu'ils requièrent, etc … .

Sera-t-il possible de numériser le secteur électoral tout en assurant la sécurité et la transparence du processus électoral ?

Dans ce mémoire , nous en apprendrons plus sur le vote électronique

- **Le premier chapitre :** présente un aperçu général sur le vote électronique.
- **Le deuxième chapitre :** donne l'état de l'art des travaux précédents et des expériences de certains pays en matière de vote électronique et explique certains systèmes de vote électronique.
- **Le chapitre 3** : présente notre système de vote, notamment sa conception en s'appuyant sur de diagrammes UML.
- **Le chapitre 4 :** se consacre à la présentation des différents outils utilisés pour la réalisation de notre projet. Il donne aborde ensuite le coté réalisation de notre projet, avec des exemples d'interfaces les plus importants.

CHAPITRE 1 :

VOTE

ELECTRONIQUE

1. Introduction :

Le vote par internet est assimilé à un mode de vote par correspondance. Les électeurs procèdent depuis n'importe quel ordinateur connecté à internet, que cet ordinateur soit chez eux, au travail, dans un lieu public ou un cybercafé. Il faut se connecter sur le site officiel de vote hébergé sur l'ordinateur du bureau centralisateur (le serveur). Après les phases d'identification et d'authentification (à l'aide d'un identifiant et d'un mot de passe généralement reçus au préalable par courrier postal), l'électeur peut faire son choix. Après confirmation, il reçoit un accusé de réception de son vote (cet accusé de réception ne mentionne pas le sens du suffrage). Les échanges d'informations empruntent le réseau internet.

L'ordinateur qui fait office de serveur se charge de la tenue de la liste des émargements, de la collecte des votes au fur et à mesure de leur réception, et du dépouillement à la fin de la période de vote

Dans ce chapitre, nous parlerons du vote électronique en général, définition , propriétés et les modules .... etc

2. Le vote électronique (définition et propriétés)

2.1. Définition :

Le vote électronique est un exemple d'application distribuée qui permet aux élections d'avoir lieu sur des réseaux informatiques ouverts [2] . Dans cette application un ensemble de votants envoie leurs bulletins à travers le réseau à un centre de dépouillement virtuel responsable de la réception, validation, et classification des bulletins.

D'une manière générale, les participants impliqués dans une élection électronique sont un collectif d'électeurs et un ensemble d'autorités de vote. Le nombre et l'utilité de ces autorités sont variables, ils dépendent du schéma de vote considéré [2].

Le scénario d'une élection électronique peut être divisé en trois phases :

- **Phase d'enregistrement** : Durant cette première étape, l'autorité de vote crée la liste électorale de toutes les personnes éligibles qui sont enregistrées pour cette opération de vote et la publie à travers le réseau.

- **Phase de vote :** Cette phase permet aux votants d'envoyer leurs bulletins de vote en utilisant les facilités de communication offertes par le réseau.

- **Phase de décompte :** A la fin de la phase de vote, l'autorité arrête la réception des bulletins et le processus de décompte des résultats est déclenché. Finalement, les résultats sont publiés et mis à la disposition des votants à travers le réseau.

2.2.Propriétés :

L'application du vote étant destinée à être exécutée sur le réseau, un bon système de vote électronique doit assurer quelques propriétés qui définissent des exigences concernant sa sécurité et son implémentation [3] [4]. Dans ce qui suit, nous allons définir les exigences de sécurité dont nous tiendrons compte lors de la conception du système.

Précision : Une élection est précise si elle vérifie les exigences suivantes :

- Un vote ne doit pas être altéré, par conséquent les résultats du vote ne doivent pas être modifiés en ajoutant des votes invalides ou en changeant le contenu des bulletins par exemple (intégrité).
- Un vote valide doit être compté.
- Un vote invalide ne doit pas être compté.

Démocratie : Cette propriété est assurée si :

- Seuls les votants éligibles peuvent voter.
- Chaque votant ne peut voter qu'une seule fois. La propriété de démocratie est généralement liée à l'intégrité de la liste électorale (liste des votants éligibles). Pour cela, quelques mécanismes supplémentaires doivent être ajoutés pour empêcher l'administrateur de cette liste de casser cette propriété.

Confidentialité : Nous qualifions de vote confidentiel, un vote dans lequel :

- ni l'autorité du vote ni personne d'autre ne doit pouvoir faire le lien entre un votant et son vote (anonymat) : l'anonymat constitue probablement la pierre angulaire de tout système de vote électronique [5].
- aucun votant ne peut prouver qu'il a voté dans un chemin particulier : ce dernier facteur de confidentialité est aussi important pour la prévention contre l'achat du vote, en effet les électeurs ne peuvent vendre leurs votes que s'ils sont capables de prouver à l'acheteur qu'ils ont réellement voté d'après leurs vœux.

Vérifiabilité : Il existe deux définitions de cette propriété, la vérifiabilité universelle et la vérifiabilité individuelle. Un système de vote est universellement vérifiable si toute personne peut indépendamment vérifier que tous les bulletins ont été comptés correctement. Un système de vote est individuellement vérifiable (définition plus faible) si chaque votant peut indépendamment vérifier que son propre bulletin a été correctement compté [6].

Résistance à la collusion :

- aucune entité électorale (serveur participant au vote), ou aucun groupe d'entités, ne peut introduire de votes ou empêcher un citoyen de voter. Si toutes les entités font partie de la conspiration, alors cette propriété n'est pas assurée. [7]

Disponibilité :

- le système fonctionne correctement durant toute la période de vote .
- chaque votant peut accéder au système durant toute la période de vote.

Capacité de reprise :

- le système permet à un votant ayant interrompu le processus de vote de reprendre où il en était, ou de recommencer toute la procédure. [8]

Robustesse :

- le système est capable de mettre en échec les tentatives d'usurpation d'identité des serveurs, ainsi que les tentatives d'utilisation d'applets non officielles.

L'anonymat :

- Pour la plupart des élections, l'anonymat du vote est requis. Cela veut dire qu'il doit être impossible de savoir comment un votant particulier a voté, à moins que ce ne soit révélé par le résultat (par exemple si le vote est unanime). Selon l'enjeu des élections, l'anonymat peut ne pas être suffisant. Afin d'éviter la coercition et l'achat de vote, il est également nécessaire que le protocole soit résistant à la coercition : il doit être impossible d'enregistrer des informations qui pourraient convaincre une tierce personne de la valeur du vote [9]

Avant d'expliquer le schéma de vote proposé et comment celui-ci va essayer de remplir les exigences de sécurité citées auparavant, nous allons brièvement présenter les principaux types de protocoles de vote décrits dans la littérature.

3. Synthèse et critiques des protocoles de vote électroniques

Les premiers protocoles de vote électronique n'utilisent pas de techniques cryptographiques. Ces protocoles sont basés généralement sur deux autorités de vote : la première est utilisée pour l'authentification des votants enregistrés, et la deuxième chargée de la collection des bulletins et le décompte des résultats. Malgré leur simplicité, ces protocoles présentent des inconvénients majeurs. En effet, ils ne répondent pas à la majorité des propriétés citées précédemment [10].

Dès lors, des protocoles utilisant les mécanismes cryptographiques ont été proposés. Ces derniers introduisent le chiffrement pour assurer la confidentialité du vote, et la signature numérique pour assurer l'authentification des votants et garantir ainsi qu'ils ne peuvent voter plus d'une fois. Pour garantir l'anonymat des votants, certains de ces protocoles se sont basés sur l'utilisation de deux autorités pour séparer les deux tâches d'authentification du votant et le décompte de son bulletin. Cependant le problème d'anonymat s'est toujours posé à cause du risque de collusion existant entre les deux autorités pouvant ainsi déterminer qui a voté pour qui [10].

Par conséquent, et afin de dissocier complètement le votant de son vote, la technique de signature en aveugle introduite par David Chaum en 1982 a été utilisée [7]. Cette technique permet à l'autorité chargée de l'authentification des votants de signer leurs bulletins sans avoir la moindre idée sur le contenu. De cette manière, le risque de collusion entre les deux autorités est éliminé : la première n'ayant aucune information sur les bulletins qu'elle a validé. Ceci est similaire au fait de placer un document avec une feuille de papier Carbonne dans une enveloppe. Si quelqu'un signe cette dernière, le document sera signé aussi, la signature reste alors attachée au document même s'il est retiré de l'enveloppe. Parmi les protocoles de vote basés sur la signature en aveugle, nous distinguons les travaux de Fujioka, Okamoto et Ohta qui ont défini un protocole de vote utilisant deux autorités centrales et est à la base du protocole Sensus décrit dans [11].

4. Les modules de système de vote

Pour mener une opération de vote, i-vote utilise quatre modules représentant respectivement le votant, l'ACL, l'ACD, en plus du module qui représente l'organisateur de

l'élection et qui est chargé d'automatiser la phase d'inscription et la construction dynamique du bulletin de vote. [12]

4.1.Le module Organisateur

Le module Organisateur est invoqué par l'administrateur de l'opération de vote. Ce dernier doit introduire un mot de passe afin de pouvoir l'exécuter.

En plus de la phase d'inscription des votants, le module Organisateur est responsable des préparations nécessaires au vote. Son rôle se résume essentiellement en :

– la construction du bulletin de vote : en utilisant HMTL comme langage de construction, l'administrateur du vote définit le modèle du bulletin de vote qui sera employé durant l'élection. Ce modèle dépend des spécificités que présente chaque opération de vote tel que son genre (élection, referendum, . . .), le nombre de choix suggéré pour le vote, etc.

– le module Organisateur est également utilisé pour préparer la liste de population, déclencher et arrêter les différentes phases de l'élection organisée.

4.2.Le module ACL

Le module ACL est chargé de l'accomplissement de la phase de validation tout en garantissant qu'un seul bulletin sera validé pour chaque votant enregistré.

4.3. Le module ACD

Le module ACD est responsable de l'étape de collection des bulletins de vote et le décompte des résultats ainsi que leur publication.

4.4. Le module Votant

Ce module fonctionne comme étant un agent du votant. Il doit pouvoir :

- Présenter un bulletin de vote lisible au votant (utilisation d'une interface graphique ou textuelle).
- Prendre en charge les votes des électeurs.
- Exécuter toutes les opérations cryptographiques qui doivent être effectuées par le votant.
- Obtenir et recevoir les validations nécessaires et les accusés de réception.
- Délivrer le bulletin de vote aux différentes autorités (ACL, ACD).
- Vérifier les résultats du scrutin et éventuellement protester en cas d'erreur

5. Types de vote par Internet :

Il existe trois types de vote électronique, qui sont décrits comme suit:

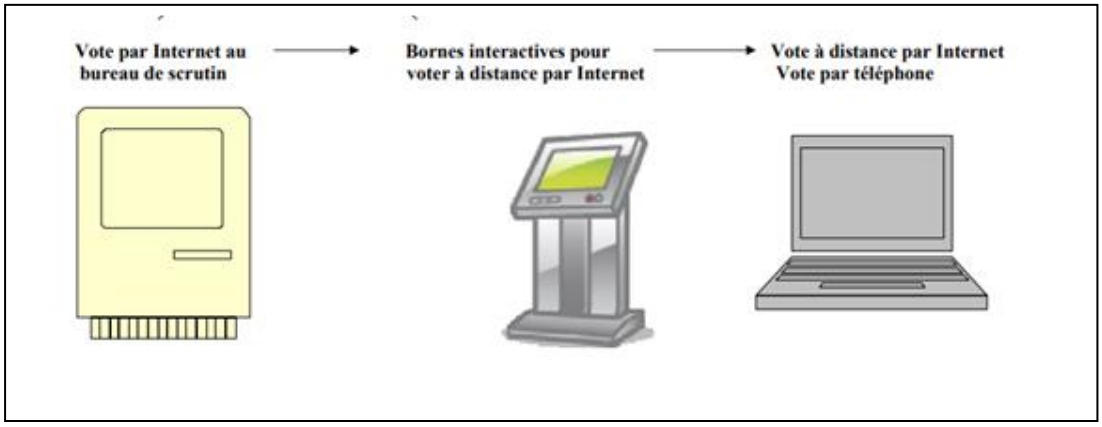

FIGURE 1.1 Types de vote par Internet .

6. Conclusion

Dans ce chapitre nous avons présenté un aperçu général sur vote électronique, afin d'avoir une vision sur les outils et les protocoles pouvant servir au développement de notre projet à partir des objectifs tracés pour la réalisation de ce mémoire, et dans le chapitre suivant, Nous présenterons les travaux précédents dans le vote électronique .

CHAPITRE 2 :

ETAT DE L’ART

1. Introduction :

Les systèmes mis en œuvre sont très divers, les approches des États aussi, mais, dans tous les cas, les informations sont rares et la plupart du temps très partielles. Nous n'avons trouvé aucun document public permettant d'avoir une description précise d'une des applications de vote sur internet en service. De nombreuses informations restent donc inconnues comme, par exemple, les langages de programmation et les systèmes de gestion de bases de données utilisés, la structure des programmes et du stockage des données, les systèmes de contrôle des communications par internet, etc. Dresser un tableau synoptique des expériences en les comparant sur un ensemble de critères s'est révélé irréalisable. Le panorama ci-dessous réalise la synthèse et l'analyse des informations qui ont pu être collectées.

Le vote à distance par internet a été peu utilisé. Seul l'Estonie l'a généralisé à l'ensemble de ses votants, sans en rendre toutefois l'utilisation obligatoire. D'autres pays l'ont testé sur de petits effectifs d'électeurs.

Et c'est ce dont nous parlerons dans ce chapitre

2. Australie :

2.1.Le système iVote utilisé en New South Wales (Australie) :

2.1.1. Procédure de définition et de sélection du système de vote *:*

L'état de New South Wales (NSW) offre, depuis 2011, la possibilité à certains groupes de personnes de voter par internet, en complément des options de vote par téléphone, par courrier, et en personne.

L'introduction du vote par internet en NSW a été étudiée suite à un jugement rendu en 2008, affirmant que la Commission électorale du NSW avait agi de manière discriminatoire en n'offrant pas à une personne aveugle les moyens de voter de manière indépendante et secrète, comme proposé à la majorité de l'électorat [13] . Sur demande du Parlement de NSW, la Commission électorale a étudié en 2010 la possibilité d'offrir une option de vote par internet qui permettrait de voter de manière indépendante et secrète aux personnes qui ne pouvaient le faire par les moyens de vote disponibles. Sur base d'un rapport positif [14] et de premiers contacts pris avec des vendeurs, la décision a été prise de mettre en place une solution de vote par internet et par téléphone pour les élections générales de 2011.

Le choix du système de vote et de son processus de mise à jour, se sont déroulés sur base d'une suite de prises de contact avec des fournisseurs potentiels, de demandes publiques d'information (RFI) et d'appels d'offre (RFP) [15] .La conception, la mise en œuvre, et les mises à jour du système de vote, baptisé iVote, ont été confiées à la société Scytl pour toutes les élections qui ont eu lieu depuis 2011. Le système a connu un certain nombre d'évolutions, et la description qui suit est basée sur la version du système utilisée en 2019 [16] .

2.1.2. Organisation d'une élection :

Le système de vote par internet est composé de deux composants principaux :

1. Un système d'inscription des électeurs, qui appartient et est géré par la Commission électorale, et est hébergé par un fournisseur tiers.

2. Le système de vote iVote proprement dit, qui inclut la plate-forme de vote et celle de vérification des votes, est la propriété de Scytl, et est déployé sur les serveurs d'autres fournisseurs.

Inscription. L'usage de iVote étant limité à une portion relativement restreinte de la population (quelques centaines de milliers de personnes, sur base de conditions spécifiques), les votants désireux de voter par iVote doivent soumettre une demande d'inscription à la Commission électorale. Lors de cette inscription, le votant choisit aussi un mot de passe (ou code PIN) qui servira à l'identification. Si l'inscription du votant est autorisée, le votant reçoit un identifiant iVote ("iVote number"), qui peut lui être transmis par la Commission électorale via différents canaux : SMS, email, courrier postal, ou téléphone. L'identifiant de vote et le mot de passe du votant sont aussi utilisés pour protéger une clé de signature qui sera utilisée par le votant pour signer son bulletin de vote.

Préparation du vote. Avant le début de l'élection, le Bureau électoral génère un certain nombre de clés qui sont stockées sur des cartes à puce et, conjointement, garantissent la confidentialité du vote. Les bulletins de vote sont aussi définis, en ce compris sous la forme de fichiers audio.

Vote. Les votants dont l'inscription a été confirmée peuvent voter à partir du site web de l'élection. Ils s'authentifient sur base de l'identifiant et du mot de passe générés durant la procédure d'inscription, confirment qu'ils n'ont pas déjà voté par ailleurs, et soumettent leur bulletin de vote chiffré à l'aide de la clé publique correspondant aux clés secrètes générées par le Bureau électoral et signé. Le votant reçoit alors un reçu dérivé de son bulletin de vote ainsi

qu'un QR code qui peut être utilisé lors d'étapes de vérifications ultérieures détaillées ci-dessous.

2.1.3. Utilisabilité :

Un des objectifs initiaux de iVote était d'offrir un canal de vote complémentaire au vote papier, afin de permettre à davantage de personnes de voter sans assistance. Le système de vote par internet a ainsi été introduit en même temps qu'une option de vote par téléphone. En pratique, il s'est avéré que ces canaux de vote ont été bien plus largement utilisé par des votants se trouvant hors du NSW que par des personnes en situation de handicap, qui utilisent ces canaux moins que cela n'avait été anticipé[17] . Le vote par téléphone n'a aussi obtenu qu'un très faible succès: en 2015 et en 2019, plus de 99% des personnes s'étant inscrites pour voter par internet ou par téléphone ont voté par internet.

2.1.4. Garanties d'intégrité

Identification des électeurs : Comme indiqué plus haut, tout utilisateur d'iVote doit préalablement s'inscrire et initialiser un mot de passe qui pourra être utilisé conjointement à l'identifiant iVote qui est fourni en cas de validation de l'inscription. L'inscription se fait en ligne, et la preuve d'identité se fait au moyen de documents reconnus par le service de vérification de documents (DVS) géré par l'état de NSW: il n'y a pas de document d'identité officiel obligatoire en Australie, mais un projet de création de carte d'identité électronique est en cours.

2.1.5. Fidélité du bulletin de vote

Lorsqu'un électeur vote, son navigateur produit un bulletin de vote chiffré et signé et l'envoie vers le serveur de vote. Afin de permettre au votant de vérifier que le bulletin de vote que son navigateur a transmis a été correctement reçu et reflète son intention de vote, plusieurs options sont proposées.

Le votant est ainsi invité à installer une App de vérification sur son smartphone et, au moment de la soumission du bulletin chiffré, le navigateur présente aussi au votant un QR code qui peut être scanné au moyen de l'App en question. Ce QR code contient la graine à partir de laquelle sont dérivées toutes les valeurs aléatoires utilisées pour la production du bulletin de vote. Sur base de cela, et de l'identifiant et du mot de passe du votant, l'App va alors recalculer le bulletin de vote du votant, télécharger le bulletin de vote enregistré sur le serveur, "déchiffrer" ce bulletin, et montrer au votant les choix qu'il contient, pour

vérification. En cas de vote par téléphone, la même procédure est effectuée sur un serveur à distance, et le vote contenu dans le bulletin enregistré est lu au votant.

La première option (emploi d'une app) a le mérite de garantir au votant que son vote a été correctement enregistré, même si la machine utilisée pour voter était infectée par un malware, et évite que le vote ne se trouve exposé en clair aux serveurs de vote. La seconde option vise les mêmes objectifs de vérifiabilité, mais est plus sensible au niveau de la confidentialité du vote, dans le mesure où celui-ci se retrouve en clair sur un serveur et transmis par téléphone. Par ailleurs, outre le QR code mentionné plus haut, le votant reçoit une empreinte digitale de son bulletin chiffré (un haché). Cette empreinte peut être utilisée, plus tard, pour vérifier que le vote est bien enregistré dans le système, sans avoir été modifié.

2.1.6. Suivi des bulletins de vote et du décompte

Lorsque la phase de vote est terminée, une étape de vérification des urnes démarre. On s'assure ainsi que:

1. chacun des bulletins de vote se trouvant dans l'urne correspond bien à un votant inscrit;
2. le système d'audit de iVote (un ensemble de serveurs distincts de ceux qui reçoivent et stockent les bulletins de vote) confirme qu'aucun bulletin de vote n'a été modifié ou supprimé de l'urne;
3. tous les éléments cryptographiques internes des bulletins de vote sont valides (signatures correctes, preuves à divulgation nulles valides, …).

Une fois ces vérifications terminées, les bulletins de votes sont anonymisés : on retire les signatures et les preuves de validité, et les chiffrés passent à travers un mixnet, qui mélange et transforme les chiffrés des bulletins de vote, tout en prouvant que le résultat de ces opérations n'a pas changé le contenu des votes. Enfin, les cartes à puce des porteurs de clés sont rassemblées, et les bulletins de vote anonymisés sont déchiffrés, à nouveau de manière vérifiable. Le décompte est alors réalisé au départ des bulletins de vote ainsi obtenus en clair

2.1.7. Procédures de résolution de conflits

Au cas où un votant choisit de vérifier que son bulletin de vote a été correctement enregistré et reflète son intention de vote, il pourrait arriver qu'un problème soit détecté. Il n'est

évidemment pas possible de déterminer si on est face à un dysfonctionnement du système de vote, ou face à un votant qui a fait une erreur ou est de mauvaise foi. Le votant confronté à de telles difficultés est invité à contacter le service de support d'iVote, et se verra offert la possibilité d'obtenir un nouvel identifiant iVote et de voter à nouveau. En même temps, l'identifiant précédent et l'éventuel bulletin de vote associé sont invalidés.

2.1.8. Garanties de confidentialité

La confidentialité du vote reste toujours relativement limitée lors d'un vote à distance, ne seraitce que parce qu'il est impossible de garantir que la personne qui vote est seule à voir son bulletin de vote. La confidentialité du vote repose ici sur:

1. l'honnêteté de l'électeur,
2. l'honnêteté de l'ordinateur que le votant emploie pour exprimer son vote,
3. l'honnêteté du serveur de vote (qui aurait la possibilité de transmettre un client de vote malicieux),
4. l'honnêteté de l'appareil employé pour vérifier la correction du bulletin de vote (via le mécanisme de QR code),
5. l'honnêteté de l'App employée pour vérifier la correction du bulletin de vote
6. l'honnêteté d'au moins un des serveurs faisant partie du mixnet,
7. l'honnêteté d'au moins une des personnes dépositaires des cartes à puce contenant les clés de déchiffrement,
8. l'honnêteté de la machine sur laquelle ces clés de déchiffrement sont rassemblées pour l'opération de déchiffrement.

Si ces conditions sont satisfaites, alors aucun résultat partiel de l'élection ne pourra être obtenu tant que le déchiffrement n'a pas été réalisé, et les votes resteront secrets. Le système ne divulgue pas non plus de liste des personnes ayant voté, ce qui peut potentiellement faciliter des attaques visant à "bourrer les urnes" en y ajoutant des bulletins au nom de personnes qui n'auraient pas voté.

Finalement, un votant qui souhaite mettre son vote en vente, ou est victime de coercition, pourra par exemple permettre à un tiers de réaliser la procédure d'inscription en son nom et de voter à sa place. Cependant, le votant pourra toujours contacter le service de support d'iVote, invoquer que son vote a été transmis sous contrainte pour pouvoir invalider le bulletin qui aurait été soumis par le tiers. Il recevra alors de nouveaux identifiants qui lui permettront de transmettre un nouveau bulletin.

2.2.Sécurité et audit du développement du système

2.2.1. Analyses du protocole

Avant les élections de 2019, des auditeurs ont été engagés pour examiner le système, au sein du monde académique et du secteur privé (notamment, le groupe DemTech au Danemark). Par ailleurs, une partie du code source de iVote a été rendu disponible pour audit, sous de strictes conditions de confidentialité (tant vis-à-vis de Scytl que vis-à-vis de la Commission électorale du NSW), et ce dès janvier 2019. Il est difficile d'évaluer si ces clauses de confidentialité ont permis une diffusion et évaluation réelle du code, et elles ont certainement dissuadé certains experts du monde académique d'accéder au code. En juin 2019, les conditions d'accès aux parties du code source de iVote ont été assouplies par Scytl, permettant notamment de rendre publique toute vulnérabilité qui aurait été détectée 45 jours après en avoir informé Scytl et la Commission électorale du NSW. A notre connaissance, aucune preuve de sécurité du protocole iVote n'a été réalisée, ou requise.

2.2.2. Évaluation du système

Il n'y a pas eu à proprement parlé de test d'intrusion organisé pour le système iVote. Des vulnérabilités ont cependant été identifiées et ont fait l'objet de publicité dans la presse. En 2015, Halderman et Teague [18] ont effectué un audit indépendant (et non sollicité) du système iVote, principalement sur base de la plate-forme de démonstration. Cette analyse a mis en évidence le fait que iVote faisait usage d'un outil de mesures statistiques qui était chargé dans le navigateur du votant en même temps que le reste du système de vote, au départ d'un site web tiers, dont la sécurité était faible. Il était alors possible, pour un attaquant capable d'intercepter le trafic internet d'un votant, d'injecter dans la page web un code arbitraire, permettant au minimum de violer le secret du vote et, dans le pire des cas, de modifier le vote par la même occasion. Différents moyens de mettre en échec le protocole de vérification des bulletins de vote ont aussi été mis en évidence.

En mars 2019, différentes vulnérabilités du système sVote proposé pour usage en Suisse ont été identifiées, dans le cadre d'un processus de review public. Il est apparu que les élections générales du NSW étaient en cours au même moment, soulevant la question de la présence de ces mêmes librairies dans le système iVote, vu que les deux systèmes provenaient du même fournisseur. Il a ainsi été confirmé que certaines des faiblesses de sVote étaient présentes dans iVote, dont le code a dû être mis à jour en cours d'élection [19] .

Ceci illustre l'interdépendance qui est créée entre différents états proposant du vote par internet via un même fournisseur: la Suisse, qui a encouragé un processus d'évaluation public de son système de vote, hors de tout contexte d'élection, a permis la découverte, et la correction en urgence, d'une vulnérabilité dans le système iVote en cours d'élection, et ce dans un contexte où l'accès au code d'iVote n'était possible que sous des conditions restrictives [20] .

3. Estonie :

3.1.Système de vote par internet utilisé en Estonie :

Le système de vote par internet estonien a été inauguré en 2005 lors des élections municipales (une première mondiale), et est toujours en place à ce jour. Il a été utilisé lors de nombreuses élections : quatre élections locales, trois élections du parlement européen, et quatre élections parlementaires.

3.1.1. Organisation d'une élection :

Les électeurs utilisent leur carte d'identité électronique pour le vote. La carte d'identité estonienne est obligatoire pour l'ensemble de la population , et sert à la fois de document d'identification ainsi que de carte à puce. La carte à puce contient deux paires de clés accompagnées de certificats, l'une permettant à l'utilisateur de s'authentifier à distance de manière sûre, et l'autre de signer digitalement (supporté par l'infrastructure à clé publique du gouvernement estonien). Les électeurs chiffrent leur bulletin de vote à l'aide de la clé publique du système de vote (qui est par définition publiquement disponible), et le signent à l'aide de leur clé privée de signature.

Le système de vote est composé de différents serveurs, séparés physiquement, de manière à ce qu'aucune pièce d'équipement ne possède à la fois un bulletin de vote (et sa signature), et la clé privée centrale du système de vote. De plus, un système de registre garde la trace de l'entièreté du processus d'enregistrement et de comptabilisation des bulletins de vote. L'intégrité du vote est donc assurée par ces deux principes : séparation des fonctions et auditabilité des registres. La relation entre ces différents éléments est représentée dans la figure ci-dessous.

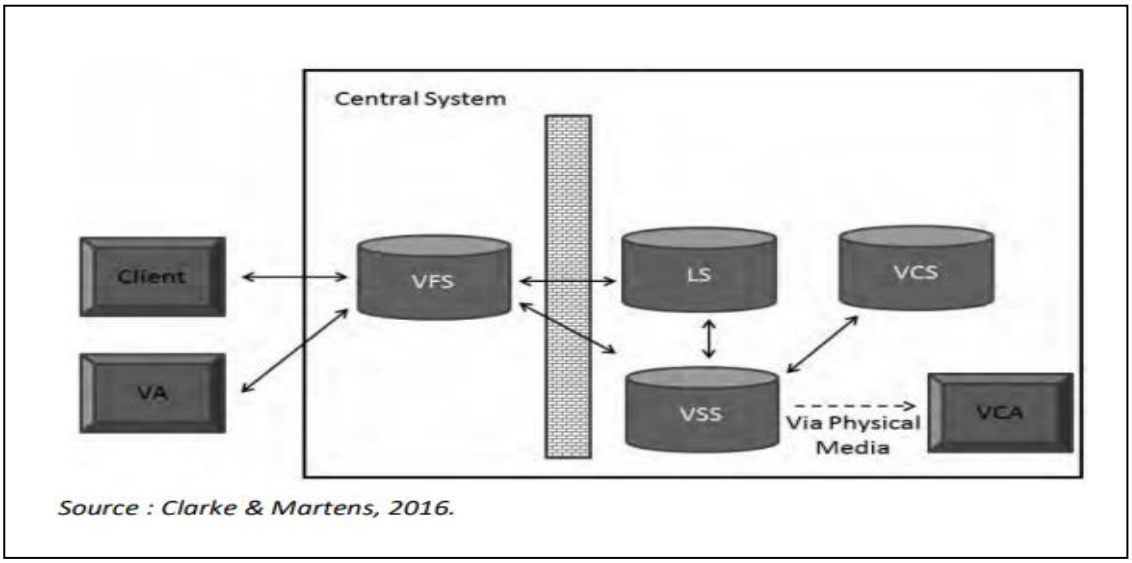

Figure 2.1 : La relation entre les éléments du système

3.1.2. Composants du système estonien de vote par Internet :

Les rôles de ces différents composants sont :

Client (application de vote) : l'application/client (Windows/Mac OS/Linux) que l'électeur utilise pour voter. • VA (Verification Application) : l'application/client (smartphone/tablette) que l'électeur utilise pour vérifier son vote.

- VFS (Vote Forwarding Server) : authentifie l'électeur, fait suivre chaque bulletin de vote au LS et VSS (est le seul serveur publiquement accessible). Contient également la liste des électeurs et des candidats. • LS (Log Server) : maintient un registre pour le VFS et le VSS.
- VSS (Vote Storage Server) : enregistre les bulletins de vote valides. Communique avec le VCS, qui vérifie la validité de la signature des bulletins de vote. Produit également un reçu pour l'électeur, et produit une liste de bulletins anonymisés pour le VCA. Gère également la suppression d'éventuels bulletins précédents, en particulier lors d'un vote en bureau de vote.
- VCS (Validity Confirmation Server) : vérifie la signature de chaque bulletin de vote, et fournit au VSS une attestation de validité. Le VCS est une entité indépendante du système de vote, et est également utilisé pour d'autres applications d'authentification et/ou de signature liées à la carte d'identité estonienne.

- VCA (Vote Counting Application) : déchiffre chaque bulletin de vote, et comptabilise les votes pour chaque district électoral. Le VCA n'intervient que lorsque la période de vote est terminée. Il reçoit les bulletins chiffrés du VCS par média physique (DVD), et tient son propre registre, séparé du LS.

3.1.3. Participation à une élection :

Pour chaque élection, le vote est ouvert pour une période de 1 à 6 jours (en fonction de l'élection) avant le jour de l'élection. Chaque vote peut être modifié autant de fois que souhaité (seul le vote final compte). Il est également possible de se rendre à un bureau de vote et d'y voter à nouveau pendant cette période (invalidant alors tout vote par internet fait au préalable et dans le futur). Ceci permet à l'électeur de voter à nouveau s'il a été influencé pendant son vote. En revanche, cela crée aussi la possibilité inverse où un électeur est forcé à voter à nouveau (en particulier si c'est peu de temps avant la date limite), ou est rendu incapable de voter à nouveau (par exemple en confisquant sa carte d'identité).

La procédure de vote, en situation normale, se déroule de la manière suivante :

L'électeur utilise l'application sur son ordinateur personnel, et s'authentifie au VFS à l'aide de sa carte d'identité et de son lecteur de carte. C'est une authentification à deux facteurs : possession de la carte, et connaissance du PIN (PIN1, pour authentification).

1. Le VFS détermine la liste des candidats valides correspondant à la région de l'électeur, et la communique à l'application.
2. L'électeur choisit un candidat. L'application chiffre le bulletin de vote (à l'aide de la clé publique du système de vote central).
3. L'application demande ensuite à l'électeur de signer le bulletin chiffré, à nouveau à l'aide de la carte d'identité et d'un PIN (PIN2, pour signature digitale). Le ballot chiffré et signé est alors envoyé au VFS, qui le fait suivre au VSS.
4. Le VSS contacte le VCS afin d'attester de la validité de la signature. Le cas échéant, le VCS produit une confirmation de validité signée, et le VSS stocke le bulletin de vote. Si la signature n'est pas valide, le VCS informe le VSS, qui en averti l'application (par le biais du VFS), et le processus s'arrête. 6. Si le bulletin est confirmé valide, le VSS vérifie si un bulletin pour le même électeur n'a pas déjà été enregistré. Si c'est le cas, le bulletin précédent est effacé.
5. Le VSS envoie un reçu à l'application (par le biais du VFS), et averti l'électeur du succès du processus. L'électeur peut dès alors vérifier son vote (procédure expliquée

par après). Une fois la période de vote terminée, la comptabilisation se déroule de la manière suivante :

6. Une liste des utilisateurs du vote par internet est imprimée depuis le VSS, pour chaque bureau de vote. Cette liste est comparée avec la liste des électeurs ayant voté physiquement sur place. Chaque vote présent dans les deux listes est supprimé du VSS (la priorité étant donnée au vote en bureau de vote).
7. Le VSS trie les bulletins de vote par candidat, en enlève leurs signatures, et les enregistre sur média physique (DVD), pour transfert au VCA.
8. Le VCA, lit la liste des bulletins de votes (depuis le média physique). Plusieurs fonctionnaires électoraux insèrent un dispositif USB dans le VCA. Ces dispositifs contiennent une "boîte noire transactionnelle" (ou HSM pour Hardware Security Module), qui contient la clé privée du système électoral central, ce qui permet de déchiffrer les bulletins de vote de manière sûre.
9. Le VCA vérifie ensuite que chaque bulletin déchiffré correspond à un candidat valide pour l'électeur associé. Le cas échéant, le total de votes du candidat est incrémenté de un. Une fois que tous les bulletins ont été ainsi traité, le compte final est imprimé.

Lors du processus de vote et de décompte, le LS et le VCA maintiennent plusieurs registres, permettant l'auditabilité de chaque bulletin de vote.

- LOG1 (LS) : numéro d'identification de l'électeur et emprunte numérique (hash) du bulletin de vote quand un vote est reçu (étape 5).
- LOG2 (LS) : numéro d'identification de l'électeur et raison de révocation en cas de vote précédent rendu obsolète par un nouveau vote (étape 6) ou par un vote en bureau de vote (étape 8).
- LOG3 (LS) : emprunte numérique des bulletins de vote avant d'être inscrits sur média physique (étape 9).
- LOG4 (VCA) : emprunte numérique du bulletin de vote si invalide lors du décompte (étape 11).
- LOG5 (VCA) : emprunte numérique du bulletin de vote si valide lors du décompte (étape 11).

3.1.4. Utilisabilité

Le logiciel utilisé durant le processus de vote électronique est disponible sur Windows, macOS et Linux. Le logiciel de vérification du vote est une application disponible sur

smartphone et tablette. Ceci garantit que deux appareils indépendants seront utilisés lors du vote.

3.1.5. **Garanties d'intégrité** :

Identification des électeurs : L'électeur est authentifié par le certificat intégré dans la puce de sa carte d'identité, et par la connaissance du PIN1 de cette puce (celui lié à l'authentification).

Fidélité du bulletin de vote : Chaque utilisateur du vote électronique peut vérifier son vote. Cette vérification est possible jusqu'à 30 à 60 minutes (en fonction du type de l'élection) après le vote. Cela permet donc à l'électeur de vérifier que le vote enregistré sur le serveur de vote est le bon (vérification individuelle), tout en protégeant la confidentialité de celui-ci après cette courte période. L'application de vérification ne produit pas de reçu. Un vote peut être vérifié jusqu'à trois fois. Il n'est par contre pas possible pour l'électeur de vérifier directement si, lors du compte final, son propre vote a été correctement comptabilisé. Comme déjà mentionné, un électeur a la possibilité de voter à nouveau, autant de fois qu'il désire, jusqu'au jour de l'élection.

Le processus de vérification est le suivant. Lorsqu'un vote est confirmé par l'application de vote sur ordinateur, un message confirmant la réception du vote est affiché, ainsi qu'un QR-code permettant la vérification du vote. Le QR-code peut alors être scanné par l'utilisateur à l'aide de l'application sur smartphone/tablette. Cette application contacte alors le VFS et lui demande le vote chiffré correspondant à l'électeur, stocké sur le VSS (si la période de vérification est écoulée, le VFS refuse de répondre à la demande). Le candidat correspondant au vote est déterminé en calculant un bulletin de vote pour chaque candidat valide, et à l'aide d'un nombre aléatoire contenu dans le QR-code (ce nombre aléatoire est généré lors du vote et est contenu dans chaque vote chiffré). Seul le candidat lié au vote enregistré correspondra à celui généré depuis le QRcode, et l'application affiche son nom.

Étant donné que l'application sur smartphone est liée à l'identité de l'électeur, le smartphone connait le lien électeur-vote. Par contre, le serveur de vote n'a pas la possibilité de connaître le contenu du vote. Le processus de détermination du candidat (en itérant sur l'ensemble des candidats possibles) permet d'éviter une attaque par phishing simple, où une application malicieuse demanderait directement l'information sur le candidat potentiel à l'électeur lors de la vérification.

Ce processus ne protège en revanche pas contre des attaques plus complexes, par exemple par collusion entre une application malicieuse de vérification et un serveur de vote compromis, ou une situation dans laquelle le VSS est compromis, et le vote envoyé lors d'une demande de vérification est différent de celui enregistré. Cependant en pratique ces attaques sophistiquées ont de grandes chances d'être détectées si elles sont employées à grande échelle.

3.1.6. Qualité du décompte :

Une fois le décompte effectué, il est possible d'effectuer la vérification suivante :

- Le contenu du LOG1 (votes reçus) doit correspondre à la somme de ceux du LOG2 (votes rendus obsolètes) et du LOG3 (votes envoyés au VCA pour comptabilisation).
- Le contenu du LOG3 (votes à comptabiliser) doit correspondre à la somme de ceux du LOG4 (votes invalides) et du LOG5 (votes valides).

Cette vérification est donc capable de détecter des incohérences, si elles apparaissent. En revanche, si le système de registre a été compromis, il peut ne pas être possible de détecter une fraude.

3.1.7. Garanties de confidentialité :

Une fois que le résultat de l'élection a été déterminé avec certitude, les disques durs des serveurs liés au système de vote électronique sont détruits [21], ainsi que le DVD utilisé pour transmettre les bulletins au VCA.

Le service national électoral conserve les votes électroniques pendant un mois après le jour de l'élection. Une fois cette période dépassée, et une fois la décision finale sur les éventuelles plaintes déposées a été atteinte, le service national électoral détruit les votes électroniques, les données personnelles des électeurs contenues dans les registres, et la clé privée pour le déchiffrement des votes [22] .

3.2.Sécurité et audit du développement du système :

3.2.1. Analyses du protocole *:*

Le code source du système de vote côté serveur a été publié en Juin 2013, après une pression populaire menée par l'informaticien Tanel Tammet. Le code source a été publié sur GitHub et a été disponible pour l'ensemble des élections suivantes. En revanche, ni le code source de l'application de vote, ni celui de l'application de vérification n'ont été publiés, car il a été jugé qu'il serait alors trop facile de créer des applications malicieuses.

3.2.2. Évaluation du système :

Le comité électoral national estonien a conduit une étude du système de vote par internet en 2003 et ensuite en 2010.

Le système de vote estonien a été fort critiqué dans la littérature scientifique. Ces critiques visent à la fois les aspects théoriques et pratiques. Un exemple de critique est l'utilisation de lecteurs de carte d'identité sans écran ni clavier. Cela rend donc la communication carte - VFS invisible pour l'électeur, ce qui permet, si l'ordinateur de l'électeur est compromis, à un attaquent de contrôler cette communication. Cette menace peut être partiellement avec l'introduction de l'application de vérification, ainsi que la transition vers des lecteurs de carte avec écran et clavier [23] .

Le système de registre a également été critiqué : il permet de détecteur des erreurs, mais un attaquant ayant pris contrôle d'un ou plusieurs composants du système peut être capable de modifier ce qui est enregistré, afin de rendre son intervention indétectable [24] .

Plus récemment (2014), le système de vote a été critiqué par Springall et al. Ces critiques concernent : des contrôles de procédure inadéquats, une sécurité opérationnelle laxiste, transparence insuffisante, et vulnérabilités dans le code source publié. Les auteurs détaillent également des attaques qu'ils ont été capables de monter contre leur reproduction du système de vote estonien. Ces critiques ont ensuite fait l'objet de plusieurs échanges entre les auteurs et la commission nationale électorale estonienne [25] .

Néanmoins, le système de vote a reçu un support considérable du public et des partis politiques estoniens. Le rapport de l'OSCE/ODIHR (Organization for Security and Cooperation in Europe / Office for Democratic Institutions and Human Rights) de 2011 mentionne que "Les parties prenantes électorales ont exprimé leur confiance dans le processus, y compris le vote par Internet" [26] .

En 2016, des informaticiens de l'Université d'Oxford [27], bien que reconnaissant le succès relatif du vote électronique, ont affirmé que les responsables du système "se sont appuyés, depuis la création du système, sur l'établissement de la confiance par le biais de relations interpersonnelles" et que "cela peut fonctionner pour une société unie et connectée comme celle de l'Estonie", mais "les processus informels (y compris les enseignements tirés) devraient être clarifiés et documentés officiellement".

En août 2017, une faille de sécurité a été découverte, affectant 750 000 cartes d'identité créés entre le 16 octobre 2014 et le 26 octobre 2017 [28]. Les organisations estoniennes compétentes responsables de la carte d'identité ont depuis publié un correctif sous la forme d'une mise à jour du certificat et publié une procédure détaillée (https://www.id.ee) pour vérifier si une mise à jour est nécessaire et comment l'exécuter.

Le rapport des observateurs électoraux de l'OSCE/ODIHR de 2015, ainsi que les rapports détaillés de l'équipe d'observation indépendante dirigée par Alex Halderman en 2015 et la pression publique exercée par des militants locaux, ont motivé l'introduction de la vérifiabilité universelle du décompte des voix en 2017. La vérification du décompte est effectuée par mixnet en utilisant les propriétés homomorphiques du système de chiffrement ElGamal. La vérification universelle du décompte n'est pas une partie obligatoire du processus et est effectuée par un auditeur de données. Le décompte des votes avec mixnet se fait en parallèle avec l'extraction des votes déchiffrés sur le VCA.

Enfin, début juin 2019, le ministre de l'Entrepreneuriat et de la Technologie de l'information Kert Kingo du gouvernement nouvellement élu a créé un groupe de travail inclusif pour évaluer "la vérifiabilité, la sécurité et la transparence"[29] du système de vote électronique estonien. Le groupe de travail était composé de fonctionnaires, de représentants d'universités et d'instituts de recherche, de critiques et de créateurs du système. En décembre 2019, ils ont présenté les résultats de l'enquête de six mois, avec 25 propositions visant à améliorer l'infrastructure de base du système de vote électronique estonien[30] .

4. Norvège :

4.1. Le système utilisé en Norvège

Procédure de définition et de sélection du système de vote Le vote par internet a été appliqué à deux reprises en Norvège : en 2011 pour une élection du gouvernement local, et en 2013 pour les élections parlementaires. Lors de l'élection de 2011, 10 municipalités ont participé à une tentative de vote par anticipation via internet. Les mêmes municipalités (ainsi que "Larvik" et "Fredrikstad") ont également participé à des essais de vote par internet lors de l'élection parlementaire de 2013. En 2011, 22,6% des personnes à même de voter dans ces municipalités ont voté à l'avance et 16,6% par internet. En 2013, 36,3% ont voté à l'avance et 28% par Internet. Dans le cas des votes par internet, la plupart ont été reçus au cours des trois derniers jours avant la fin du vote par anticipation [31] .

En Norvège, l'accent a été mis sur le fait que l'électeur peut toujours se rendre au bureau de vote et voter à nouveau, s'il a voté par voie électronique et changé d'avis, ou bien s'il a été influencé/contraint par d'autres lors du vote électronique.

Les essais pour le système de vote par internet ont été stoppés en 2014, et n'ont plus été reproduits depuis. Les conclusions qui ont mené à cette décision sont que, malgré que le système a bien fonctionné en pratique, qu'il ait été populaire parmi ses utilisateurs, et qu'il n'y ait pas eu d'irrégularité majeur ou de problème important de performance/disponibilité, le taux de participation n'a pas fondamentalement changé [32]. Il est apparu que les votes par internet sont statistiquement similaires aux votes physiques (à l'exception des votes multiples, plus souvent présents dans le vote par internet, phénomène expliqué sans doute par la relative facilité de voter à nouveau dans ce cas). Enfin, il a été constaté que les électeurs n'avaient pas les connaissances et/ou ne faisaient pas les efforts nécessaires pour comprendre les propriétés de sécurité du système.

Une autre dimension importante mise en avant pour expliquer cette décision est que l'élection de 2013 a apporté à un changement de gouvernement en 2014, et qu'il y avait un manque de volonté politique pour continuer à financer le projet. Le ministère du gouvernement local et de la modernisation aurait déclaré [33]: "Les projets pilotes menés en 2011 et 2013 ont apporté des connaissances et une expérience intéressantes et précieuses. En l'absence de volonté politique générale d'introduire le vote par Internet, le Gouvernement a conclu qu'il serait inapproprié de consacrer du temps et de l'argent à d'autres projets pilotes."

4.1.1. Organisation d'une élection :

Les élections norvégiennes sont un quelque peu complexes, et les élections du gouvernement local et les élections parlementaires fonctionnent différemment. Chaque électeur reçoit une liste de candidats groupés par partis politiques. Dans le cas des élections du gouvernement local, l'électeur choisit un parti, et peut ensuite y ajouter un certain nombre de candidats d'autres partis. Dans le cas des élections parlementaires, l'électeur choisit un parti, et peut réordonner les candidats au sein de la liste de ce parti, ainsi que d'en supprimer certains. Dans les deux cas, un bulletin de vote consiste donc en une liste de taille variable de candidats. Dans le cas des élections parlementaires, l'ordre de cette liste importe (à l'inverse des élections du gouvernement local). La participation à une élection n'est pas obligatoire en Norvège.

Le fait que ces bulletins soient complexes implique que de nombreux bulletins distincts ont essentiellement le même effet sur l'élection (par exemple si deux bulletins différents ont beaucoup de candidats en commun, ou si les têtes de leurs listes sont égales). Ceci veut dire qu'il est possible de "marquer" un bulletin de vote, par exemple en votant (en plus d'un ensemble de candidats "cible") pour un ensemble de candidats uniques. Si des bulletins peuvent être marqués de cette façon (tout en restant légitimes et donc non-détectables), cela signifie que des votes peuvent être achetés. Cette possibilité devant être évitée à tout prix pour une élection démocratique, il est donc important que les bulletins de vote soient secrets, y-compris lors du comptage.

Les protocoles utilisé dans les élections de 2011 et de 2013 sont distincts mais similaires. Le système de 2013 est "significativement plus efficace" et fait l'objet "d'une analyse améliorée" [34] . Le gain en performance est dû principalement à l'utilisation de "multi-ElGamal" et de preuves à divulgation nulle de connaissance (NIZK, Non-Interactive Zero-Knowledge proofs) plus efficaces que celles de la version de 2011. De plus, en 2013, le client applet java a été remplacé par une implémentation en javascript, plus alignée avec les pratiques recommandées et les technologies mieux supportées de l'époque.

La figure ci-dessous représente une vue d'ensemble du système de vote [35]. Cette vue d'ensemble témoigne de la relative complexité du système, mais démontre certains aspects de sa sécurité, comme la sauvegarde de registres (logs) sur les différents systèmes, l'isolation physique et logique de certains sous-systèmes indépendants, et les différentes interfaces et communications entre ces sous-systèmes.

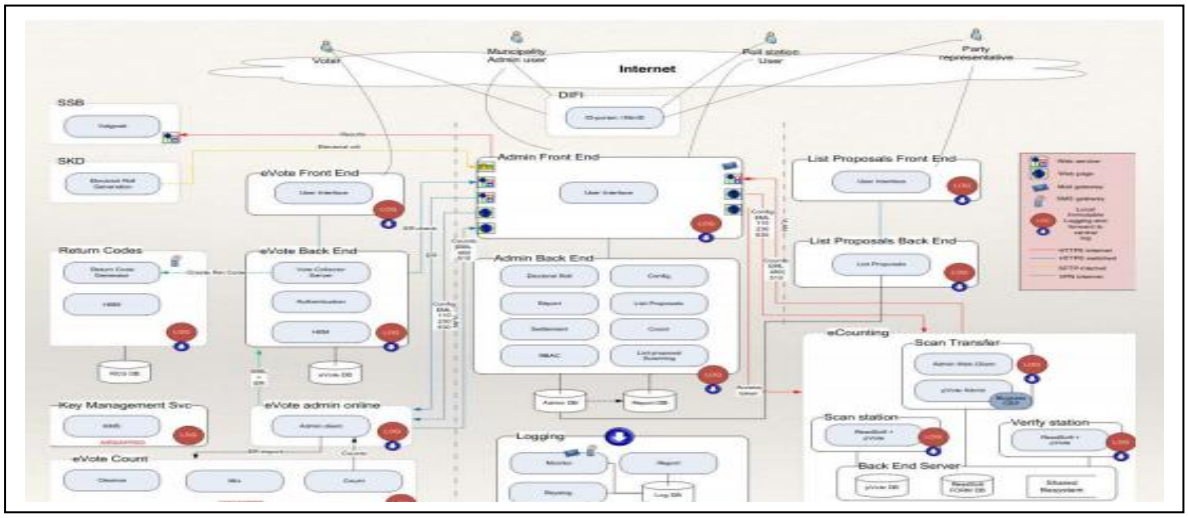

Figure 2.2 : une vue d'ensemble du système de vote

4.1.2. Vue d'ensemble du système norvégien de vote par internet :

Le protocole cryptographique du système de vote par internet norvégien est relativement complexe, mais utilise des outils mathématiques raisonnablement standard et bien étudiés :

- Les bulletins sont chiffrés avec ElGamal, permettant de respecter leur anonymat grâce aux propriétés homomorphiques de ElGamal
- Des preuves divulgation nulle de connaissance (zero-knowledge proofs) et signatures de Schnorr sont utilisées pour diverses vérifications pendant le vote
- Des mixnets sont utilisés pour séparer électeurs et bulletins
- Le partage de secret de Shamir (secret sharing) est utilisé pour séparer les clés de déchiffrement (et donc la responsabilité) entre les différents opérateurs

4.1.3. Utilisabilité :

Le système est implémenté en java sur linux côté serveur, et en HTML/javascript côté client (2013). Après le vote de 2011, les autorités ont contacté deux centres de recherche et l'IFES (International Foundation for Electoral Systems) pour effectuer une évaluation du système de vote. L'évaluation a utilisé des méthodes de recherche à la fois qualitatives et quantitatives, y compris des enquêtes par questionnaire dans les municipalités d'essai, des entretiens approfondis avec des groupes sélectionnés, des groupes de discussion pour les jeunes et des études d'observation de l'utilisabilité pour les électeurs handicapés. L'institut de recherche sociale (Institutt for samfunnsforskning) a fait un rapport sur le second essai de 2013.

Les conclusions sont multiples et globalement positives :

- La participation du vote par internet est similaire au vote physique
- Les personnes ayant voté par internet sont très satisfaites du système, ajoutant qu'il est facile d'utilisation
- La confiance envers le gouvernement et les élections est très élevé en Norvège. Les essais de vote par internet ne semblent avoir eu qu'un impact faible sur une baisse de confiance des utilisateurs (possiblement liée à la faible confiance générale des technologies liées à l'internet) Les rapports d'évaluation sont disponibles sur le site Internet du ministère des Collectivités locales et du Développement régional [36] .

4.1.4. Garanties d'intégrité :

dentification des électeurs : L'authentification se base sur l'infrastructure à clé publique norvégienne existante. Il s'agit d'une authentification multifacteur, utilisant un jeton d'authentification et code par SMS [37] .

Suivi des bulletins de vote : L'une des méthodes de suivi de vote est l'utilisation de codes de retour ("return code"). Avant l'élection, l'électeur reçoit par voie postale une "carte de vote", un document contenant un certain nombre de codes de retour. Ces codes sont uniques pour chaque électeur, et correspondent aux différents partis. Lors du vote, une fois le bulletin soumis, l'électeur reçoit un code de retour par SMS Ce code de retour est ensuite comparé par l'électeur avec la liste de codes de retour sur sa carte de vote personnelle. C'est une hypothèse de sécurité fondamentale que la carte de vote ne puisse être liée par quelqu'un d'externe au SMS reçu ou à la personne correspondante.

Une seconde méthode de suivi est qu'une fois le bulletin de vote soumis, l'interface web affiche un haché (sha256 du bulletin chiffré). Une fois l'élection terminée, le gouvernement norvégien publie sur github une liste des hachés de tous les bulletins soumis. Un électeur peut donc chercher son haché dans cette liste.

Qualité du décompte **:** Lors du décompte, deux systèmes implémentés et opérés indépendamment (l'un par le gouvernement et l'un par un parti tiers) ont été utilisés, afin de déterminer s'il existe une différence majeure dans le décompte (diversification software).

4.1.5. Garanties de confidentialité

Le contenu de chaque bulletin de vote est chiffré (ElGamal). L'ensemble des communications entre client et serveur ainsi qu'entre serveurs sont encapsulées par un canal sûr (TLS). L'éventualité de coercition est majoritairement mitigée par la possibilité de voter plusieurs fois, ainsi que par la possibilité de se résoudre au vote physique en bureau de vote, qui supplante tout vote par internet. Si la carte de vote, SMS de retour, et le haché de retour sont gardés secrets, la participation (ou la non-participation) à l'élection est gardée secrète. Enfin, la confidentialité de résultats intermédiaires de l'élection sont garantis par diverses mécanismes de sécurité mis en place côté serveur, en particulier : outils cryptographiques utilisés (chiffrement homomorphique, mixnets), séparation physique de différent sous-systèmes, séparation de responsabilité des opérateurs, communications encapsulées par canaux sûrs.

4.2.Sécurité et audit du développement du système

4.2.1. Analyses du protocole :

Kristian Gjøsteen, de la NTNU (Norwegian University of Science and Technology) a publié deux papiers scientifiques sur le protocole de vote norvégien de 2011 et de 2013 respectivement. Dans ces documents, il décrit les protocoles et les outils cryptographiques utilisés et fournit des preuves de sécurité pour l'aspect mathématique du vote. En ce qui concerne la qualité de l'implémentation du protocole, comme expliqué dans la section "Évaluation du système", une société tierce a effectué un audit du code source du système de 2011.

4.2.2. Évaluation des élections

Une série de moniteurs surveillent ("shadow") les opérateurs pendant la période de vote et lors du décompte.

4.2.3. Principes de développement :

Le système de vote par internet a été mis en place par le projet e-vote 2011, en coopération avec Scytl Secure Electronic Voting (une compagnie espagnole spécialisée dans le déploiement de solutions de vote électronique) et Kristian Gjøsteen de la NTNU. Une documentation partielle aurait été rassemblée dans l'optique d'obtenir un certificat de critères communs pour un éventuel déploiement national. Cependant, le projet ayant été annulé en 2014, ceci n'a jamais été mené à terme [38] .

4.2.4. Evaluation du système :

Le code source serveur est publique (bien qu'à licence propriétaire). Un rapport d'audit du code source (côté serveur) de l'élection de 2011 a été effectué en 2013 par mnemonic, une société norvégienne de cybersécurité [39]. Le code source y est décrit comme de qualité faible. Un certain nombre de problèmes mineurs ont été découverts, et une série de recommandations a été proposée. Cependant, "mnemonic n'a découvert aucune faiblesse cryptographique critique qui empêcherait l'utilisation du système de vote par Internet lors des prochaines élections." Il faut toutefois remarquer que cette analyse est une vue d'ensemble, étant donné la complexité et la taille du projet (environ 200000 lignes de code) et le peu de ressources en temps et personnel attribuées à l'audit [40] .

Une démonstration d'une attaque de phishing (hameçonnage) a été réalisée par Kai A. Olsen et Hans Fredrik Nordhaug du Molde University College en 2011 [41]. Ils ont créé une

page web ressemblant à la page officielle. L'objectif était d'obtenir des codes de retour de la carte de vote d'un électeur naïf. Ceci permettrait de lier cet électeur à son vote par le biais du code de retour reçu par SMS.

En 2013, 5 jours avant élections, un bug côté client a été découvert [42]. Ce bug concernait une mauvaise sélection de nombres aléatoires dans le processus de chiffrement, amenant à la révélation d'information sur le texte clair (contenu du bulletin de vote) dans certains cas. Cependant, grâce à l'encapsulation de ces chiffrés dans un canal TLS, aucun vote n'aurait été révélé. Ceci constitue malgré tout une faute importante et témoigne de l'importance de la vérification des implémentations d'applications de sécurité.

En 2013, la BBC publie un article critiquant le système de vote par internet norvégien lors de l'élection parlementaire[43]. Ils y citent en particulier qu'une faille de sécurité aurait permis à 0,75% des électeurs de voter deux fois (une fois en ligne, et une fois en bureau de vote). Ce fait aurait cependant été nié par le gouvernement norvégien [44] .

5. Conclusion :

Dans ce chapitre, nous avons parlé des travaux précédents et de l'expérience de certains pays en matière de vote électronique et expliqué certains systèmes de vote électronique pour essayer de réaliser notre propre système que nous expliquerons dans le chapitre suivant

CHAPITRE 3 :

PRESENTATION ET CONCEPTION DE NOTRE SYSTEME

1. Introduction

Dans ce chapitre, nous vous donnons une explication détaillée de l'application et de son mécanisme de travail et quelques méthodes de sécurité

Le développent de n'importe quel système d'information nécessite une démarche très important dans le cycle de vie d'un logiciel, et la modélisation en pratique est important dans les développements des logiciels, dans notre projet nous choisit le langage de modélisation UML qui nous allons exposer dans ce chapitre

2. Présentation générale du projet :

Ce travail vise à créer une application Web pour les élections pour l'Université visant à faciliter le processus de nomination des chefs de départements et des chefs de classes par le biais d'élections en ligne .

L'administrateur a créé un compte utilisateurs (approprié) et envoyer des calculs par e-mail, après avoir reçu le nom d'utilisateur et le mot de passe, l'application, connectez - vous pour enquêter, puis changer le mot de passe forcé via une interface personnalisée afin

À la fin, l'utilisateur vote sur les élections précédemment écrites par l'administrateur

Et ci-dessous, nous allons aux tâches qui peuvent être effectuées par l'administrateur et l'utilisateur dans l'application :

2.1.Tâches d'administration

- Écrire, modifier et supprimer un vote
- Ajouter et supprimer un utilisateur
- Modifier ses informations
- Voir les résultats des votes pendant et après la fin de l'heure de vote

2.2.Tâches utilisateur :

- Modifier ses informations
- Voter
- Accès à la liste des électeurs

- Voir les résultats des votes après la fin de l'heure de vote

2.3.Quelques méthodes de sécurité

❖ L'admirateur est celui qui ajoute l'utilisateur et envoie les informations de connexion pour donner au admirateur les pleins pouvoirs pour sélectionner les votants

❖ Une fois que l'utilisateur a reçu les informations de connexion, il doit changer le mot de passe pour empêcher l'administrateur d'entrer dans le compte de l'utilisateur

❖ L'utilisateur a le droit de voir la liste des utilisateurs (électeurs) pour éviter que l'administrateur ajoute des utilisateurs inconnus

2.4.Méthode de cryptage des informations :

Fonction de hachage : la fonction de hachage convertit des séquences de caractères de différentes longueurs en séquences de même longueur. Par exemple, la fonction de hachage confère à des mots de passe différents une quantité définie de caractères autorisés. Une conversion de la valeur de hachage dans le sens inverse, c'est-à-dire vers la séquence de caractères initiale, est exclue.

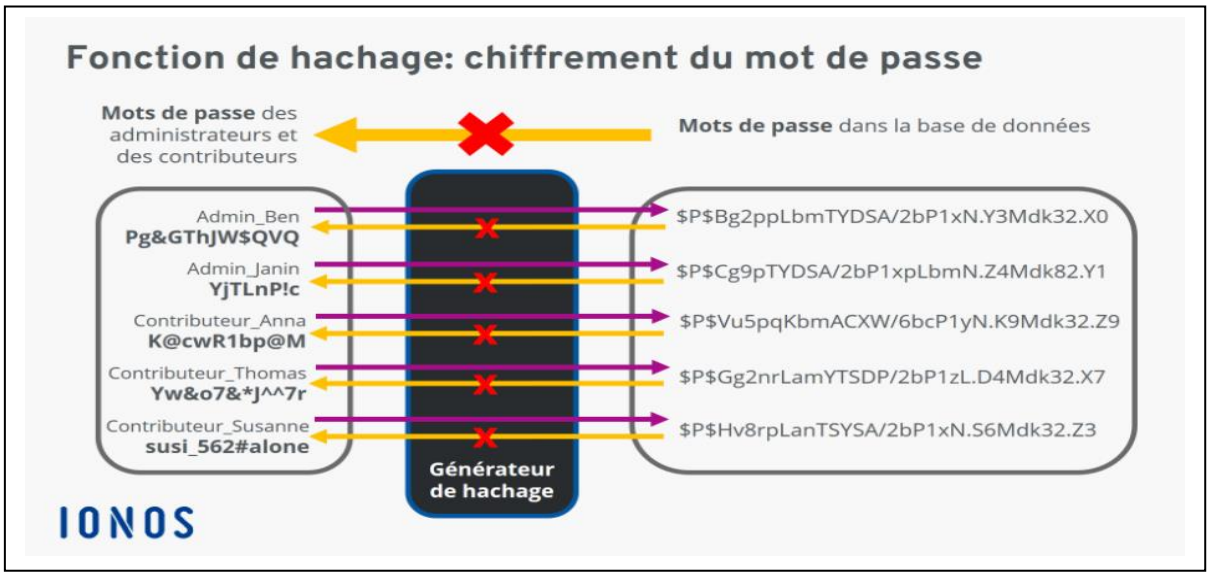

FIGURE 3.1: Exemple, la fonction de hachage

Dans cet exemple, la fonction de hachage génère une valeur de hachage de même longueur à partir de mots de passe d'une longueur différente et les enregistre dans la base de données. Il est impossible de procéder à une conversion dans le sens inverse.

Quelles sont les caractéristiques d'une fonction de hachage ?
Des exigences définies sont imposées à une fonction de hachage pour qu'elle présente des **caractéristiques** données. Ces exigences sont les suivantes :

2.4.1. Sens unique de la fonction de hachage :

Une valeur de hachage générée **ne doit pas permettre de générer à nouveau le contenu des données initial**. Dans l'exemple ci-dessus, il doit donc être impossible de retrouver le mot de passe « susi_562#alone » à partir de la valeur de hachage générée « PHv8rpLanTSYSA/2bP1xN.S6Mdk32.Z3 ».

2.4.2. Absence de collisions :

En aucun cas, une valeur de hachage identique ne doit être attribuée à des données initiales différentes. Chaque saisie doit générer une autre valeur de hachage. Lorsque cet objectif est atteint, on parle de fonction de hachage cryptographique. Dans l'exemple ci-dessus, on ne constate aucune valeur de hachage identique et donc aucune collision entre les données générées. D'autres technologies permettent d'éviter les collisions de ce type.

2.4.3. Célérité de la fonction de hachage :

Si la conversion des données en valeur de hachage prenait trop de temps, ce processus n'aurait pas d'utilité. La fonction de hachage doit donc travailler avec une extrême rapidité. Dans les bases de données, les valeurs de hachage sont stockées dans ce qu'on appelle des tables de hachage pour garantir un accès rapide.

3. UML

UML est l'abréviation de « Unified Modeling language », c'est un langage unifie pour la modélisation. UML est un ensemble d'outils pour aide la modélisation de la future des applications informatique. UML c'est une méthode utilisant des graphismes pour la création de modèles orientés objet vers de la conception et de modélisation de logiciels orientés objet

3.1.Diagramme de cas d'utilisation :

Permet la représentation des fonctionnalités nécessaires aux utilisateurs. On peut faire un diagramme de cas d'utilisation pour le logiciel entier ou pour chaque package, ce diagramme clarifié comment les utilisateurs externes (acteur), dialoguer avec ces cas d'utilisation.

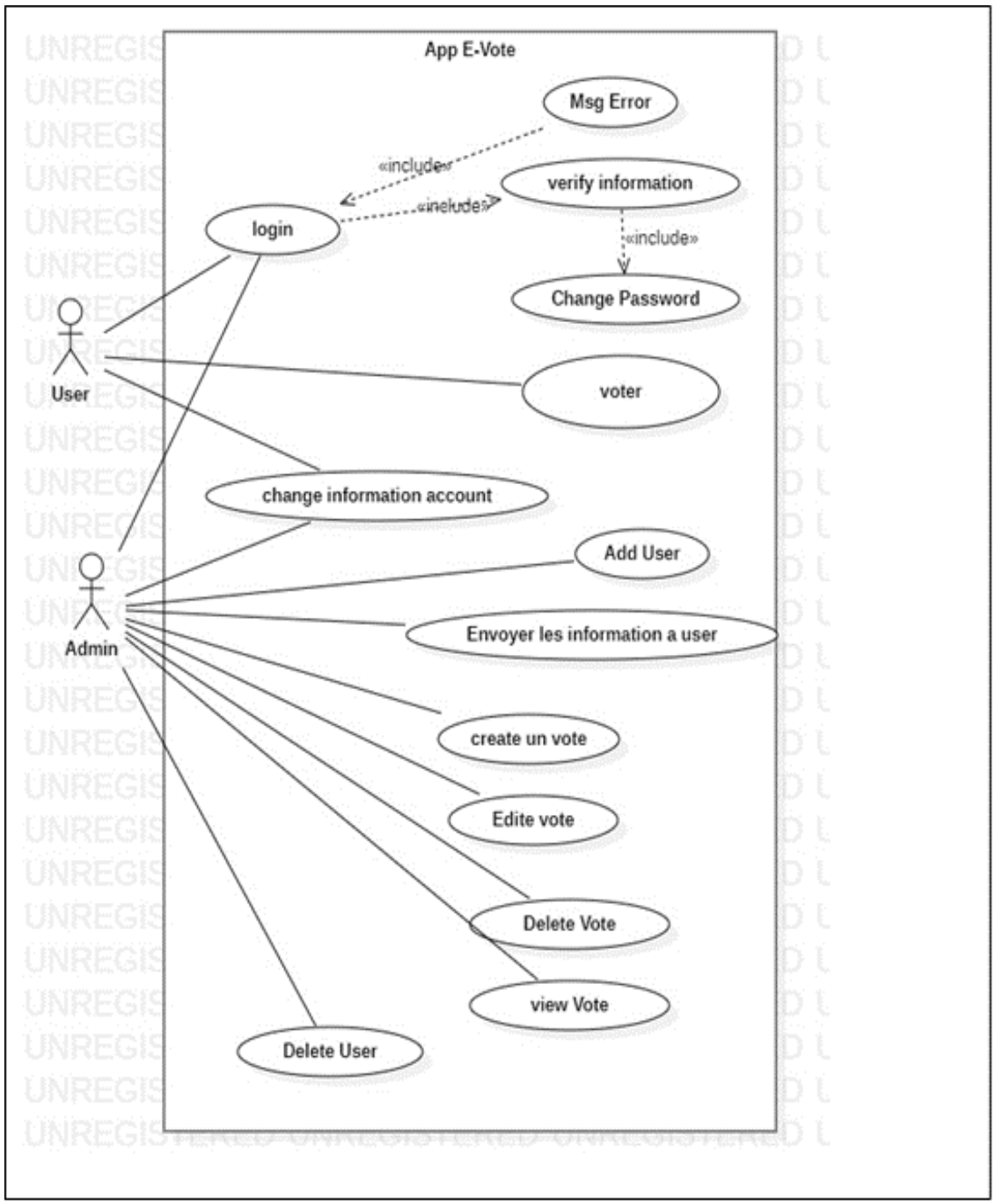

FIGURE 3.2 : Diagramme de cas d'utilisation **.**

3.2.Diagramme de classes

Le diagramme de classe représente les entités manipulées par les utilisateurs c'est le diagramme le point centrale dans le développement orienté objet et le plus utilisé il présenter les types d'objets et les relations entre aux.

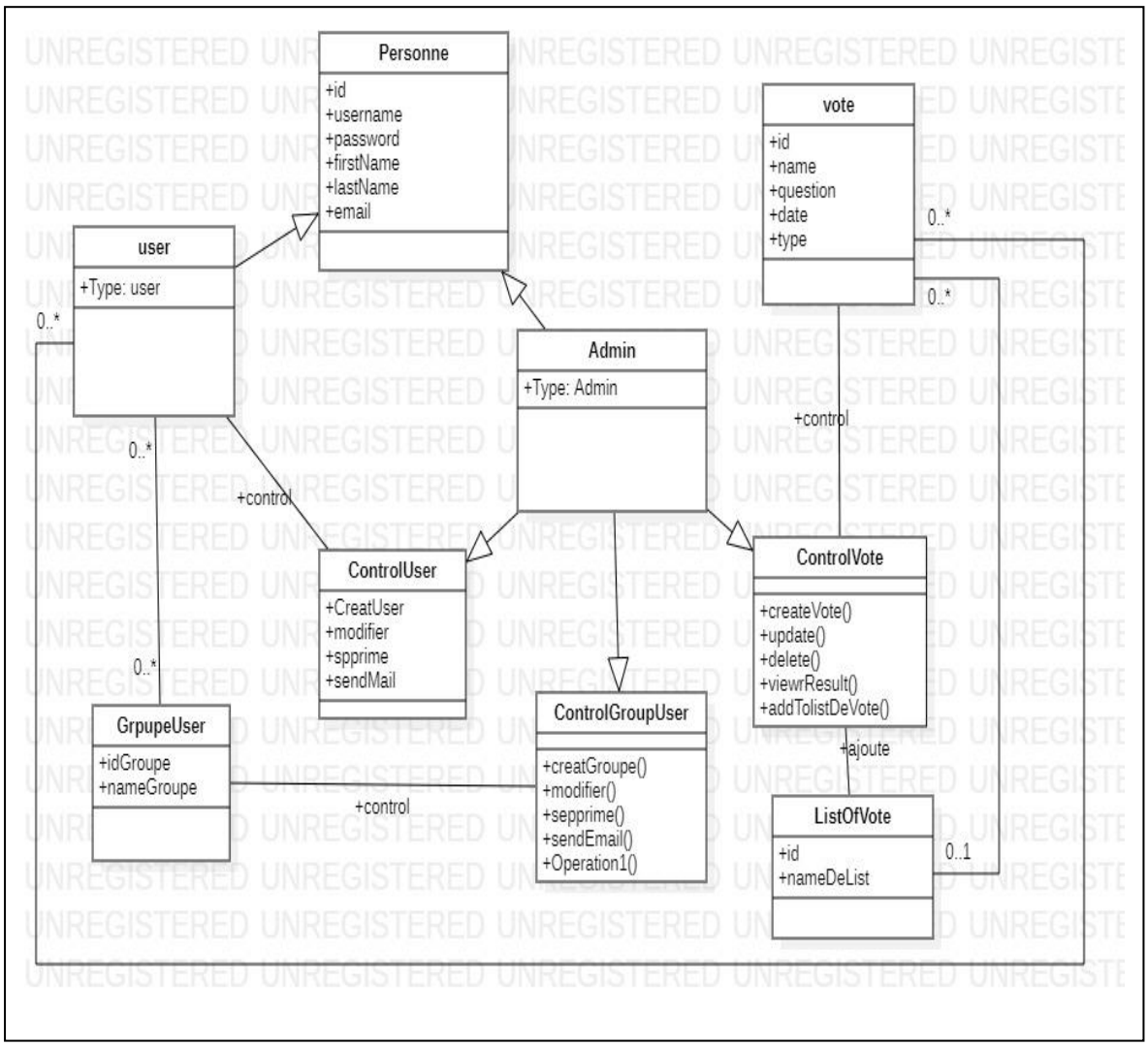

FIGURE 3.3 : Diagramme de Class **.**

3.3.Diagramme de séquence

Permet décrire les interactions entre les objets d'un système selon un ordonnancement temporel, cette interaction fait par l'envoi de messages (message synchrone ou message asynchrone), qui appelle une méthode.

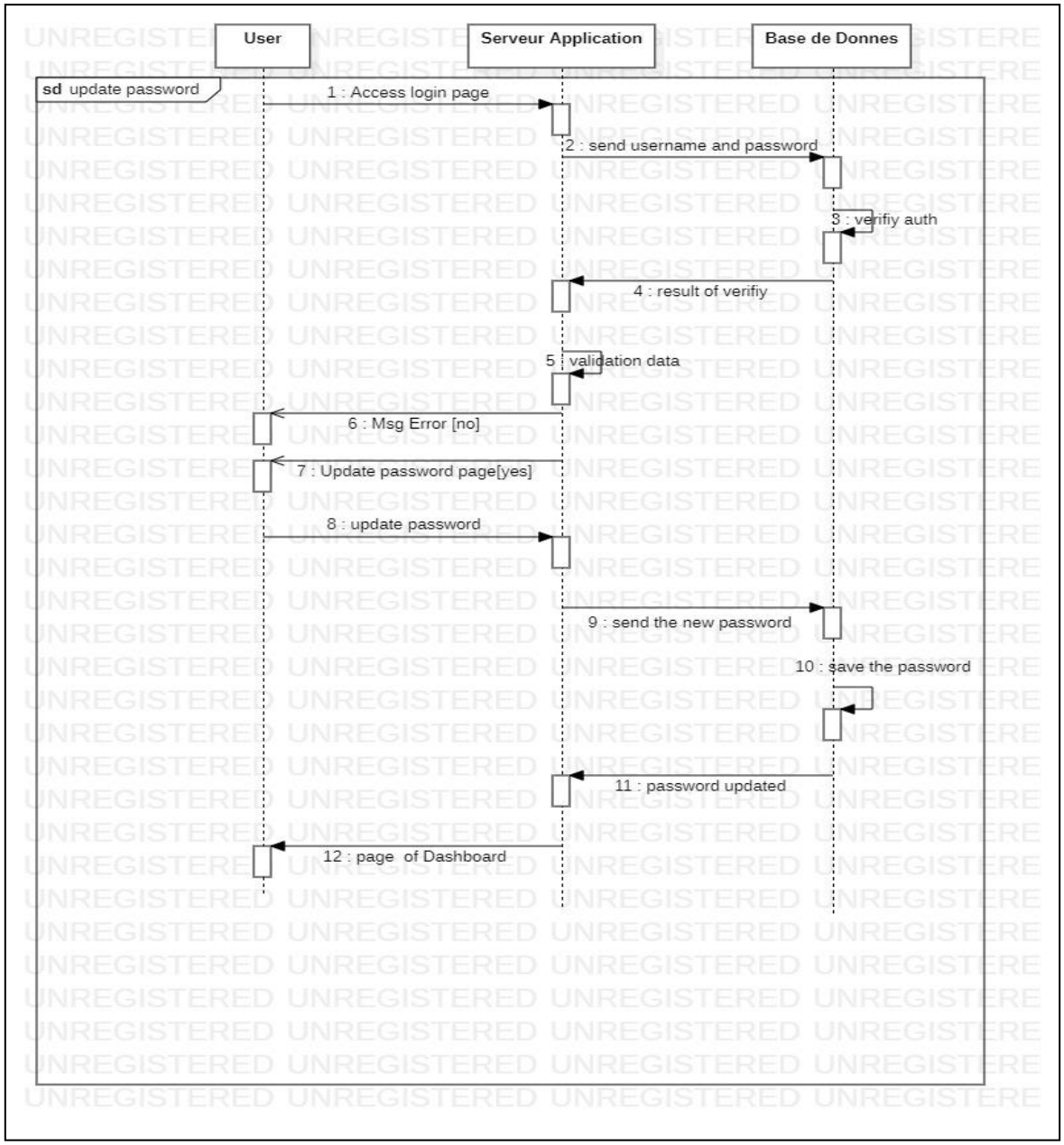

FIGURE 3.4 : Diagramme de Séquence Cas update password

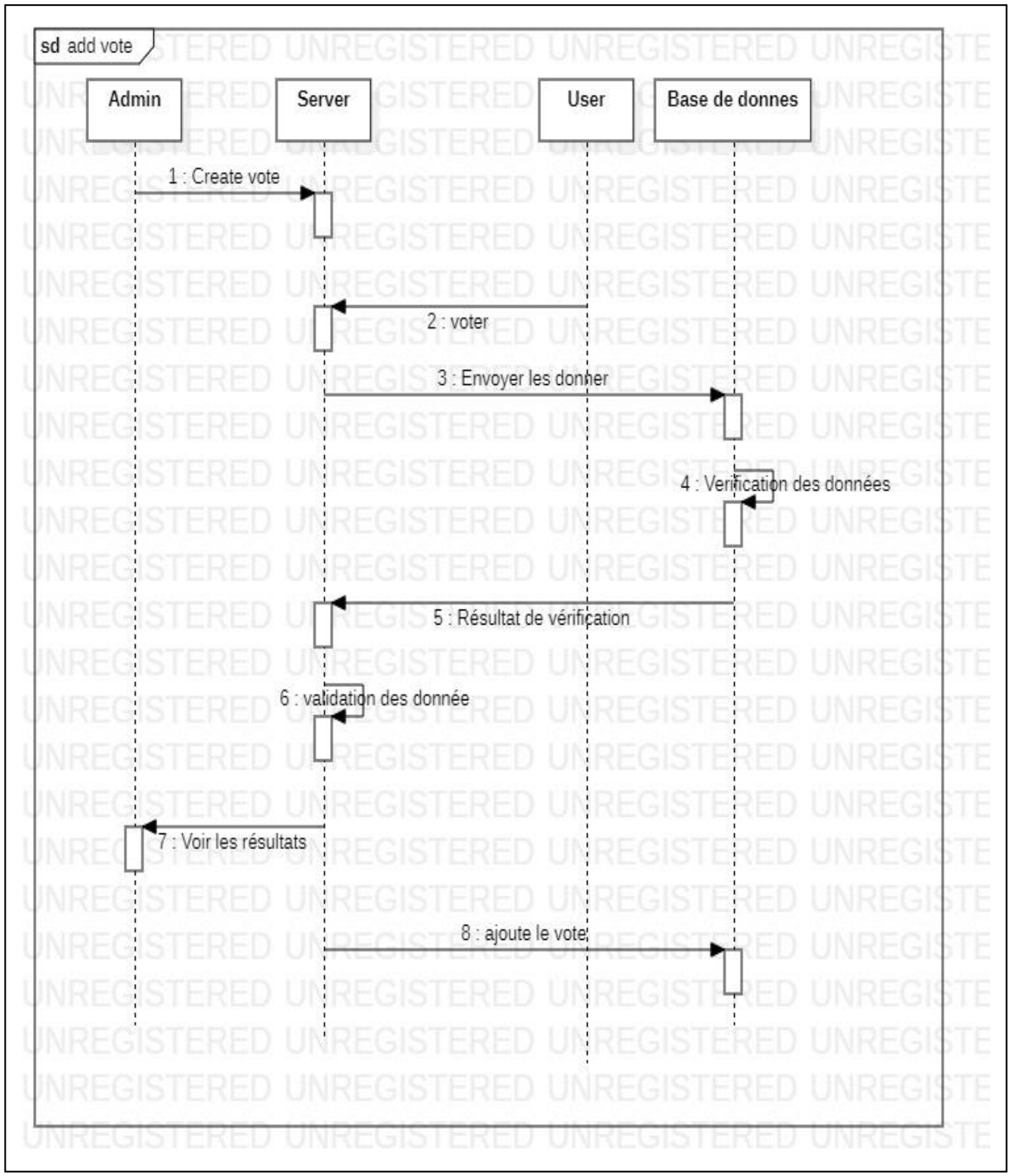

FIGURE 3.5 : Diagramme de Séquence add vote

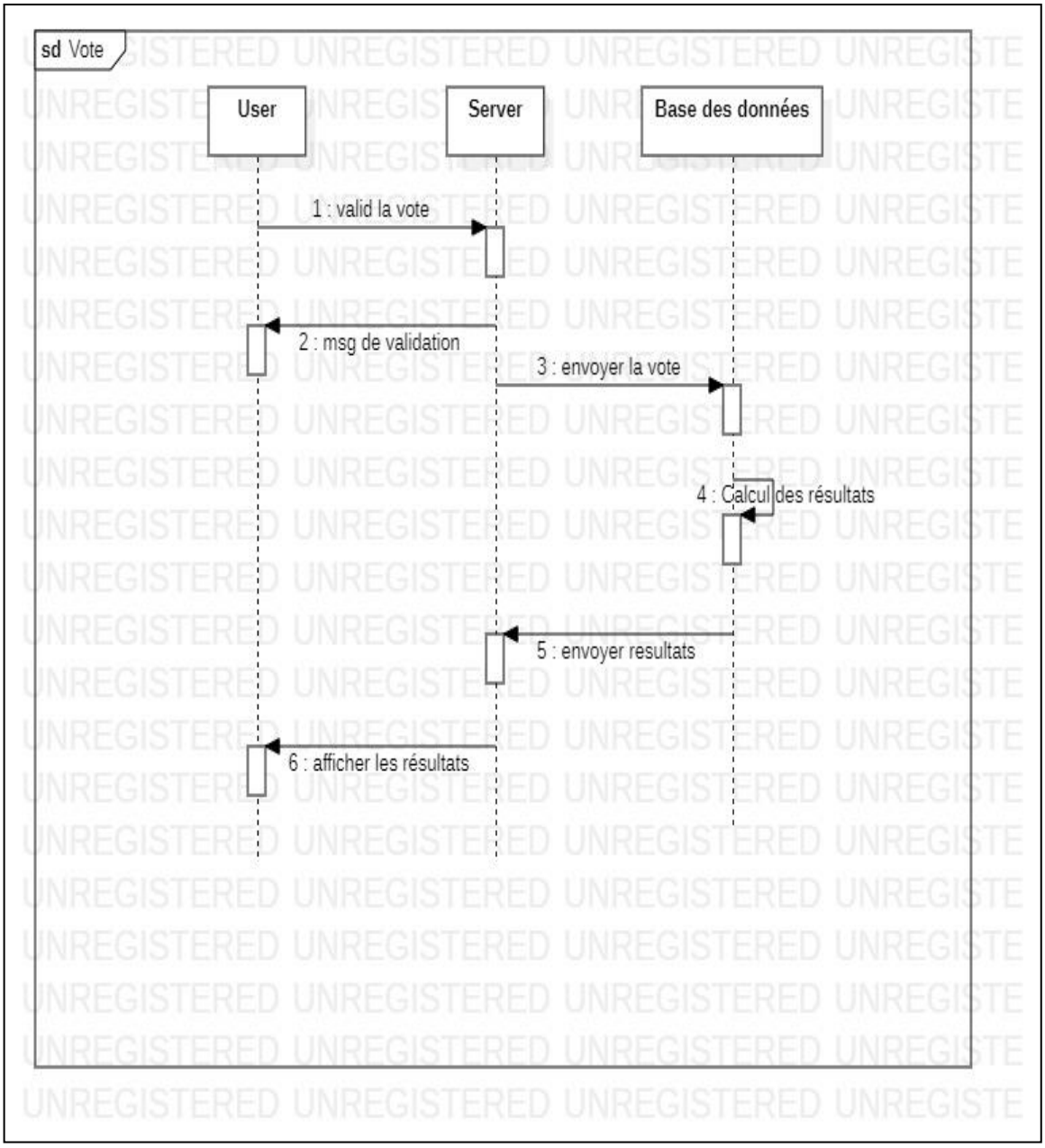

FIGURE 3.6 : Diagramme de Séquence vote

4. Les Tableux de base des données

Colonne	Type	Nul	Par défaut
ID (Clé primaire)	Int (11)	No	
Title	Varchar (500)	No	
Message	text	No	

Table 3.1 Email Templates

Colonne	Type		Nul	Par défaut
ID (Clé primaire)	Int (11)		No	0
Total_membres	Int (11)		No	0
Active_today	Int (11)		No	0
Timestamp	Int (11)		No	0

Table 3.2 Home_Stats

Colonne	Type	Nul	Par défaut
ID (Clé primaire)	Int (11)	No	
Username (Clé	varchar (500)	No	
unique)	Int (11)	No	0
count	Int (11)	No	0
Timestamp			

Table 3.3 Login_attempts

Colonne	**Type**	**Nul**	Par défaut
ID (Clé primaire)	int(11)	No	
userid -> clé étrangère	int(11)	No	0
(users)	varchar(255)	No	
token	int(11)	No	0
timestamp	varchar(500)	No	
IP			

Table 3.4 Password_Reset

Colonne	Type	Nul	Par défaut
ID *(Clé primaire)* name layout_path	int(11) varchar(255) varchar(255)	No No No	

Table 3.5 Sites Layout

Colonne	Type	Nul	Par défaut
ID *(Clé primaire)*	int(11)	No	
site_desc	varchar(500)	No	
upload_path	varchar(500)	No	
upload_path_relative	varchar(500)	No	
site_email	varchar(500)	No	
site_logo	varchar(1000)	No	logo.png
date_format	varchar(25)	No	
avatar_upload	int(11)	No	1
file_types	varchar(500)	No	
file_size	int(11)	Yes	0
par défaut_votes	int(11)	No	250
enable_ads	int(11)	No	0
install	int(11)	No	1
login_protect	int(11)	No	0
activate_account	int(11)	No	0
layout	varchar(255)	No	
stripe_publish_key	varchar(255)	No	
checkout2_accountno	int(11)	No	
checkout2_secret	varchar(255)	No	

Table 3.6 Site Setting

Colonne	Type	Nul	Par défaut
ID *(Clé primaire)*	int(11)	No	
email (clé unique)	varchar(255)	No	
password	varchar(100)	No	
token	varchar(255)	No	
username (clé unique)	varchar(25)	No	
first_name	varchar(25)	No	
last_name	varchar(25)	No	
avatar	varchar(1000)	No	par défaut.png
joined	int(11)	No	0
joined_date	varchar(10)	No	
online_timestamp	int(11)	No	0
oauth_provider	varchar(40)	No	
oauth_id	varchar(1000)	No	
oauth_token	varchar(1500)	No	
oauth_secret	varchar(500)	No	
email_notification	int(11)	No	1
aboutme	varchar(1000)	No	
points	decimal(10,2)	No	0.00
active	int(11)	No	1
activate_code	varchar(255)	No	

Table 3.7 Users

Colonne	Type	Nul	Par défaut
ID *(Clé primaire)* name par défaut	int(11) varchar(40) int(11)	No No No	 0

Table 3.8 User groups

Colonne	**Type**	**Nul**	Par défaut
ID *(Clé primaire)*	int(11)	No	
userid -> clé étrangère (users)	int(11)	No	0
name	varchar(255)	No	
question	text	No	
timestamp	int(11)	No	0
show_results	int(11)	No	0
status	int(11)	No	0
votes	int(11)	No	0
created	int(11)	No	0
updated	int(11)	No	0
hash	varchar(255)	No	
vote_type	int(11)	No	0
votes_today	int(11)	No	0
votes_today_timestamp	int(11)	No	0
votes_month	int(11)	No	0
votes_month_timestamp	int(11)	No	0
themeid	int(11)	No	0
cookie_restricted	int(11)	No	0
user_restricted	int(11)	No	
public	int(11)	No	

Table 3.9 User vote

Colonne	Type	Nul	Par défaut
ID *(Clé primaire)*	int(11)	No	
userid -> clé étrangère (users)	int(11)	No	0
voteid -> clé étrangère (user_votes)	int(11)	No	0
answerid	int(11)	No	0
user_agent	varchar(255)	No	
timestamp	int(11)	No	0
date_stamp	varchar(60)	No	

Table 3.10 User vote answers

Colonne	Type	Nul	Par défaut
ID *(Clé primaire)*	int(11)	No	
userid -> clé étrangère (users)	int(11)	No	0
timestamp	int(11)	No	0
votes	int(11)	No	0
vote_votes	int(11)	No	0
vote_votes_today	int(11)	No	0

Table 3.11 User stats

5. Conclusion

Le but de ce chapitre était d'apprendre à utiliser l'application et de donner quelques diagrammes pour comprendre facilement son mécanisme de travail .

Et nous donnerons une image plus claire de l'application en montrant des captures d'écran des pages les plus importantes de l'application en plus des outils de développement d'applications dans le chapitre suivant .

CHAPITRE 4

REALISATION DE NOTRE SYSTEME

1. Introduction

Dans ce chapitre nous allons développer un application web d'un vote électronique en ligne, pour cela nous allons décrire les logiciels et les langages de programmation utilisés, qui nous ont permis la réalisation de ce travail et qu'on a utilisé et on évoquera le système d'exploitions, ainsi nous présenterons quelques exemples des interfaces représentant la plateforme qui ont été réalisées.

2. Environnement de développement :

Dans cette partie nous allons présenter chacun des logiciels de programmation, langage de programmation, logiciel de traitement d'image qu'on a utilisé le système d'exploitions

2.1. Le système d'exploitation :

L'environnement de base pour ce travail est le système d'exploitation Windows 10 , pour obtenir des performances de façon plus facile, et il est lié à la machine. Donc Windows 10 , fournit un travail plus efficace, qui offre la fiabilité et l'efficacité.

Dans cette partie on va donner quelque définition sur les langages de programmations

2.1.1. . PHP (Hypertext Preprocessor) :

Plus connu sous le nom de PHP, c'est un langage de programmation WEB principalement utilisé pour produire des pages Web dynamiques(client/serveur) via un serveur HTTP (ex: Apatche), on désigne parfois PHP comme une plateforme plus qu'un simple langage.

Les codes du PHP sont appelés « scripts », et ils sont inclus dans le code HTML. Exemple (script):

Site officiel : https://www.php.net/

2.1.2. HTML(HyperText Markup Language)

C'est un langage de balise permettant le codage des pages WEB. HTML permet également de structurer sémantiquement et de mettre en forme l'interface des sites, d'inclure des ressources multimédias

telles que les images, les formulaires de saisie, et les programmes informatiques.Il permet de créer des documents interopérables avec des équipements très variés de manière conforme aux exigences de l'accessibilité du web. Il est souvent utilisé conjointement avec des langages de programmation et des formats de présentation (feuilles de style en cascade).
HTML est initialement dérivé du Standard Generalized Markup Language (SGML).

Site officiel : https://developer.mozilla.org/fr/docs/Web/HTML

2.1.3. JavaScript

Le javascript est un langage informatique utilisé sur les pages web.
Ce langage à la particularité de s'activer sur le poste client, en d'autres mots c'est votre ordinateur qui va recevoir le code et qui devra l'exécuter. C'est en opposition a d'autre langage qui sont activé côté serveur. L'exécution du code est effectuée par votre navigateur internet tel que firefox ou google chrome.

Site officiel : https://developer.mozilla.org/fr/docs/Web/JavaScript

2.1.4. . CSS

CSS est l'acronyme de Cascading Style Sheet, est un langage de conception simple destiné à simplifier le processus de présentation des pages Web
, donc utilisé sur l'internet pour mettre en forme les fichiers HTML ou XML, donc ce code pour gérer le désigne d'une page web.

Site officiel : https://www.w3schools.com/css/

2.2. Outils de développement :

2.2.1. XAMPP :

XAMPP signifie Cross-Platform (X), Apache (A), MySQL (M), PHP (P) et Perl (P).C'est un ensemble de logiciels permettant de mettre en place facilement un serveur Web et un serveur FTP. Il s'agit d'une distribution de logiciels libres (X Apache MySQL Perl PHP) facile à installer offrant une bonne souplesse d'utilisation permettent l'exploitation d'un serveur Apache, de l'SGBD MySQL et l'interpréteur PHP.

XAMPP est également multiplate-forme, ce qui signifie qu'il fonctionne aussi bien sur Linux, Mac et Windows.

Site officiel : https://www.apachefriends.org/fr/index.html

2.2.2. . Serveur Apache :

Apache est un logiciel de serveur web gratuit et open-source qui

alimente environ 46% des sites web à travers le monde. Le nom officiel est Serveur Apache HTTP et il est maintenu et développé par Apache Software Foundation.

utilisé principalement sur les hébergements Internet en Linux, bien qu'il soit également utilisable en Windows.

Site officiel : https://www.hostinger.fr/tutoriels/quest-ce-quapache-serveur-web-apache

2.2.3. MySQL :

Est un système de gestion de base de données (SGBD). Comme serveur de bases de données relationnelles Open Source, Basé sur Structured Query Language (SQL). Aussi MySQL est le plus souvent associé à des applications basées sur le Web

Site officiel : https://www.mysql.com/fr/

2.2.4. *Bootstrap* :

est une collection d'outils utiles à la création du design (graphisme, animation et interactions avec la page dans le navigateur, etc.) de sites et d'applications web. C'est un ensemble qui contient des codes HTML et CSS, des formulaires, boutons, outils de navigation et autres éléments interactifs, ainsi que des extensions JavaScript en option. C'est l'un des projets les plus populaires sur la plate-forme de gestion de développement GitHub.

Site officiel : https://getbootstrap.com/

2.2.5. Un éditeur Visual Studio Code :

Lighting fast, free, and extensible code editor from Microsoft, based on open source, that runs on Windows, macOS, and Linux. Built-in rich language support for web development: HTML, JavaScript, TypeScript, CSS, SCSS, Less, Markdown, etc. Out of the box support for multi-cursor, Emmet, split view, formatting, code folding, and many more code editing features. Rich ecosystem of extensions for all major languages, community themes, services, and features.

Site officiel : https://code.visualstudio.com/migrate-from-brackets/

2.2.6. CodeIgniter :

est un framework PHP puissant avec un très faible encombrement, conçu pour les développeurs qui ont besoin d'une boîte à outils simple et élégante pour créer des applications Web complètes.

Site officiel : https://www.codeigniter.com/

3. Présentation de l'application (Les principe maquettes IHM)

3.1. Page d'authentification :

Dans cette page l'utilisateur ou l'administrateur peut être identifié en tapant son nom et son mot de passe. Si les informations d'authentification sont erronées, le système affiche une nouvelle page d'identification avec un message d'avertissement.

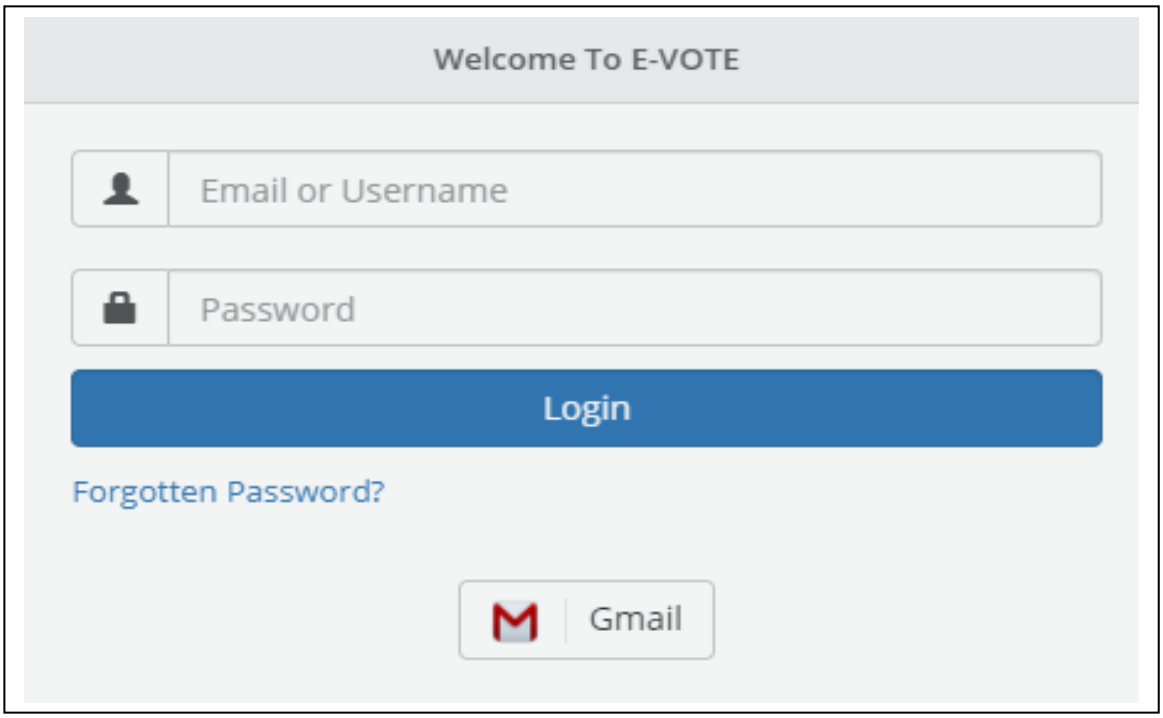

FIGURE 4.1 : Capteur de Page d'authentification .

3.2. Page de changement de mot de passe :

Dans le cas où l'utilisateur entre le début à travers les informations qui lui sont envoyées par l'administrateur fait face à la page pour changer le mot de passe

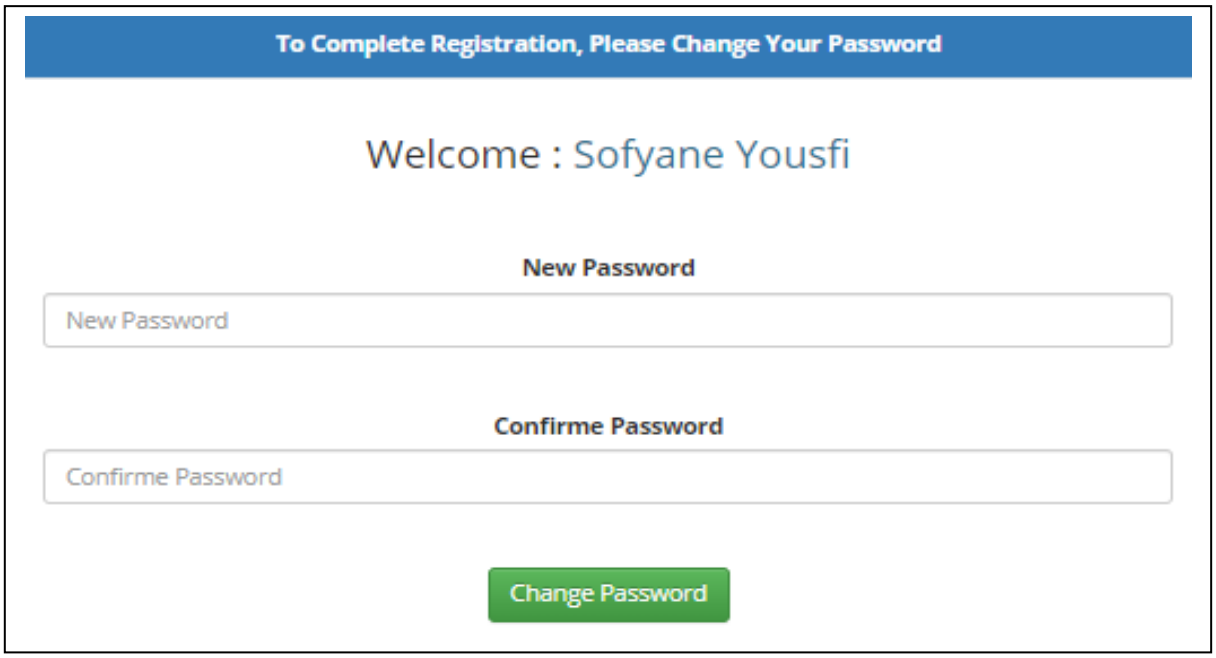

FIGURE 4.2 : Capteur de Page changement de mot de passe .

3.3. Page add User :

Dans cette page, l'administrateur peut voir, ajouter ou supprimer un utilisateur

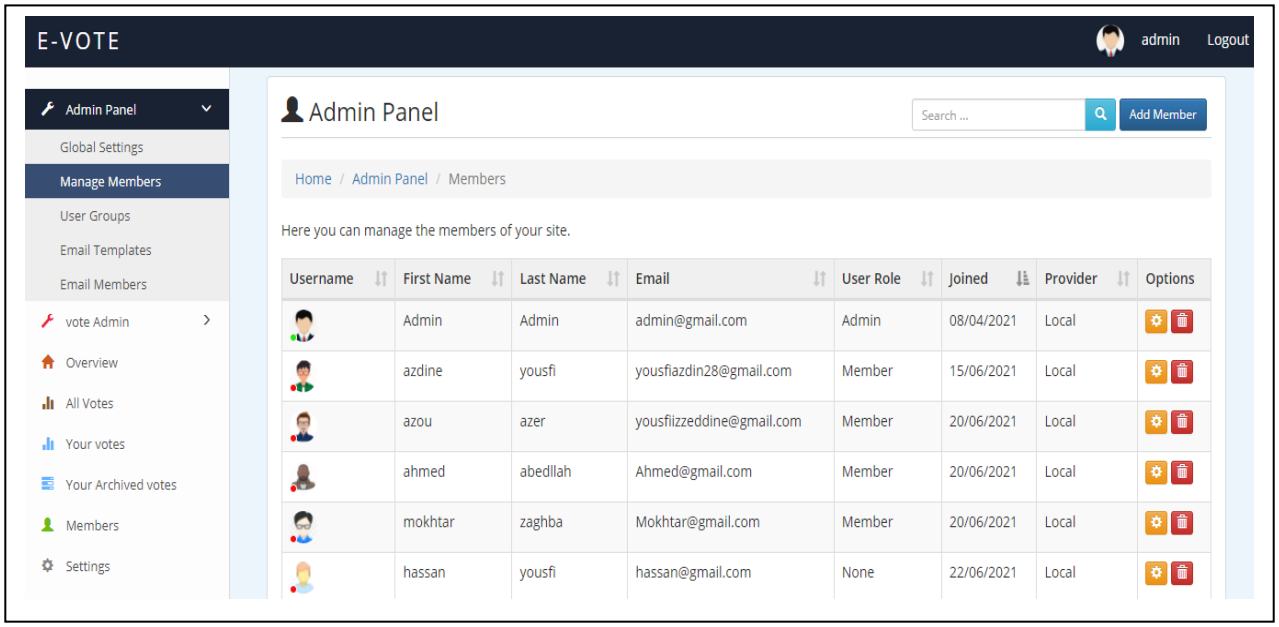

FIGURE 4.3 : Capteur manager user

3.4.. Dashboard :

Après l'authentification l'administrateur , une zone de tableau de bord vous sera présent

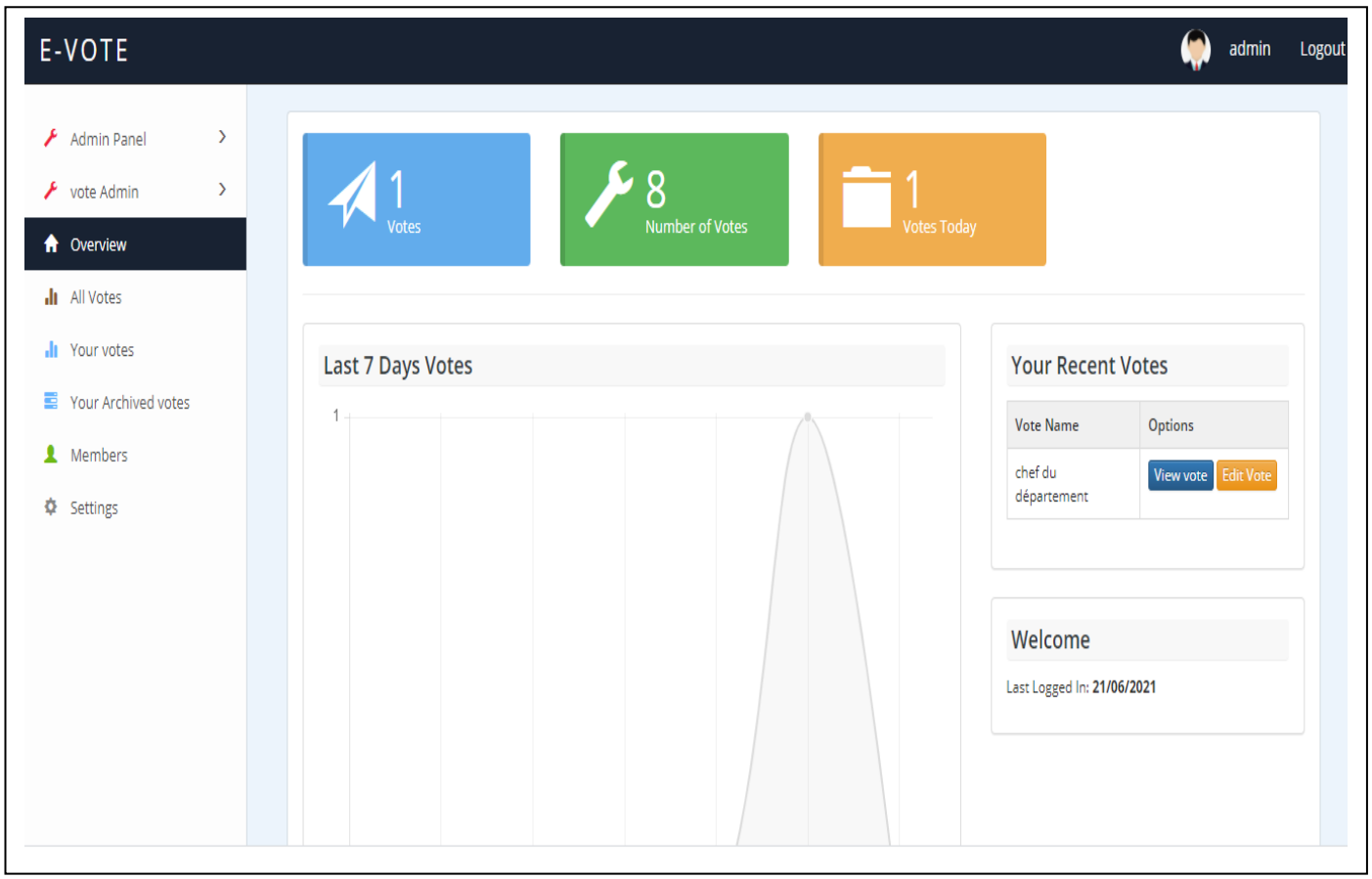

FIGURE 4.4 : Capteur de Page Dashbord.

Cette zone vous donne un aperçu des votes que vous avez créés. , vous ne verrez probablement pas beaucoup d'informations, mais lorsque vous commencerez à voter, vous pourrez voir le nombre récent de votes que vous avez obtenus au cours des 7 derniers jours, le total des votes obtenus et d'autres données intéressantes et utiles qui vous aideront à obtenir un aperçu rapide de vos sondages actuels.

Vous remarquerez également une barre latérale qui contient des liens utiles que vous pouvez naviguer. Si vous êtes connecté en tant qu'utilisateur administrateur, vous remarquerez le lien du panneau d'administration. En cliquant dessus, vous développerez le menu, vous présentant plus d'options.

3.5. Your Votes

Le nœud du système est la zone de vos votes. C'est là que vous pouvez créer de nouveaux votes et gérer ceux qui existent déjà. Il y a deux zones pour afficher vos sondages: Vos votes et Vos votes archivés. Les sondages archivés sont ceux que vous définissez sur Archivé

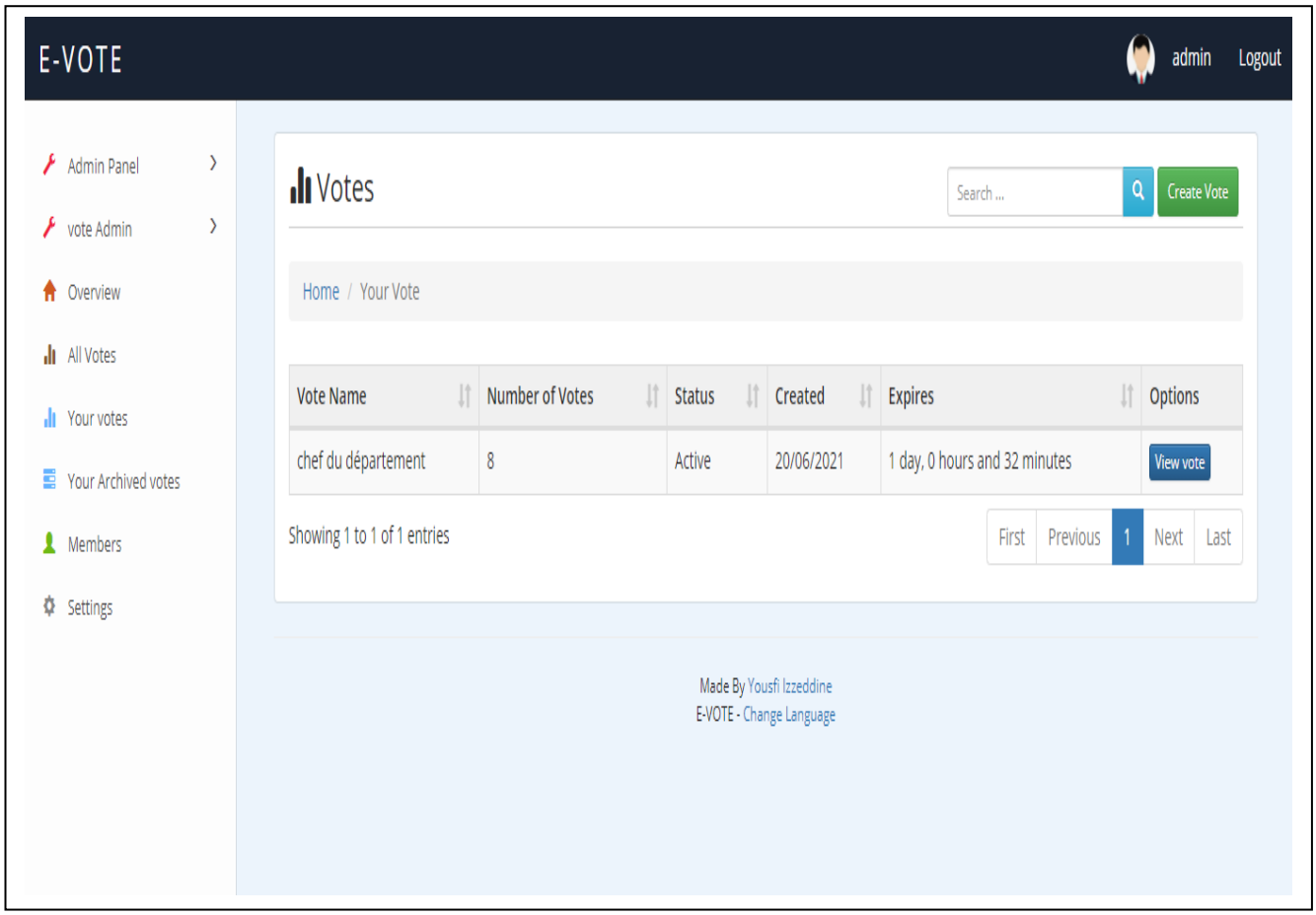

FIGURE 4.5 : Capteur de Page your vote .

3.6. Create Vote :

Cette section vous permet de créer un tout nouveau vote. Ici, vous pouvez donner un nom à votre vote et appliquer divers paramètres à votre vote. Vous pouvez faire expirer un vote après un certain laps de temps en sélectionnant des options limitées dans le temps. Il y a aussi la possibilité de permettre à l'utilisateur de voter pour plusieurs options lors du vote. Il existe également d'autres options, telles que les thèmes de vote, qui modifient la façon dont votre vote individuel est affiché.

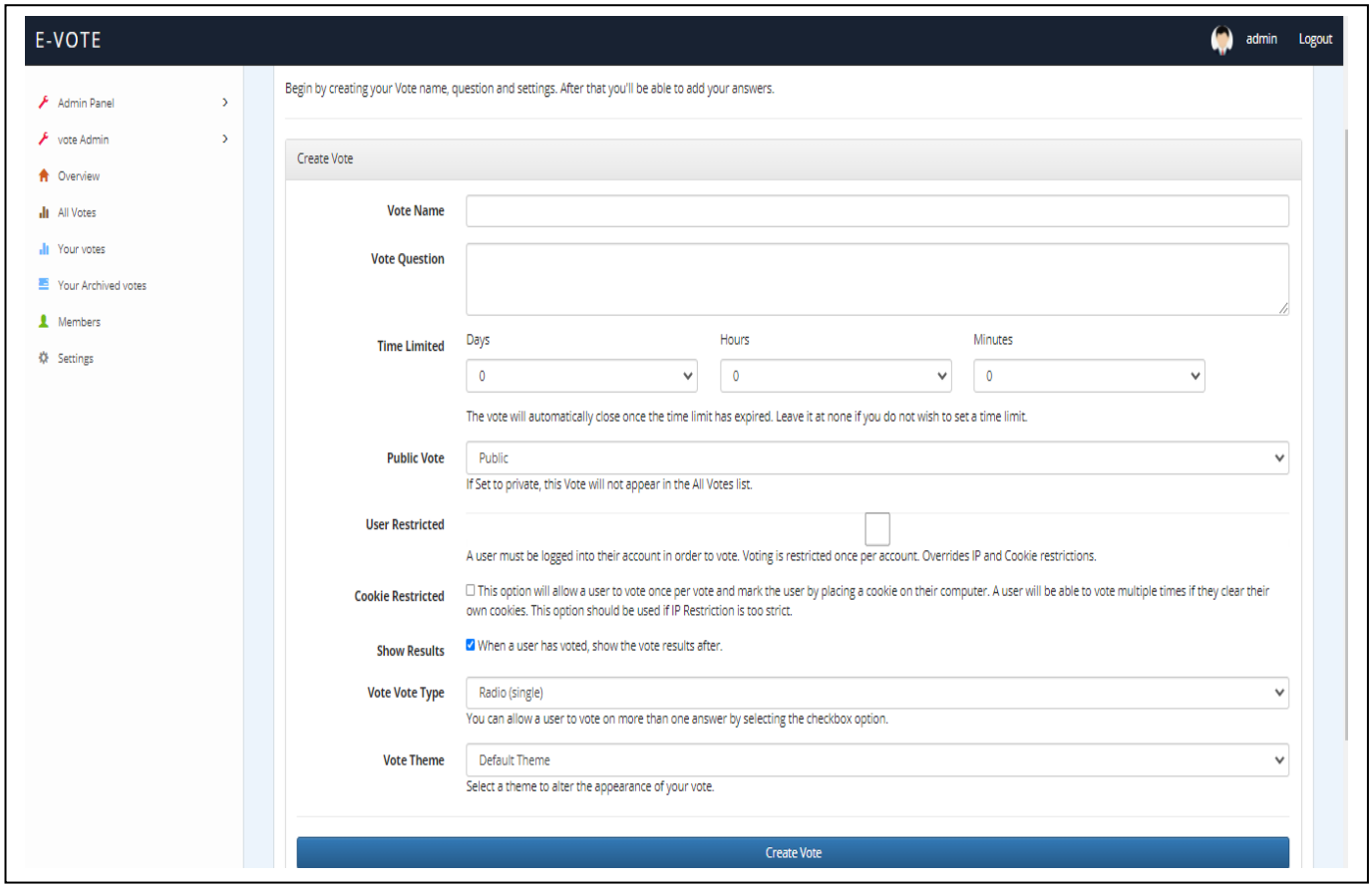

FIGURE 4.6 : Capteur de Page cérate vote .

3.7. Voir les résultats du vote :

De là, les résultats du vote peuvent être vus via un graphique ou par le pourcentage de chaque candidat

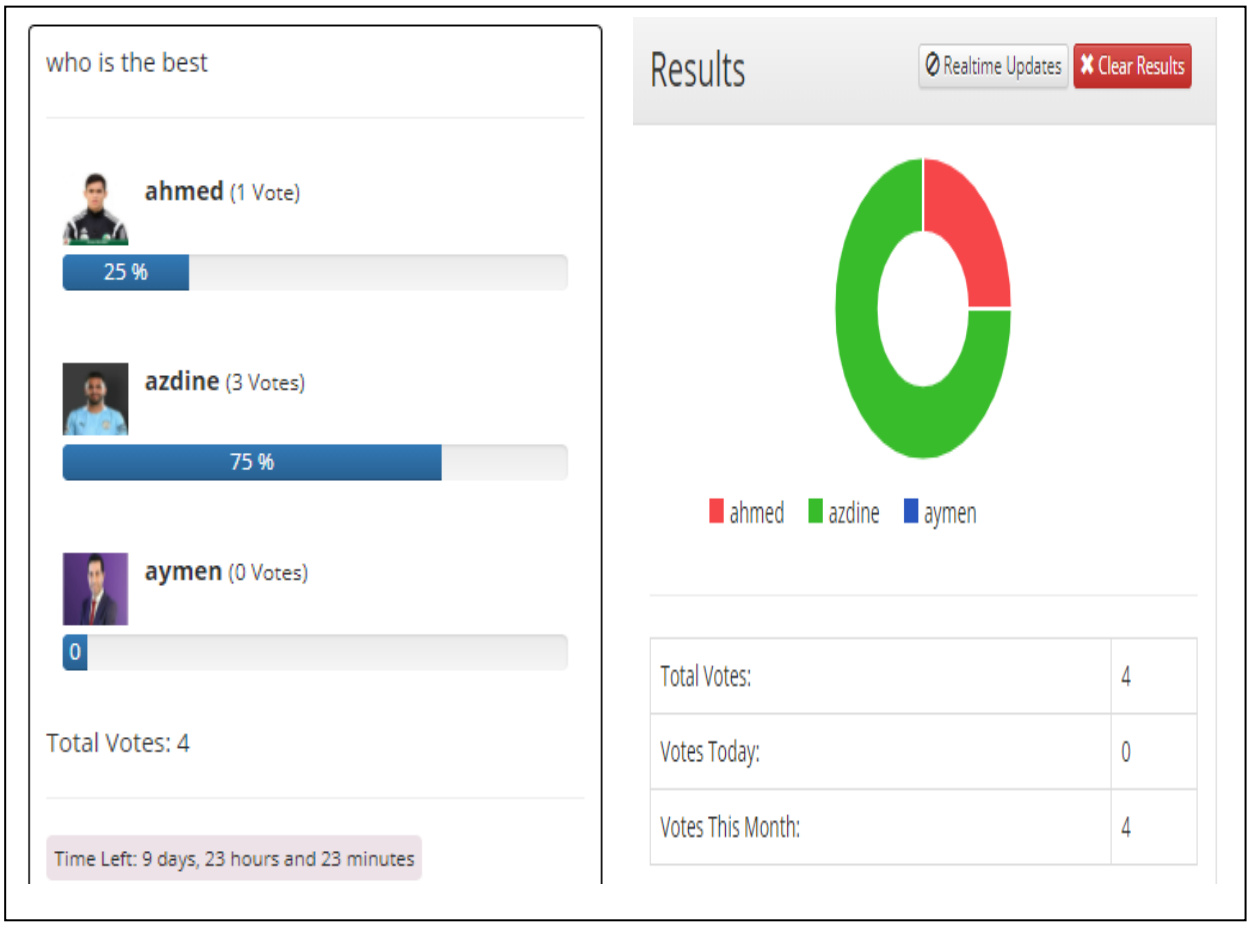

FIGURE 4.7 : Capteur de Page Voir les résultats du vote .

4. Exemples de code source :

5.1.Login :

```php
private function login_protect($email)
    {
        if($this->settings->info->login_protect) {
            // Add Count
            $s = $this->login_model
                ->get_login_attempts($_SERVER['REMOTE_ADDR'],
                    $email, (15*60));
            if($s->num_rows() > 0) {
                $s = $s->row();
                $this->login_model->update_login_attempt($s->ID, array(
                    "count" => $s->count+1
                    )
                );
            } else {
                $this->login_model->add_login_attempt(array(
                    "IP" => $_SERVER['REMOTE_ADDR'],
                    "username" => $email,
                    "count" => 1,
                    "timestamp" => time()
                    )
                );
            }
        }
    }
```

FIGURE 4.8 : Example de code login .

5.2.Cérate vote :

```php
public function create_pro()
    {
        $this->requirements();
        $name = $this->common->nohtml($this->input->post("name"));
        $question = $this->common->nohtml($this->input->post("question"));
        $days = intval($this->input->post("days"));
        $hours = intval($this->input->post("hours"));
        $minutes = intval($this->input->post("minutes"));
        $ip_restriction = intval($this->input->post("ip_restriction"));
        $show_results = intval($this->input->post("show_results"));
        $vote_type = intval($this->input->post("vote_type"));
        $themeid = intval($this->input->post("themeid"));
        $cookie_restriction = intval($this->input->post("cookie_restriction"));
        $user_restriction = intval($this->input->post("user_restriction"));

        $public = intval($this->input->post("public"));

        $theme = $this->polls_model->get_poll_theme($themeid);
        if($theme->num_rows() == 0) $this->template->error(lang("error_66"));

        $time = 0;
        $time = ($days * (3600 *24)) + ($hours * 3600) + ($minutes * 60);
        if($time > 0) {
            $time = time() + $time;
        }

        if(empty($name)) $this->template->error(lang("error_70"));
        if(empty($question)) $this->template->error(lang("error_71"));

        $hash = md5(rand(1,10000000) . "polls");

        $pollid = $this->polls_model->create_poll(array(
            "userid" => $this->user->info->ID,
            "name" => $name,
            "question" => $question,
            "timestamp" => $time,
            "created" => time(),
            "ip_restricted" => $ip_restriction,
            "show_results" => $show_results,
            "updated" => time(),
            "hash" => $hash,
            "vote_type" => $vote_type,
            "themeid" => $themeid,
            "cookie_restricted" => $cookie_restriction,
            "user_restricted" => $user_restriction,
            "public" => $public
            )
        );

        $this->session->set_flashdata("globalmsg", lang("success_34"));
        redirect(site_url("polls/edit_poll/" . $pollid));
    }
```

FIGURE 4.9: Example de code cérate vote .

6. Conclusion

La première partie de ce chapitre a été concrétisée par la présentation des différents outils utilisés pour la réalisation de notre projet, justifier le choix du langage tel que php, Mysql, ainsi XAMPP comme outil de développement. Dans la deuxième partie nous avons donné le coté réalisation de notre projet, avec des exemples d'interfaces plus important.

CONCLUSION GÉNÉRALE

Dans ce mémoire, nous avons abordé le thème « Conception et réalisation d'un système de vote électronique pour université .

Au début, nous avons abordé une connaissance générale du vote électronique, puis nous avons présenté quelques travaux antérieurs et expliqué certains de ses systèmes pour fournir le système que nous avons réalisé .

Nous avons utilisé le langage UML pour modéliser notre système Pour donner une idée de la façon de créer l'application et son mécanisme de travaille.

Vu la contrainte de temps ce travail n'est qu'un début et il reste ouvert à plusieurs extensions.Nous envisageons à moyen terme, de compléter l'implémentation des éléments suivants:

- sécurité Mieux
- Interface simplifiée et facilité d'accès

Au terme de ce présent mémoire, nous considérons notre travail comme un petit pas en avant

Résume

Au cours des dix dernières années, on a beaucoup parlé du vote électronique, et plus particulièrement du vote par Internet, comme méthode de vote supplémentaire susceptible de simplifier le processus électoral et de le rendre plus efficace pour les partis politiques, pour les candidats, pour l'administration électorale et, surtout, pour les électeurs. Divers genres de vote par Internet ou à distance ont été mis en œuvre avec plus ou moins de succès. Si certains systèmes ont bien fonctionné, des projets pilotes dans d'autres administrations électorales ont été annulés, parfois même avant la mise en place du prototype, en raison de craintes ou de problèmes ayant trait à la sécurité, à la fiabilité technique et à la protection des renseignements personnels.

L'objectif de ce travail est de concevoir et mettre en œuvre un système de vote électronique pour l'université, qui permet la réalisation d'élections via Internet tout en assurant la sécurité de l'information des électeurs et la transparence du processus électoral.

Mots clés : E-vote, vote en ligne, vote électronique élection, vote par Internet .

Summary

Over the past decade, there has been a great deal of talk about electronic voting, particularly Internet voting, as an additional method of voting that could simplify the electoral process and make it more efficient for political parties, candidates, electoral administration and, above all, voters. Various types of Internet and remote voting have been implemented with varying degrees of success. While some systems have worked well, pilot projects in other electoral jurisdictions have been cancelled, sometimes even prior to the implementation of the prototype, due to concerns or issues related to security, technical reliability and privacy.

The objective of this work is to design and implement an electronic voting system for the university, which allows the conduct of elections via the Internet while ensuring the security of voter information and the transparency of the electoral process.

Keywords: E-voting, online voting, electronic voting election, Internet voting ,

ملخص :

على مدى العقد الماضي ، كان هناك قدر كبير من الحديث عن التصويت الإلكتروني ، وخاصة التصويت عبر الإنترنت ، كطريقة إضافية للتصويت يمكن أن تبسط العملية الانتخابية وتجعلها أكثر كفاءة للأحزاب السياسية والمرشحين والإدارة الانتخابية ، وقبل كل شيء ، الناخبين. تم تنفيذ أنواع مختلفة من الإنترنت والتصويت عن بعد بدرجات متفاوتة من النجاح. وفي حين أن بعض النظم قد نجحت بشكل جيد ، فقد ألغيت مشاريع تجريبية في ولايات انتخابية أخرى ، حتى في بعض الأحيان قبل تنفيذ النموذج الأولي ، بسبب شواغل أو قضايا تتعلق بالأمن والموثوقية التقنية والخصوصية

الهدف من هذا العمل هو تصميم وتنفيذ نظام التصويت الإلكتروني للجامعة ، مما يسمح بإجراء الانتخابات عبر الإنترنت مع ضمان أمن معلومات الناخب و شفافية العملية الانتخابية

الكلمات الرئيسية : التصويت الإلكتروني ، التصويت عبر الإنترنت ، انتخابات التصويت الإلكترونية ، التصويت عبر الإنترنت

BIBLIOGRAPHIE

[1] Une analyse comparative du vote électronique , rapport Canadien 2010

https://carleton.ca/canadaeurope/wp-content/uploads/AComparativeAssessmentOfInternetVotingFINALFeb19-f.pdf

[2] B. Schneier. Cryptographie appliquée. International Thomson Publishing Company, Paris 1997.

[3] A. Riera-Jorba. Design of Implementable Solutions for Large Scale Electronic Voting Schemes. PhD Thesis, Universitat Autònoma de Barcelona, décembre 1999.

[4] A.D. Rubin. Security considerations for remote electronic voting over the Internet. 29th Research Conference on Communication, Information and Internet Policy (TPRC 2001), octobre 2001. http: //www.arxiv.org/abs/cs.CY/0108017.

[5] M.J. Radwin. An untraceable, universally verifiable voting scheme. Seminar in Cryptology, December 12, 1995. http://www.radwin.org/michael/projects/voting.pdf.

[6] The logi.crypto Java Package, version 1.1.1. http://www.logi.org/logi.crypto/ index.html

[7] C. Benaloh, Verifiable secret-ballot elections, PhD Thesis, Yale University, Department of Computer Science, (1987)

[8] D. Bleichenbacher, Chosen ciphertext attacks against protocols based on the rsa encryption standard, Advances in Cryptology : Proceedings of CRYPTO '98, (1998), p. 1–12.

[9]. https://www.inria.fr/fr/vote-par-internet

[10] L.F.Cranor et R.K. Cytron. Sensus : A security conscious electronic polling system for the Internet. Proceedings of the Hawaii International Conference on System Sciences, janvier 1997, Wailea, Hawaii, USA.

[11] D. Chaum. Untraceable electronic mail, return addresses and digital pseudonyms. Communications of the ACM, vol. 24, no. 2, pages 84–88, 1981.

[12] Benmeziane, S., & Khelladi, L. I-Vote: Un système de vote électronique hautement sécurisé. *Atelier SEcurité des Communications sur Internet (SECI'02) Hôtel El Mechtel, Tunis, Tunisie 19–21 septembre 2002*, 47.

[13] Elections Québec (2020). Vote par internet – etude en contexte québécois. https://www.electionsquebec.qc.ca/francais/chercheurs/vote-par-internet.php.

[14] Electoral Commission NSW (2010). Report on the Feasibility of providing "iVote" Remote Electronic Voting System. https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/Report on-the-feasibility-of-providing-iVote-remote-electronic-voting-system-(PDF-1004kB).pdf.

[15] Electoral Commission NSW (2010). Report on the Feasibility of providing "iVote" Remote Electronic Voting System. https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/Report on-the-feasibility-of-providing-iVote-remote-electronic-voting-system-(PDF-1004kB).pdf.

[16] Electoral Commission NSW (2019a). iVote refresh project for the 2019 NSW State election. https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/iVote%20reports/iVoteRefresh.pdf.

[17] Electoral Commission NSW (2015). Report on the conduct of the 2015 state general election. https://www.elections.nsw.gov.au/NSWEC/media/NSWEC/Reports/Election%20reports/2015 - State-election-report-(PDF-8.4MB).pdf.

[18] Halderman, J.A. and Teague, V. (2015). The New South Wales iVote system: Security failures and verification flaws in a live online election. E-voting and identity - 5th international conference, voteid 2015 (2015), 35–53.

[19] Electoral Commission NSW (2019b). NSW Electoral Commission iVote and Swiss Post e-voting. https://www.elections.nsw.gov.au/About-us/Media-centre/News-media-releases/NSWElectoral-Commission-iVote-and-Swiss-Post-e-vo.

[20] Haines, T. et al. (2020). How not to prove your election outcome. 2020 IEEE symposium on security and privacy (May 2020).

[21] National Electoral Committee (2015). E-hääletamise süsteemi infoturbe poliitika (e-voting system information security policy). https://www.valimised.ee/sites/default/files/uploads/eh/EHA-02-03-2.1_ehaaletamise_infoturbe_poliitika.pdf.

[22] Estonian Parliament (2002). Riigikogu valimise seadus (riigikogu election act). https://www.riigiteataja.ee/akt/125102016022.

[23]. Schryen, G. and Rich, E. (2009). Security in large-scale internet elections: A retrospective analysis of elections in Estonia, The Netherlands, and Switzerland. IEEE Transactions on Information Forensics and Security. 4, 4 (2009), 729–744.

[24]. Schryen, G. and Rich, E. (2009). Security in large-scale internet elections: A retrospective analysis of elections in Estonia, The Netherlands, and Switzerland. IEEE Transactions on Information Forensics and Security. 4, 4 (2009), 729–744.

[25]. Halderman, J.A. et al. (2014). Security analysis of the Estonian internet voting system. Nr. May. (2014).

[26] OSCE (2011). Estonia, parliamentary elections, 6 March 2011: Final report. https://www.osce.org/odihr/77557.

[27] Nurse, J. et al. 2016. An independent assessment of the procedural components of the Estonian internet voting system (2016).

[28] Silver Tambur (2017). Possible security risk affects 750,000 Estonian id-cards. https://estonianworld.com/technology/possible-security-risk-affects-750000-estonian-idcards/.

[29]. Ministère de l'économie et la communication (2019). Le ministre du commerce extérieur et de l'informatique convoquera un groupe de travail sur le vote électronique et le vote électronique (en estonien). https://www.mkm.ee/et/uudised/valiskaubandus-ja-it-minister-kutsub-kokkuelektroonilise-valimissusteemi-ja-elektroonilise

[30] Postimees (2019). E-voting task force finishes report including 25 proposals for improving system. https://news.postimees.ee/6849632/e-voting-task-force-finishes-report-including-25-proposalsfor-improving-system.

[31] Gouvernement norvégien (2015). Evaluation of the e-voting trial in 2013. https://www.regjeringen.no/en/historical-archive/Stoltenbergs-2nd-Government/Ministry-of-Local-Government-and-Regiona/tema-og-redaksjonelt-innhold/kampanjesider/e-votetrial/evaluations-of-the-e-voting-trials/evaluation-of-the-e-voting-trial-in-2013/id2465637/.

[32] Gouvernement norvégien (2014). Internet voting pilot to be discontinued. https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/.

[33]). Gouvernement norvégien (2014). Internet voting pilot to be discontinued. https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/.

[34] Gjøsteen, K. (2013). The norwegian internet voting protocol. International conference on e-voting and identity, 1–18.

[35] Bjørstad Tor E. (2014). The rise and fall of internet voting in Norway (31C3 talk). https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2551/original/31c3-final.pdf.

[36]; Gouvernement norvégien (2013). Evaluation of the e-voting trial in 2011. https://www.regjeringen.no/no/dokumentarkiv/stoltenberg-ii/krd/tema-og-redaksjoneltinnhold/kampanjesider/e-valg-2011-prosjektet/evaluering/evalueringen-av-e-valgforsoket-ertilgje/id684642/.

[37] Bjørstad Tor E. (2014). The rise and fall of internet voting in Norway (31C3 talk). https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2551/original/31c3-final.pdf.

[38] Bjørstad Tor E. (2014). The rise and fall of internet voting in Norway (31C3 talk). https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2551/original/31c3-final.pdf.

[39] Bjørstad Tor E. (2013). Source code audit of Norwegian electronic voting system. https://www.regjeringen.no/globalassets/upload/krd/prosjekter/evalg/kildekode/evalg_rapport_kildekodegjennomgang.pdf.

[40] Bjørstad Tor E. (2014). The rise and fall of internet voting in Norway (31C3 talk). https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2551/original/31c3-final.pdf.

[41] Zachariassen Espen (2011). Tout le monde a été trompé dans un faux e-choix (en norvégien).https://www.tu.no/artikler/alle-ble-lurt-i-falskt-e-valg/246389.

[42] Zachariassen Espen (2013). Erreur de cryptage des votes électroniques (en norvégien). https://www.tu.no/artikler/feil-i-krypteringen-av-e-stemmer/234436.

[43] BBC (2014). E-voting experiments end in norway amid security fears. https://www.bbc.com/news/technology-28055678.

[44] Bjørstad Tor E. (2014). The rise and fall of internet voting in Norway (31C3 talk). https://fahrplan.events.ccc.de/congress/2014/Fahrplan/system/attachments/2551/original/31c3-final.pdf.